Research Insights

Improving the Safety and Efficiency of Emergency Services

Emerging Tools and Technologies for First Responders

Information Resources Management Association

IGI Global
DISSEMINATOR OF KNOWLEDGE

Improving the Safety and Efficiency of Emergency Services:

Emerging Tools and Technologies for First Responders

Information Resources Management Association
USA

A volume in the Trending Topics
Book Series (TTBS) Book Series

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Information Resources Management Association, editor.
Title: Improving the safety and efficiency of emergency services : emerging tools and technologies for first responders / Information Resources Management Association, editor.
Description: Hershey, PA : Information Science Reference, [2020] | Includes bibliographical references and index. | Summary: "This book addresses the latest tools that can support first responders in their ultimate goal: delivering their patients to safety. It also explores how new techniques and devices can support first responders in their work by addressing their safety, alerting them to accidents in real time, connecting them with medical experts to improve the chances of survival of critical patients, predicting criminal and terrorist activity, locating missing persons, and allocating resources"-- Provided by publisher.
Identifiers: LCCN 2019042033 (print) | LCCN 2019042034 (ebook) | ISBN 9781799825357 (h/c) | ISBN 9781799825364 (s/c) | ISBN 9781799825371 (eISBN)
Subjects: LCSH: Emergency management--Information technology. | Technological innovations. | First responders. | Accident victims.
Classification: LCC HV551.2 .I498 2020 (print) | LCC HV551.2 (ebook) | DDC 363.34/80684--dc23
LC record available at https://lccn.loc.gov/2019042033
LC ebook record available at https://lccn.loc.gov/2019042034

This book is published in the IGI Global book series Trending Topics (TTBS) (ISSN: pending; eISSN: pending)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Trending Topics Book Series (TTBS) Book Series

Mehdi Khosrow-Pour, D.B.A.
Information Resources Management Association, USA

ISSN:pending
EISSN:pending

MISSION

Every day all over the world, researchers are making groundbreaking discoveries that address current challenges and solve complex problems across a variety of fields. Due to advancements in technology, changes in demographics, adjustments to societal norms, the development of political and economic structures, and more, new theories, methods, strategies, techniques, and applications are constantly being established in response to both existing and evolving issues.

Based on the success of IGI Global's latest Trending Topics Campaign, which provides news snippets and trending research breakthroughs relevant to IGI Global content, IGI Global has launched this new book series, titled the **Trending Topics Book Series**, which offers small anthologies of reprinted IGI Global book chapters and journal articles hand-selected by IGI Global's Executive Editorial Board on topics currently trending and stirring up discussion and/or controversy.

Spanning across topics such as the multigenerational workforce, legislation for sustainability, emotional branding, privacy on mobile devices, robotics in healthcare, and bio-based product development, this book series aims to provide researchers, academicians, professionals, and students with the most up-to-date studies in order to advance knowledge across all industries.

COVERAGE

- Privacy on Mobile Devices
- Eco-Cities
- Millennials
- Inclusive Learning
- Aging Workforce
- Bio-Based Product Development
- Multi-Generational Workforce
- Robotics in Healthcare
- Environmental Legislation and Sustainability
- Women in STEM Fields

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at Acquisitions@igi-global.com or visit: http://www.igi-global.com/publish/.

The Trending Topics Book Series (TTBS) Book Series (ISSN pending) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, www.igi-global.com. This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit http://www.igi-global.com/book-series/trending-topics-book-series/228608. Postmaster: Send all address changes to above address.

Titles in this Series

For a list of additional titles in this series, please visit:
https://www.igi-global.com/book-series/trending-topics-book-series/228608

Alternative Pain Management Solutions for Avoiding Prescription Drug Overuse
Information Resources Management Association (USA)
Medical Information Science Reference • © 2020 • 388pp • H/C (ISBN: 9781799816805) • US $245.00

Developing Safer Online Environments for Children Tools and Policies for Combatting Cyber Aggression
Information Resources Management Association (USA)
Information Science Reference • © 2020 • 416pp • H/C (ISBN: 9781799816843) • US $215.00

Five Generations and Only One Workforce How Successful Businesses Are Managing a Multigenerational Workforce
Information Resources Management Association (USA)
Business Science Reference • © 2020 • 364pp • H/C (ISBN: 9781799804376) • US $215.00

Developing Eco-Cities Through Policy, Planning, and Innovation Can It Really Work?
Information Resources Management Association (USA)
Engineering Science Reference • © 2020 • 374pp • H/C (ISBN: 9781799804413) • US $195.00

IGI Global
DISSEMINATOR OF KNOWLEDGE

701 East Chocolate Avenue, Hershey, PA 17033, USA
Tel: 717-533-8845 x100 • Fax: 717-533-8661
E-Mail: cust@igi-global.com • www.igi-global.com

List of Contributors

Abejith, M. / *SASTRA University, India*......293
Baker, Abu / *KP Information Technology Board, Pakistan*......340
Boak, George / *York St. John University, UK*......180
Bogdanoski, Mitko / *Military Academy "General Mihailo Apostolski", Macedonia*......239
Brill, Floriane / *Brigade de Sapeurs Pompiers de Paris (BSPP), France*......1
Canonico, Massimo / *University of Piemonte Orientale, Italy*......67
de Silva, Eugenie / *University of Leicester, UK & Virginia Research Institute, USA*......271
Eftelioglu, Emre / *University of Minnesota, USA*......209
Gazzolo, Diego / *Neonatal Intensive Care Unit of Alessandria Children Hospital, Italy*......67
Gold, Jeff / *York Business School, UK*......180
Grangeat, Amélie / *French Alternative Energies and Atomic Energy Commission (CEA), France*......1
Humphries, Georgina / *Canterbury Christ Church University, UK*......434
Hvannberg, Ebba Thora / *University of Iceland, Iceland*......399
Kagawa, Takuhiro / *Kobe University, Japan*......193
Karatas, Mumtaz / *National Defense University, Turkey*......142
Kebbell, Mark / *Griffith University, Australia*......320
Korakis, Antonis / *National Center for Scientific Research Demokritos, Greece*......38
Krlic, Marija / *York St. John University, UK*......180
Lapebie, Emmanuel / *French Alternative Energies and Atomic Energy Commission (CEA), France*......1
Law, Nancy / *University of Hong Kong, Hong Kong*......372
Leung, Lawrence / *Hong Kong Police College, Hong Kong*......372
Logesh, R. / *SASTRA University, India*......293
Metelmann, Bibiana / *Greifswald University, Germany*......88
Metelmann, Camilla / *Greifswald University, Germany*......88
Montani, Stefania / *University of Piemonte Orientale, Italy*......67
Nakamura, Masahide / *Kobe University, Japan & RIKEN AIP, Japan*......193

Ozgur, Ceyhun / *Valparaiso University, USA*...358
Pandey, Kavita / *Jaypee Institute of Information Technology, India*...............19
Papadopoulos, Homer / *National Center for Scientific Research Demokritos, Greece*...38
Raclot, Stéphane / *Brigade de Sapeurs Pompiers de Paris (BSPP), France*...1
Razi, Nasuh / *Turkish Naval Forces, Turkey*...142
Risteski, Aleksandar / *Ss. Cyril and Methodius University, Macedonia*........239
Romyn, David / *Griffith University, Australia*..320
Rudinsky, Jan / *University of Iceland, Iceland*...399
Saiki, Sachio / *Kobe University, Japan*..193
Seema, S. / *Ramaiah Institute of Technology, India*..114
Shakdher, Arjun / *Jaypee Institute of Information Technology, India*............19
Shekhar, Shashi / *University of Minnesota, USA*...209
Shetty, Chetan / *Ramaiah Institute of Technology, India*...............................114
Sowmya, B. J. / *Ramaiah Institute of Technology, India*.................................114
Srinivasa, K. G. / *CBP Government Engineering College, India*...................114
Stoilkovski, Marjan / *Ministry of Interior, Macedonia*..................................239
Striani, Manuel / *University of Turin, Italy*..67
Strozzi, Mariachiara / *Neonatal Intensive Care Unit of Alessandria Children Hospital, Italy*...67
Subramaniyaswamy, V. / *SASTRA University, India*....................................293
Tang, Xun / *University of Minnesota, USA*...209
Tozan, Hakan / *Istanbul Medipol University, Turkey*.....................................142
Umamakeswari, A. / *SASTRA University, India*...293
Umasankar, Sunil / *SASTRA University, India*..293
Watt, Peter / *York St. John University, UK*..180
Wilkinson, Dawn Heather / *West Yorkshire Police, UK*.................................180
Williams, Joseph / *Canterbury Christ Church University, UK*......................434

Table of Contents

Preface xi

Section 1
Fire, Rescue, and Emergency Medical Services

Chapter 1
Mapping of Areas Presenting Specific Risks to Firefighters Due to Buried Technical Networks 1
Amélie Grangeat, French Alternative Energies and Atomic Energy Commission (CEA), France
Stéphane Raclot, Brigade de Sapeurs Pompiers de Paris (BSPP), France
Floriane Brill, Brigade de Sapeurs Pompiers de Paris (BSPP), France
Emmanuel Lapebie, French Alternative Energies and Atomic Energy Commission (CEA), France

Chapter 2
REDAlert+: Medical/Fire Emergency and Warning System using Android Devices 19
Arjun Shakdher, Jaypee Institute of Information Technology, India
Kavita Pandey, Jaypee Institute of Information Technology, India

Chapter 3
Predicting Medical Resources Required to be Dispatched After Earthquake and Flood, Using Historical Data and Machine Learning Techniques: The COncORDE Emergency Medical Service Use Case 38
Homer Papadopoulos, National Center for Scientific Research Demokritos, Greece
Antonis Korakis, National Center for Scientific Research Demokritos, Greece

Chapter 4
TEEM: Technology-Enhanced Emergency Management for Supporting Data Communication During Patient Transportation..67
Massimo Canonico, University of Piemonte Orientale, Italy
Stefania Montani, University of Piemonte Orientale, Italy
Diego Gazzolo, Neonatal Intensive Care Unit of Alessandria Children Hospital, Italy
Mariachiara Strozzi, Neonatal Intensive Care Unit of Alessandria Children Hospital, Italy
Manuel Striani, University of Turin, Italy

Chapter 5
Live Video Communication in Prehospital Emergency Medicine 88
Camilla Metelmann, Greifswald University, Germany
Bibiana Metelmann, Greifswald University, Germany

Chapter 6
Effective Prevention and Reduction in the Rate of Accidents Using Internet of Things and Data Analytics 114
B. J. Sowmya, Ramaiah Institute of Technology, India
Chetan Shetty, Ramaiah Institute of Technology, India
S. Seema, Ramaiah Institute of Technology, India
K. G. Srinivasa, CBP Government Engineering College, India

Chapter 7
Assessing the Performance of a SAR Boat Location-Allocation Plan via Simulation..142
Mumtaz Karatas, National Defense University, Turkey
Nasuh Razi, Turkish Naval Forces, Turkey
Hakan Tozan, Istanbul Medipol University, Turkey

Section 2
Security and Law Enforcement

Chapter 8
Introducing Predictive Policing Technologies (PPT): An Action Research-Oriented Approach for EBOCD Initiatives...180
Peter Watt, York St. John University, UK
George Boak, York St. John University, UK
Marija Krlic, York St. John University, UK
Dawn Heather Wilkinson, West Yorkshire Police, UK
Jeff Gold, York Business School, UK

Chapter 9
PRISM: Visualizing Personalized Real-Time Incident on Security Map 193
Takuhiro Kagawa, Kobe University, Japan
Sachio Saiki, Kobe University, Japan
Masahide Nakamura, Kobe University, Japan & RIKEN AIP, Japan

Chapter 10
Crime Hotspot Detection: A Computational Perspective 209
Emre Eftelioglu, University of Minnesota, USA
Shashi Shekhar, University of Minnesota, USA
Xun Tang, University of Minnesota, USA

Chapter 11
Novel First Responder Digital Forensics Tool as a Support to Law Enforcement 239
Mitko Bogdanoski, Military Academy "General Mihailo Apostolski", Macedonia
Marjan Stoilkovski, Ministry of Interior, Macedonia
Aleksandar Risteski, Ss. Cyril and Methodius University, Macedonia

Chapter 12
Detecting Individual-Level Deception in the Digital Age: The DETECT Model © 271
Eugenie de Silva, University of Leicester, UK & Virginia Research Institute, USA

Chapter 13
Sentiment Analysis of Tweets for Estimating Criticality and Security of Events..293
V. Subramaniyaswamy, SASTRA University, India
R. Logesh, SASTRA University, India
M. Abejith, SASTRA University, India
Sunil Umasankar, SASTRA University, India
A. Umamakeswari, SASTRA University, India

Chapter 14
Using the Internet to Plan for Terrorist Attack 320
David Romyn, Griffith University, Australia
Mark Kebbell, Griffith University, Australia

Chapter 15
JPSC KP: Joint Public Safety Cell App 340
Abu Baker, KP Information Technology Board, Pakistan

Chapter 16
Resources in Parks and Police Management Applying Decision Utility to Solve Problems With Limited Resources 358
Ceyhun Ozgur, Valparaiso University, USA

Section 3
Training Tools

Chapter 17
Design Principles for Online Role Play Simulations to Address Groupthink Tendency in Professional Training: An Exploration..372
Lawrence Leung, Hong Kong Police College, Hong Kong
Nancy Law, University of Hong Kong, Hong Kong

Chapter 18
Transferability of Voice Communication in Games to Virtual Teams Training for Crisis Management..399
Jan Rudinsky, University of Iceland, Iceland
Ebba Thora Hvannberg, University of Iceland, Iceland

Chapter 19
Analysis of a Training Package for Law Enforcement to Conduct Open Source Research..434
Joseph Williams, Canterbury Christ Church University, UK
Georgina Humphries, Canterbury Christ Church University, UK

Related Readings.. 452

Index.. 462

Preface

During emergency situations, society relies upon the efficient response time and effective services of emergency facilities that include fire departments, law enforcement, search and rescue, and emergency medical services (EMS). First responders are obligated to arrive quickly to the scene of accidents, natural disasters, and terrorist attacks in order to improve the likelihood of survival of those affected by the incident. As such, it is imperative that emergency crews are outfitted with technologies that can cut response time and also predict where such events may occur and prevent them from happening.

The safety of first responders is also of paramount concern. Too often it is reported that emergency personnel have died on the scene, and while their jobs do carry a high level of risk, oftentimes they are killed while doing routine tasks, such as traffic stops. New tools can be implemented to map areas of vulnerability for emergency responders, and new strategies can be devised in their training to ensure that they are conditioned to respond efficiently to an emergency and conscious of best safety protocols.

In response to the need for advanced research that can address these current issues and offer innovative solutions, IGI Global is pleased to offer this comprehensive reference of reprinted IGI Global book chapters and journal articles that have been hand-picked by our senior editorial staff on this topic that is currently trending and stirring up discussion and controversy within the field of business. The following book aims to equip law enforcement, fire departments, paramedics, emergency medical technicians, hospital staff, doctors, and rescuers with the latest tools and technologies available to support them in conducting their work. Additionally, it is intended for IT consultants and technology developers looking to aid in the development of new technologies and government officials and policymakers looking to implement these tools in their community's emergency services. Finally, the book will empower academicians, researchers, and students researching the latest techniques and devices that can be utilized by first responders to make their work safer and more efficient.

Based on the success of IGI Global's latest Trending Topics Campaign, which provides news snippets and trending research breakthroughs relevant to IGI Global content, this compilation intends to address the latest tools that can support first responders in their ultimate goal: delivering their patients to safety. Readers will come to understand how new techniques and devices can support first responders in their work by addressing their safety, alerting them to accidents in real-time, connecting them with medical experts to improve the chances of survival of critical patients, predicting criminal and terrorist activity, locating missing persons, and allocating resources.

The following book is designed to act as a single reference source on conceptual, methodological, and technical aspects and will provide insight into emerging topics including but not limited to video communication, vulnerability mapping, predictive policing technologies, crime hotspot detection, digital forensics tools, Groupthink, and crisis management training.

Improving the Safety and Efficiency of Emergency Services: Emerging Tools and Technologies for First Responders is organized into three sections that provide comprehensive coverage of important topics. The sections are:

1. Fire, Rescue, and Emergency Medical Services
2. Security and Law Enforcement
3. Training Tools

The following paragraphs provide a summary of what to expect from this invaluable reference source:

Section 1, "Fire, Rescue, and Emergency Medical Services," opens this extensive reference source by highlighting emerging technologies that support fire and rescue personnel and paramedics by assisting in their safety and efficiency when conducting emergency calls. The first chapter in this section, "Mapping of Areas Presenting Specific Risks to Firefighters Due to Buried Technical Networks," by Prof. Amélie Grangeat from French Alternative Energies and Atomic Energy Commission (CEA), Gramat, France; Profs. Stéphane Raclot and Floriane Brill of Brigade de Sapeurs Pompiers de Paris (BSPP), Paris, France; and Prof. Emmanuel Lapebie from French Alternative Energies and Atomic Energy Commission (CEA), Gramat, France, examines vulnerability areas for firefighters wherein a difficult incident occurs together with a specific risk such as buried networks and proposes a method developed for the Paris Fire Brigade for vulnerability mapping. The next chapter in this section, "REDAlert+: Medical/Fire Emergency and Warning System Using Android Devices," authored by Profs. Arjun Shakdher and Kavita Pandey from Jaypee Institute of Information Technology, Noida, India, examines a mobile application based on the principle of VANETs in combination with wireless communication and database management that when integrated with emergency vehicles and hospitals provides a seamless medical response system at times of an emergency. In the following chapter, "Predicting Medical Resources Required to be Dispatched After Earthquake and Flood, Using Historical Data and Machine Learning Techniques: The COncORDE Emergency Medical Service Use Case," by Profs. Homer Papadopoulos and Antonis Korakis from the National Center for Scientific Research Demokritos, Agia Paraskevi, Greece, a method is presented to predict the medical resources required to be dispatched after large-scale disasters to satisfy the demand. In the next chapter, "TEEM: Technology-Enhanced Emergency Management for Supporting Data Communication During Patient Transportation," the authors, Profs. Massimo Canonico and Stefania Montani from the University of Piemonte Orientale, Alessandria, Italy; Profs. Diego Gazzolo and Mariachiara Strozzi from the Neonatal Intensive Care Unit of Alessandria Children Hospital, Alessandria, Italy; and Prof. Manuel Striani from the University of Turin, Turin, Italy, describe a client-server architecture, designed for supporting data recording and transmission during emergency patient transportation by ambulance. The clients are a set of mobile apps, interfaced to the monitoring devices in the ambulance that automatically send all the recorded data to a server at the destination center. The next chapter, "Live Video Communication in Prehospital Emergency Medicine," by Profs. Camilla Metelmann and Bibiana Metelmann from Greifswald University, Germany, explores the concept of using video-communication in real-time from the emergency site to an emergency doctor that offers an opportunity to enhance the quality of emergency medicine. The core piece of this study is a video camera system called "LiveCity camera," enabling real-time high quality video connection of paramedics and emergency doctors. In the following chapter, "Effective Prevention and Reduction in the Rate of Accidents Using Internet of Things and Data Analytics," by Profs. Sowmya B. J., Chetan Shetty, and Seema S. from the Ramaiah Institute of Technology, India and Prof. Srinivasa K. G. of the CBP Government Engineering College, India, accident detection kits in vehicles are proposed to automate the process of detecting and reporting accidents. The accident notifications are then sent to the concerned hospital and police station and the application guides the paradmedics and police to the accident spot. The final chapter, "Assessing the Performance of a SAR Boat Location-Allocation Plan via Simulation," authored by Prof. Mumtaz Karatas from National Defense University, Turkey; Prof. Nasuh Razi of the Turkish Naval Forces, Turkey; and Prof. Hakan Tozan from Istanbul Medipol University, Turkey, seeks to evaluate the performance of a search and rescue (SAR) boat location plan using simulation. The proposed methodology in this chapter works in two stages: First, an optimal allocation scheme of SAR resources is determined via a multi-objective mathematical model. Next, simulation is used to test the performance of the analytical solution under stochastic demand.

Section 2, "Security and Law Enforcement," includes chapters on the latest technologies and new methods that can be utilized by law enforcement for the detection and prevention of crime. The first chapter in the section, "Introducing Predictive Policing Technologies (PPT): An Action Research-Oriented Approach for EBOCD Initiatives," by Profs. Peter Watt, George Boak, and Marija Krlic from York St. John University, UK; Officer Dawn Heather Wilkinson of the West Yorkshire Police, UK; and Prof. Jeff Gold from York Business School, UK, presents the findings of a 12-week pilot study of a collaborative organizational change project which oversaw the implementation of predictive policing technology (PPT) into a territorial police force in the North of England. In the second chapter, "PRISM: Visualizing Personalized Real-Time Incident on Security Map," Profs. Takuhiro Kagawa and Sachio Saiki from the Graduate School of System Informatics, Kobe University, Kobe, Japan and Prof. Masahide Nakamura from the Graduate School of System Informatics, Kobe University, Kobe, Japan & RIKEN AIP, Tokyo, Japan, proposes a new security information service, called PRISM (Personalized Real-Time Information with Security Map) to provide security information services and regional incident information for residents. In the next chapter, "Crime Hotspot Detection: A Computational Perspective," by Profs. Emre Eftelioglu, Shashi Shekhar, and Xun Tang from the University of Minnesota, USA, crime hotspot detection is examinied in order to focus the deployment of police enforcement and predict the potential residence of a serial criminal. The following chapter, "Novel First Responder Digital Forensics Tool as a Support to Law Enforcement," authored by Prof. Mitko Bogdanoski from the Military Academy "General Mihailo Apostolski", Macedonia; Prof. Marjan Stoilkovski form the Ministry of Interior, Macedonia; and Prof. Aleksandar Risteski from Ss. Cyril and Methodius University, Macedonia, presents a novel developed First Responder script that can be used to perform a live and dead forensics analysis in support of Law Enforcement during the investigation process. The next chapter, "Detecting Individual-Level Deception in the Digital Age: The DETECT Model ©," by Prof. Eugenie de Silva from the University of Leicester, UK & Virginia Research Institute, USA, presents a discussion of a new model titled DETECT (Determining and Evaluating Truthfulness through Explicit Cue Testing) that relies upon the assessment of verbal and non-verbal cues to determine deceptive activities at the individual-level in a technologically advanced society. In the following chapter, "Sentiment Analysis of Tweets for Estimating Criticality and Security of Events," the authors, Profs. V. Subramaniyaswamy, R. Logesh, M. Abejith, Sunil Umasankar, and A. Umamakeswari from the School of Computing, SASTRA University, Thanjavur, India, propose a methodology to obtain a quantitative result called criticality to assess the level of threat for a public event. The proposed system combines this lexicon based sentimental analysis along with deep data collection and segregates the emotions into different levels to analyze the threat for an event. The next chapter, "Using the Internet to Plan for Terrorist Attack," by Profs. David Romyn and Mark Kebbell of Griffith University, Australia, discusses how terrorists can use the internet as a source of information to plan for terrorist attacks through online anonmity services such as virtual prviate networks. The use of the Internet as a reconnaissance tool for target selection is also discussed, along with how this information can be manipulated to reduce the likelihood or severity of a terrorist attack. In the next chapter, "JPSC KP: Joint Public Safety Cell App," the author, Prof. Abu Baker of the KP Information Technology Board, Pakistan, proposes a Joint Public Safety Cell app that is intended to assist the general public in efficient registration of a complaint and keep updates of security forcers' action on their complaint to prevent terorist activities. The final chapter in this section, "Resources in Parks and Police Management Applying Decision Utility to Solve Problems with Limited Resources," authored by Prof. Ceyhun Ozgur from Valparaiso University, Valparaiso, USA, provides examples of where the limited resources may occur in both park and law enforcement agencies and how the manager may overcome these problems by the affective and just sharing of resources. In police departments, affective trade-offs are shown among foot patrol, car patrol, detective analysis, and office work.

Section 3, "Training Tools," presents coverage on new strategies and tools for the effective training of emergency services personnel. The first chapter in this section, "Design Principles for Online Role Play Simulations to Address Groupthink Tendency in Professional Training: An Exploration," by Prof. Lawrence Leung from the Hong Kong Police College, Hong Kong and Prof. Nancy Law from the University of Hong Kong, Hong Kong, reports on a case study of the application of a set of design principles for an online role play simulation in addressing Groupthink in crisis management professional training. In the second chapter of this section, "Transferability of Voice Communication in Games to Virtual Teams Training for Crisis Management," authored by Profs. Jan Rudinsky and Ebba Thora Hvannberg from the University of Iceland, Reykjavik, Iceland, findings on voice communication in online games were researched to search for knowledge on how best to implement communication for virtual environments for the training of crisis management personnel. The practical significance of this work lies in the provision of design implications for a virtual environment for crisis management training. The final chapter of this section, "Analysis of a Training Package for Law Enforcement to Conduct Open Source Research," by Profs. Joseph Williams and Georgina Humphries of Canterbury Christ Church University, Canterbury, UK, introduces law enforcement officials to the open source internet research tool designed to assist with open source research investigations.

Although the primary organization of the contents in this work is based on its three sections, offering a progression of coverage of the important concepts, methodologies, technologies, applications, social issues, and emerging trends, the reader can also identify specific contents by utilizing the extensive indexing system listed at the end.

Section 1

Fire, Rescue, and Emergency Medical Services

Chapter 1
Mapping of Areas Presenting Specific Risks to Firefighters Due to Buried Technical Networks

Amélie Grangeat
French Alternative Energies and Atomic Energy Commission (CEA), France

Stéphane Raclot
Brigade de Sapeurs Pompiers de Paris (BSPP), France

Floriane Brill
Brigade de Sapeurs Pompiers de Paris (BSPP), France

Emmanuel Lapebie
French Alternative Energies and Atomic Energy Commission (CEA), France

ABSTRACT

Vehicles or freight cars on fire below a bridge or inside a tunnel are exceptional events and imply difficult intervention conditions for firefighters. A buried technical network like high voltage electricity line, gas or steam pipeline around such a fire causes additional specifics risks. Vulnerability areas for firefighters are zones where both factors exist: a difficult incident area together with a specific risk like buried networks. They require intervention teams with specific emergency response capabilities. The paper proposes a method developed for the Paris Fire Brigade for vulnerability mapping. Results aim at improving the mobilization in allocating directly the specific responses capabilities intervention teams. Results are debated from an operational point of view. Cutting off several network lines during firefighters' interventions may strongly affect the society. In case of simultaneous incidents in vulnerable areas, firefighters could be an early warning system and inform authorities of the risk of services disruption.

DOI: 10.4018/978-1-7998-2535-7.ch001

INTRODUCTION

DEMOCRITE is a project funded by the French National Research Agency under grant agreement ANR-13-SECU-0007-01 (Lapebie, 2015). It aims at developing a software platform for the French civil security on risks analysis and risk coverage. The Paris Fire Brigade (BSPP) is one of the first engaged institutions when a disaster happens in the Paris and suburbs areas. BSPP is a partner of this project, and helps to define two main lines of research for improving the quality of their emergency services. The first one concerns common incidents: based on the BSPP feedbacks database, DEMOCRITE aims at identifying correlations between incidents and local urbanism, population characteristics and period of the day. Perspectives of this axe concern for instance the "Grand Paris" project. Future fire stations and capacities should be placed in new built areas as a function of expected incidents frequency such as to optimize risk coverage. The second research main line concerns three exceptional risks. First, terrorist bombing: a simplified and fast code is under development for estimating the consequences area of a potential bombing in an urban area. Second, a quarter fire: a modeling of fire propagation speed through several buildings is proposed, not including firefighting for the moment. This could happen with the Seine centennial flooding that threatens Paris: potable water networks could be severely damaged and fire coverage would be difficult to assume. The third point concerns the results of this article: the mapping of territory vulnerabilities linked to technical networks. A perspective of this work concerns the modelling of cascading effects following firefighters dispatch that could require switching off one network. Three deliverables of the DEMOCRITE project have been produced and released to the Paris Fire Brigade in 2015. A first report explains the production of vulnerability maps and analyzes them network-by-network (DEMOCRITE, cartes, 2015). Secondly, an ArcGIS code for the DEMOCRITE toolbox has been developed in order to compute these maps. Another report on the methodology itself explains the structures of the different models inside the toolbox and the technical limits of this approach as well as its implementation with real data. (DEMOCRITE, méthode, 2015). This last report together with the statistics of the first report are presented here. Indeed, the method developed is easily transferable. Authors believe that it may help others firefighter services to apply it for a better knowledge of their specific risks.

Vulnerability zones for firefighters are defined as zones where both following factors exist: a complex incident area - like tunnels or bridges over roads/ railway lines - with a specific risk like buried networks. These areas require emergency teams with specific response capabilities.

By "vulnerabilities linked to technical networks" the authors mean areas where firefighters require the mobilization of external partners to secure the incident: gas, high voltage or steam operators (used in Paris area for building heating) send their emergency teams to cut off pipes or lines during the firefighters intervention. The presence of a dangerous technical network also implies to send a firefighters team with adequate capabilities. Currently the BSPP uses a decision system tools that sends the closest available team to the fire. The incorporation in this tool of the vulnerability map will propose specific additional capabilities to engage, which would lead to a gain of time. Of course, this knowledge does not enter in contradiction with the systematic field recognition of risks on incident but it is a new way to make operational decisions with GIS capacities. Risks link to aerial networks are already well managed because danger is visible. Authors are interested only in buried technical networks. *A priori* identification of vulnerable areas must be completed by a detailed risk assessment, for instance by asking technical operators for additional information (essential point) – for instance the depth of each network in these specific zones. Several researches on internet do not enable the authors to find any equivalent approach on specific risks mapping in anticipation for firefighters.

TYPE OF STUDIED INCIDENTS

Firefighters are careful in presence of gas, electricity or steam pipeline near of a fire for three reasons: firstly, the heat stimulus may damage the buried network and causes additional events such as explosions (gas), electric short-circuits (electric line melting) or violent steam leakages. Secondly, the use of water may cause electrocution risks around an electric buried line, or may cause a violent vaporization when cold water enters in contact with hot steam pipes. This second point concerns all fire incidents near a network. Indeed, the vulnerability map matches the buried network one. However, the first reason is not present every time: fire has to have high intensity and duration to damage buried networks. This configuration is possible when a container with combustible goods takes fire just near a non-aerial technical network – for instance buried networks or networks whose lines are following a bridge or a tunnel roof. The container could be a truck container or a freight car. This work aims at mapping all locations where such a configuration exists. The Table 1 summarizes the specific risks for firefighters in the vicinity of technical networks on a fire intervention.

Two kinds of fire incidents are studied: vehicle fire and freight car fire. This work does not make a difference between vehicles and hazardous truck - and thus between roads allowing or not the transport of hazardous goods (especially fuel) for a very practical reason: it is difficult to assess the traffic of illegal transport of such goods. The incidents studied here are exceptional events: statistically speaking, only one truck out of a billion per kilometer of tunnel is susceptible to take fire—and the only statistics found by the authors in France dates back to 1999 (AIPCR, 1999). This

Table 1. Specific risks for the firefighters linked to the vicinity of the networks to a fire in difficult intervention areas (tunnels) (BSPP 118.2, 2012)

Dangerous network	Specific risks for the firefighters on a fire incident
High voltage electricity lines	Electrocution risk linked to the use of water for firefighting. Nowadays, it is the chief of the intervention teams who asks for the RTE intervention. RTE is the French society managing the high voltage network. Only RTE has the ability to switch off one electricity line.
Electricity lines on railways	This specific risk is already managed in the Paris Fire Brigade procedures. It is thus out of scope for the present paper.
Steam pipeline	This network has at minimum 5 bar of pressure. The fire radiation may cause a quick pressure rise, with potential brutal steam release.
Gas pipeline	The fire radiation may cause a quick pressure rise in the gas pipeline. This phenomenon may produce an explosion or a structure deformation, which may generate a gas leak, leading generally to a pipe fire and sometimes an explosion. In the vicinity of a fire, such leak may start a fire called in France “C class fire”.
Fuel network	The fire radiation may cause a structure deformation, and may generate a leak and a pool fire. Even if fuel networks are dangerous ones for firefighters, they will not be included in this work since authors have no geographical data on them.

remark justifies adopting a deterministic approach and not a probabilistic one. All roads are considered for the study of vehicle fires. However, we speak only about goods traffic by rail and not people railway transport: the combustible volume has to be important enough to cause a high intensity fire for some time. The terrorism threat validates also the deterministic approach of the vulnerability maps.

DATA ANALYSIS

Two kinds of data are available in the BSPP database: data on difficult incident areas and data concerning the potential hazards. The first ones are roads and railway lines. Roads are mapped as lines in a GIS vector layer with attributes such as relative ground position, width and number of lanes. They have been mapped by Institut National de l’Information Géographique et Forestière (IGN). Railway data have been obtained by BSPP thanks to the French railway operator. Authors have been given the line vector geometry and position of railways, without indication of the width, neither the number of tracks per line. Information about the kind of traffic (freight, people) and the position of tunnels and bridges is also available. This means that roads crossings with one road bridge and road bridges over a railway have to be reconstructed on Geographical Information System (GIS). We want to map polygons (areas) of danger and not just crossing points between lines.

Concerning potential hazards, three networks (Figure 1) are available in the BSPP database with heterogeneous spatial extents: 1. the high voltage network, given by the French national operator of electricity transport, with the voltage, the name and the nature of the line - aerial or buried - (980 km). 2. the gas network, given by the national French operator of gas transport, with only the line positions (580 km). 3. the steam network (line geometry), given by the Parisian company for urban heating (390 km). These three networks may cause specific risks in the vicinity of a fire. They are all sensitive to heat, and electricity and steam are sensitive to the water used by the firefighters. Data about steam and high voltage buried networks have the same problem: the depth has not been communicated. Even if minimal depth standards exist for buried technical networks (VisioRESO, 2015), no explicit standards on the depth of networks using existing infrastructures like tunnels or bridges have been found. This is the first limit of the methodology: without knowing this point, it is difficult to assess if the risk during an intervention is real or theoretical. For instance, some high voltage lines in Paris use old gallery dozens of meter underground: the crossing in 2D of such line with a difficult intervention area is only a mark of potential vulnerability point. However, this limit underpins the interest of the analysis: By using the map of potential vulnerable area, firefighters are able to concentrate on a limited set of areas where additional information could greatly improve their own safety.

Figure 1. Extensions of the studied networks

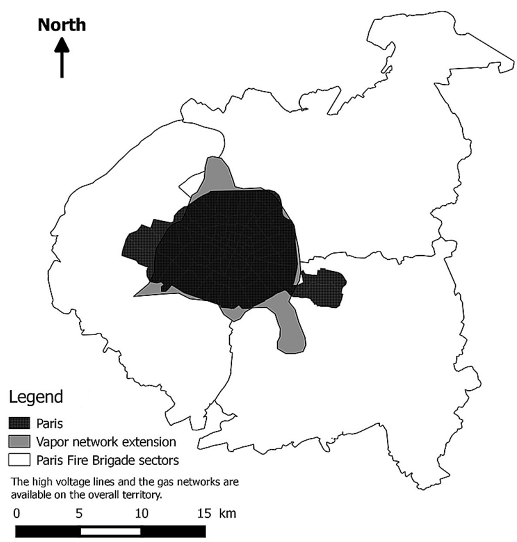
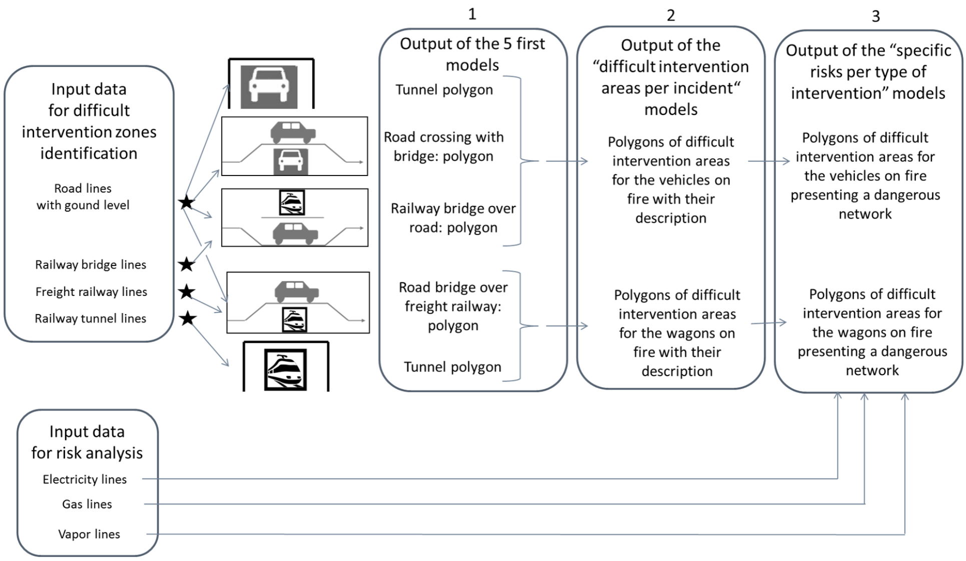


Figure 2. Flowchart of the different models: input data and expected output



IDENTIFICATION OF THE DIFFICULT INTERVENTION AREAS

Identification of all the difficult intervention areas has been automated in a toolbox under the software ArcGIS. The principles are briefly presented here. The Figure 2 illustrates the flowchart between inputs data and expected outputs of each toolbox's models. Two polygons layers are produced: one for the interventions on vehicles on fire, another for the interventions on freight cars on fire. Polygons of difficult intervention areas are distinguished according to whether they cross or not a buried network. Their extent needs to be as accurate as possible to avoid missing a technical network.

Method Hypothesis

1. Only a road can cross over a rail freight way, no rail transport way crosses over a freight way. This hypothesis comes from the fact that rail ground level is unknown in the database. It is impossible to distinguish which rail is under or over the other rail.
2. At the opposite, a road and a railway (whatever freight or public transport) may cross over a road.

3. The areas of interest are bridges and tunnels for the following reason: a buried network crosses over a road or a rail underground if there is no bridge or tunnel, but may cross over a road or a rail through tunnel or bridge if it exists. The following methodology will then identify all bridges and tunnels concerning roads, and then concerning rail freight.

Difficult Intervention Areas for Vehicles on Fire

1. **Tunnels**: underground roads are known, with the width in attribute and line geometry. Even if each underground road cannot be called a "tunnel", the authors assume that a road goes underground to pass under a road or a railway and is therefore a tunnel. The authors create a buffer around underground road lines, whose length is road width for simulating tunnel polygons.
2. **Railway Bridges**: the authors have them in a dedicated layer. They select those that cross a road line, which level is at the ground or above. The railway bridge polygons are buffers around road lines. Their widths are road widths and their lengths are rail widths. The rail width is assumed because railway width is unknown (see below the discussion on data quality).
3. **Road Crossings with Bridge**: the authors have to map them. The Figure 3 shows the model workflow: intersection of ground roads (GL = 0) and upper linear roads (underground roads are tunnels), selection of these lines, buffering of them and then cutting for having the intersection polygons. However, this simple method overestimates the number of crossing for two kinds of situations. First, if one of the roads is constituted of two numerical entities, there are two selections of road crossings and so two danger polygons for one real zone of interest (Figure 4). Second if a ground road "A" changes itself in an upper road "B" (for going over another road "C" for instance), then the intersection between entities A and B is selected as a road crossing with bridge, which is false (Figure 5). These wrong polygons have a very small surface. This characteristic is used further to discredit these wrong polygons.

Figure 3. Steps for identifying crossing roads with a bridge

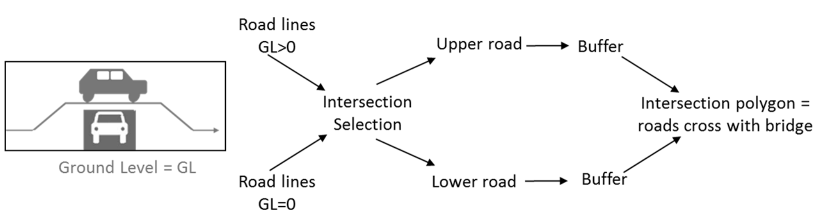


Figure 4. Illustration of the overestimated number of roads crossing

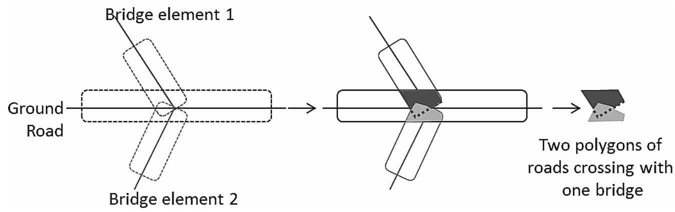
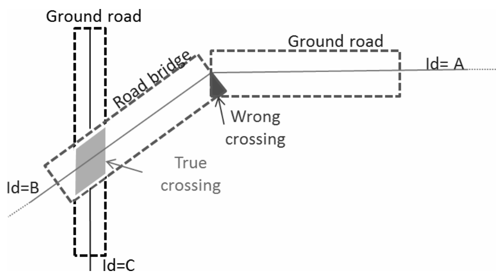


Figure 5. Illustration of a road crossing identification error



Discussion on Roads Data Quality for Applying the 3rd Model "Road Crossings with Bridge"

The application of the 3rd model on the BSPP territory has been difficult because of the non-exhaustive knowledge of road widths. The following paragraph presents the treatment of the available data. The quality of the data is an additional limit of this approach.

Authors have used the road data from the IGN BDTOPO database Version 2.1. This database is produced by the national Institute for the geographical data "IGN", with a metric precision (IGN, 2016). It includes in the road data the pedestrian ways like stairs, paths or bicycle paths. Those ways are not causes of fire incidents because no vehicles use them. However, they have to be taken into account when there is a pedestrian bridge over a road, because this bridge may hide a network in its infrastructure. The 3rd model proposes in its interface to exclude pedestrian ways for which ground level is equal to zero, but to keep the pedestrian ways that are bridges. It is important to notice that pedestrian ways have no width in this database, and it is a little limit of the approach. Indeed, pedestrian bridges are only less than 1% of the geographical entities of the IGN BDTOPO database Version 2.1.

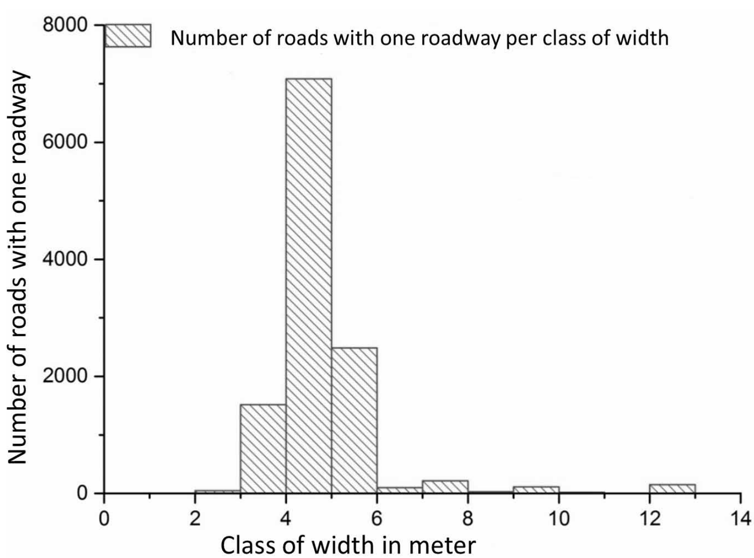
Table 2. Roads nature percentage of the roads entities without width

Nature	Percentage	Official description
Roads with one roadway	55%	This class includes all the asphalted roads that have no physical obstacle separating the two flow directions.
Gravel roads	30%	These are non-asphalted roads.
Dirt roads.	15%	Dirt roads are still available for a vehicle circulation. There are situated in non-urban areas.

The Table 2 shows the percentage of roads natures among the 15 500 entities (3% of the total numbers of entities) that have no width in the IGN BDTOPO database Version 2.1. Major roads like highways have all their width description.

Given the previous nature repartition, the authors will attribute the average width of roads with one roadway for completing the empty width description. The Figure 6 shows the statistical repartition of the width of roads with one roadway that are in the IGN BDTOPO v2.1. The average width is 4.5 m with a standard deviation of 1.7 m. The standard width attributed to roads with no width description will be 4.5 m, even if there is a relative large standard deviation. The non-exhaustivity knowledge of the roads width (data quality) is a limit of this geographical approach because it has a big influence on the area of the road crossings with bridge, and could cause to miss a dangerous network crossing due to a computed area smaller than the actual one.

Figure 6. Number of roads with one roadway per class of width

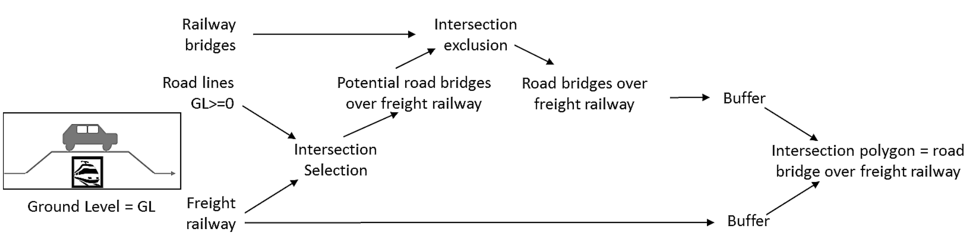


In order to retrieve only the roads intersection with a crossing and not the partial covering of roads of different ground level positions, the model uses the lines geometry intersection for the first selection, and not the buffer intersection first. This method enables also to gain time as it is a longer operation to buffer thousands of line roads and then to intersect them, rather than to cross lines and then to buffer only the selected lines. Once the crossing roads in line forms have been identified, the model rebuilds the exact area of the crossings by a geographical intersection of the road buffers.

Difficult Intervention Areas for Rail Freight Fire

1. **Rail Freight's Tunnels**: The authors know their position but not the number of ways per tunnel or the width. This is one of the toolbox's limit: when crossing rail tunnel polygons with burried technical networks, the width hypothesise has a big influence. European norms fixed the width of one railway at 3,15 meters (IURRT, 2016). The tunnel is supposed to have at least two railways (strong hypothesis for over estimating the tunnel area). The tunnel width is fixed by assumption to 6,3 meters.
2. **Road Bridges Over a Rail Freight Railway**: The authors do not know them, nor the railways ground level. The Figure 7 shows the model workflow: first, roads at the ground level and above that cross a rail freight railway are selected. Among them, those that do not cross a railway bridge are finally selected. The grade crossings are not eliminated at this step but further on when the spatial jointure with the networks is made. There is no practical reason for a buried network to cross a railway at a grade crossing rather than at any other point of the rail (there is a low probability that a buried network cross a railway at a grade crossing).

Figure 7. Methodology for identifying road bridge over rail freight way

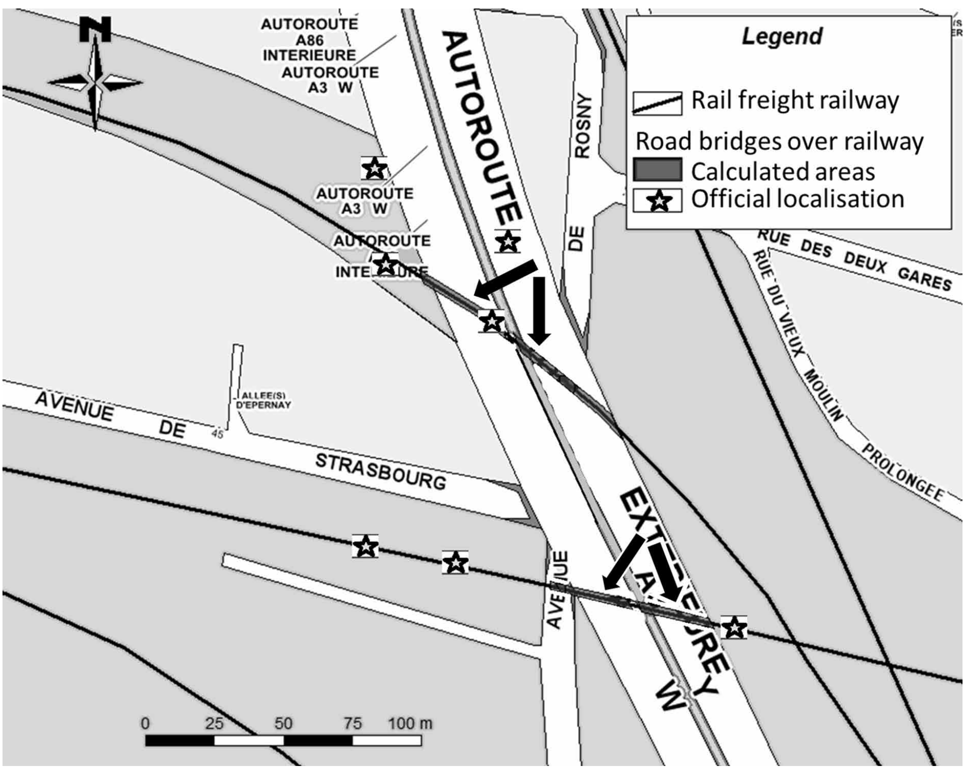


Discussion on Data Quality for Applying the Second Model “Road bridges Over a Rail Freight Railway”

There is a layer of the national railway operator (SNCF), which indicates the localisation of all the “road bridges over a rail freight railway”, with punctual entities. However, it is difficult to identify the closest road which is potentially the road bridge. Indeed, there is an important distance between the localisation of the punctual entities on the railway, and the effective crossing of the road lines that authors have in their database. This difference is shown in the Figure 8. Another method is proposed here, using only the roads lines from the IGN BDTOPO v2.1, the railways lines and the railway bridges lines, for which localisations are coherent.

The method applied here identifies more road bridges over a rail freight railway (1140 areas) than the official layer from the national railway operator (276 points), and a difference of localisation. In order to explain it, the authors have analyzed the

Figure 8. Illustration of the difference between the localisation of official points of road bridges over a rail freight railway and calculated areas from the DEMOCRITE toolbox



distance between areas calculated by the second model "Road bridges over a rail freight railway" and SNCF points. Only 62 ponctuels are inside the calculated areas, 122 points are distant of less than 5 meters of one calculated area, 140 are less than10 meters from the areas, and 171 are less than 20 meters from the calculated areas. A potential projection problem can only explain few of these localisation differences. Another explanation could be the assumption of the road widths, and so an error on the extent of the areas. However, this does not explain the fact that 40% of the points are further than 20 meters away from the computed areas. The map on the Figure 8 illustrates this difference between SNCF points and calculated areas. One of the point is far of around 50 meters of the concerned road. All the points are on the freight railway lines, but are not superimposed on the road lines of IGN.

The difference between the number of SNCF bridge points and the number of calculated areas is explained by looking at the limits of the model. If the road bridge is described by two numerical entities, the model identifies two bridges even if there is only one in this area. Moreover, the offical layer with points for road bridges may sometimes group several roads per point. For instance, a two directional road may sometimes account for two numerical road entities in the road shapefile, but only for one bridge for the SNCF layer.

Limits of the Models

There are two main limits for the previous models. First, they are sensitive to the width hypothesis on the rail network: difficult intervention areas are probably under estimated in term of space. Readers can see it on the Figure 8 above; the model output calculates the railway width for one way. However, it is under estimated close to rail junction areas. An over-estimated width would have been a problem too, because buried networks density is high in urban area: every bridge is surrounded in a close or far manner by a network. The spatial jointure between under-estimated area per railway and the network map will at least recognize zones where the network is located near the middle of the double railway (i.e. the highest risk area where a network could be damaged by the fire intensity).

The excessive numbers of road difficult intervention areas is another point. The wrong identification of road bridges is not really a limit: the spatial jointure with network maps eliminates all areas where no network is found. Indeed, wrong polygons have a small surface and statistically they do not cross a network. The surplus of difficult intervention areas caused by the numerical construction of road entities is not a real limit either. The important thing is to register areas that cross a network. It is better to have a false area of interest than to miss a dangerous area. A post treatment can easily merge road difficult intervention areas that touch each other. However, as it is a post-treatment, the number of difficult intervention areas has to be taken with precautions in the following paragraph. They are order magnitude and are always overestimated numbers.

CROSSINGS BETWEEN DIFFICULT INTERVENTION AREAS AND NETWORK MAPS: ADDITIONAL VALUES OF THE RESULTS

Once the five difficult intervention areas are mapped, a spatial jointure enables to attribute the number and the characteristics of all the networks that cross each area. The attribute table of the results obtained is illustrated in the Table 3.

As vulnerability maps are sensitive, no map of results is presented. However, statistics are not sensitive. The BSPP territory is an 850 km^2 surface with a high urban center (Paris). For the vehicle fire incidents, 7% of the difficult intervention zones cross a buried network. Among them, around 500 have high voltage electricity lines, 150 gas and 100 a steam network (Table 2). Fifty of these difficult intervention areas have two networks. For the rail freight burning, the selection is less strict but in term of number, risk zones are less numerous: less than 10% of the difficult intervention zones cross a buried network. Among them, only around 60 have high voltage electricity lines, 20 a gas network and another 20 a steam network. Ten of these difficult intervention areas have two networks. That is not so much for a wide and urban territory.

The frequency of difficult intervention area nature per network and per type of incident is also interesting (Table 2). The high roads density explains that 85% of the difficult intervention areas concerns vehicle fire. Road crossing with bridges are the most frequent difficult intervention area for vehicle fire with networks. However, the propensity to have a specific risk is higher for the road tunnels and railway bridges on roads than for the road bridges, as seen in Table 3. The railway situation is similar: 95% of the rail freight difficult intervention areas are road bridges over freight railways. The probability of having an electricity risk on a difficult

Table 3. Attribute table obtained for each specific risk zone

Origin	Danger	Description	Electricity	Gas	Steam
Road tunnel, road crossing with a bridge, rail bridge over a road	Vehicles on fire	Section name of the buried network	Number of networks crossing the difficult intervention area	Number of networks crossing the difficult intervention area	Number of networks crossing the difficult intervention area
Rail freight tunnel, road bridge over a rail freight	Freight cars on fire				

intervention zone is identic whatever its nature. For the gas and steam network, global numbers are not enough numerous for concluding.

These numbers from Table 4 and Table 5 help to understand that potential risks for firefighters linked to a buried network are indeed a non-homogeneous risk on a territory. The relatively high number of road difficult intervention areas with specific risks can discourage a one by one request of depth information to each technical operator. However, the rail freight difficult intervention zones with potential specific risks for firefighters is not so numerous: request of depth information on each zone is conceivable. This step will enable to distinguish zones without risks linked to a technical network (because depth is too high for damaging the network by fire) and zones with risks. This methodology enables it and proves by this way its interest for specific risks reduction by vulnerability mapping.

Table 4. Statistics on difficult intervention area nature as a function of specific risks

Road difficult intervention areas with specific risks	**Electricity**	**Gas**	**Steam**
Approximate number	500	150	100
Tunnel	20%	30%	30%
Railway bridge on roads	10%	20%	10%
Road crossing with bridge	70%	70%	60%
Rail freight difficult intervention areas with specific risks	**Electricity**	**Gas**	**Steam**
Approximate number	60	20	20
Tunnel	4%	6%	20%
Road bridge over rail freight way	96%	94%	80%

Table 5. Specific risk statistics as a function of difficult intervention area nature

Road difficult intervention areas propensity to have a specific risk	**Electricity**	**Gas**	**Steam**
Tunnel	10%	1%	4%
Railway bridge on roads	10%	8%	3%
Road crossing with bridge	4%	1%	Less than 1%
Rail freight difficult intervention areas propensity to have a specific risk	**Electricity**	**Gas**	**Steam**
Tunnel	7%	3%	13% (few initial zones!)
Road bridge over rail freight way	6%	2%	2%

CONCLUSION

This work takes part in the global numeric evolution of the Paris Fire Brigade (BSPP). This one aims at keeping improving the emergency safety cover quality thanks to the new technology capacities like GIS in vehicles or connected equipment. This method is easily transferable: roads, railways and dangerous networks are often available in 2D lines. Every brigade that has decision system tools based on GIS may use it for engaging accurate specific capabilities immediately after an emergency call.

The interest of the BSPP for the map results proves the practical interest of this work. Thanks to this methodology, they have obtained two vulnerability maps of potential specific risks for two types of incidents: vehicles on fire and freight cars on fire. Localization of these ones helps a better understanding of the intervention territory. The numerical feature of the maps of risks is interesting as it could be implemented in the decision help tool dedicated to the mobilization of intervention team. Moreover, this methodology legitimates the requests of information on network depth in a very limited number of risk areas to technical operators. Gathering data on these vulnerable zones is the next step of our work. In conclusion, this methodology has numerous practical advantages that participate to reduce intervention risks linked to buried networks for the firefighters.

Perspectives of this Work

In 2001 in Baltimore, a freight train derailed in a tunnel. Polypropylene caught fire and ignited adjacent cars. The firefighters took the decision not to immediately fight the fire because explosion risk was absent and because interventions conditions were difficult. However, the fire intensity caused a break in a 40-inch water directly above the fire hampered emergency response efforts. Million gallons of water flooded part of Baltimore. Beyond the adverse effects on railroad traffic, the fire and the water damaged power cables and left 1,200 buildings without electricity. Major fiber-optic lines for regional and national data traffic have also been damaged (NTSB, 2001; FRA, 2005). This event shows that firefighter's decisions on a fire in vulnerable areas may have important societal impacts.

Technical networks are lifeline systems and the disruption of their services may have important consequences on the society, depending on loss duration. Moreover, it may spread the initial failure to others technical networks, propagating the initial zones of impact through cascading effects. Cutting off one network line rarely causes a cascading effect as networks are designed in order to absorb common failures. However, the simultaneous disruption of several lines – which means simultaneous fire in vulnerable areas or a large extent fire – should be a warning signal on a potential cascading effect. As we speak about very low probability of accidental transport fires, such a combination of scenarios would be likely the result of malicious intentions.

Indeed, the vulnerability mapping in anticipation has two complementary goals:

1. The systematic identification of vulnerable areas justifies to external institutions the need for more technical details (network depth, road or rail width, real risk facing a fire) on each identified zone in order to improve the safety of firefighters in case of a fire.
2. The use of these maps in a decision support system available to firefighters could enable the building of an early warning system. If several fires occur in such areas, there is a high risk of cascading effect with large impacts on the society. Additional work has been done in the DEMOCRITE project to model cascading effects for the civil safety institutions.

There are many potential internal and external causes to a system failure that some authors have classified (Brilhac, 2009; Dassens, 2008; Rey, 2015). The thermal aggression caused by a fire is only one of them. Behind the different existing causes, we must keep in mind that cascading effects are caused by a first failure of one of the infrastructure. The work presented in this paper is part of the DEMOCRITE project for the civil safety institutions. As we speak about fast crisis, we are interested only in cascading effects between technical networks. There are many others dimensions for cascading effects, as much as the diversity of dependency links between systems (see (Rinaldi, 2001) for a classical categorization of these dependency links). However, only technical failure may spread in few hours or few days through different networks, with important consequences in the all-day life. Buried pipelines or lines destructions by fire are not limited to the dangerous networks like electricity, gas, fuel or vapor, but have to be extended to water networks and telecommunication lines (optical fibers or copper lines). Several tools exist in the literature for the modeling of cascading effects between technical networks. The paper (Grangeat, 2016) proposes a selection of them, that are considered as “off the shelf” tools potentially useful for civil safety institutions. In France, firefighters are the operational part of the emergency response when victims or major hazards occur in the society. The appearance of a major cascading effect lasting several hours or days would have major impacts on the society, but it does not imply systematically victims, fire or pollution. It would be more a question of public security and safety, or assuring the contingency of institutions and business. This means that firefighters would be the eyes and the hands but not the managers of such crisis. However, the interruption of some services may complicate the emergency channel from the victims to the firefighters. Victims may have difficulties to call firefighters if telecommunication falls; electricity blackout may complicate the electric doors opening for instance;

a loss of pressure in the water network would force firefighters to intervene on fire incidents with special vehicles water tank, that are not available in an homogenous manner in fire stations. The emergency efficiency may indeed be affected itself by the cascading effects. The better the cascading effects are known, the better the anticipation and the effective engagement of safety resources will be. For that reason, the civil safety institutions in France have promoted projects like DEMOCRITE, around the study of cascading effects for the crisis management.

ACKNOWLEDGMENT

The authors want to thank the DEMOCRITE French project (ANR-13-SECU-0007) that enables research on this problem. The work presented in this paper has been also partially funded by the CIPRNet and the PREDICT European projects. CIPRNet and PREDICT have received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450 and no 607697. The European Commission's support is gratefully acknowledged. The views expressed in this document are purely those of the writer and may not in any circumstances be regarded as stating an official position of the European Commission.

REFERENCES

AIPCR. Association mondiale de la route (1999). Rapport 05.05.B, Chapitre 2, risque incendie et incendies de dimensionnement. Web. Retrieved from http://tunnels.piarc.org/tunnels/ressources/1/54,1999-05.05.B-Chap-2.pdf

Brigade des Sapeurs Pompiers de Paris. (2012). *BSP 118 Tome 2. Règles d'engagement spécifiques par type d'intervention.*

Brilhac, J.-F., & Thibaut, O. (2009). Analyse des risques sur un territoire – Ebauche d'une nouvelle méthode globale. Techniques de l'Ingénieur. Univers: Génie Industriel, Pack: Management industriel, Base: Théorie et management des systèmes complexes.

Dassens, A., & Launay, R. (2008). Etude systémique de l'analyse de risques – Présentation d'une approche globale. *Techniques de l'Ingénieur.* Univers: Génie Industriel, Pack: Management industriel, Base: Théorie et management des systèmes complexes.

Federal Railroad Administration. Washington, D.C. (2011). Report To Congress: Baltimore's Railroad Network, Challenges and Alternatives. Retrieved from http://www.fra.dot.gov/eLib/details/L04275

Grangeat, A. (2015). *Cartes statiques des risques métiers liés à la présence de réseaux techniques*. Livrable DEMOCRITE.

Grangeat, A. (2015). *Description des toolboxs ArcGIS permettant de réaliser les cartes statiques des risques métiers liés à la présence de réseaux techniques*. Livrable DEMOCRITE.

Grangeat, A., Bony, A., Lapebie, E., Eid, M., & Dusserre, G. (2016, October). The Challenge of Critical Infrastructure Dependency Modelling and Simulation for Emergency Management and Decision Making by the Civil Security Authorities. In E. Rome et al. (Eds.), *CRITIS 2015, LNCS* (Vol. 9578, pp. 255–258).

Institut national de l'information géographique et forestière - IGN (2016). BD TOPO. Retrieved from http://professionnels.ign.fr/

International Union for Road-Rail combined Transport (2016). Railway Infrastructure. Retrieved from http://www.uirr.com/en/road-rail-ct/framework-conditions/railway-infrastructure.html

Lapebie, E. (2015). Concepts, Systèmes et Outils pour la Sécurité Globale (CSOSG) 2013: Projet DEMOCRITE. Emmanuel LAPEBIE, CEA. *Agence Nationale de la Recherche*. Retrieved from http://www.agencenationalerecherche.fr/?Projet=ANR13SECU0007

National Transportation Safety Board Washington. D.C. 20594. (2001). Railroad Accident Brief NTSB/RAB-04/08.

Rey, B. (2015). Résilience systémique d'un Territoire composé d'Activités Essentielles suite à une perturbation majeure - Approches systémique et spatiale [Thèse de doctorat]. École Nationale Supérieure des Mines de Saint-Étienne.

Rinaldi, S., Peerenboom, J., & Kelly, T. (2001). Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 21(6), 11-25.

VISIORESO. (2015). Profondeur des réseaux. Retrieved from http://www.visioreso.fr/la-reglementation/#norme_S70-003

This research was previously published in the International Journal of Information Systems for Crisis Response and Management (IJISCRAM), 8(3); edited by Murray E. Jennex and Víctor Amadeo Bañuls Silvera; pages 51-63, copyright year 2016 by IGI Publishing (an imprint of IGI Global).

Chapter 2
REDAlert+:
Medical/Fire Emergency and Warning System using Android Devices

Arjun Shakdher
Jaypee Institute of Information Technology, India

Kavita Pandey
Jaypee Institute of Information Technology, India

ABSTRACT

Each year, thousands of people in developing countries die due to delayed medical response. A common complaint is that emergency vehicles respond late and when they reach the hospital, precious time is lost in understanding the patient trauma before the doctors can get to work. A large number of deaths can be prevented if medical services can be provided to the victims in time, which can happen when the emergency wing of a hospital has advance information about the trauma before the patient reaches the hospital. Most hospitals lack communication infrastructure that allows them to coordinate with emergency vehicles bringing patients to hospital. In developed countries, Vehicular Ad-hoc Networks (VANETs) are prevalent. These networks use vehicles as mobile nodes to create a small-interconnected network on the road. A mobile application based on the principle of VANETs in combination with wireless communication and database management has been devised, that when integrated with emergency vehicles and hospitals, provides a seamless medical response system at times of an emergency.

DOI: 10.4018/978-1-7998-2535-7.ch002

INTRODUCTION

Administering prompt medical attention to a trauma victim is the goal of every emergency care responder. However, despite the best of intentions, a large percentage of patients lose out on the benefits of timely medical care. One of the main reasons for this is attributed to delayed medical treatment, prompted by a delay in reaching critical care facilities. Lack of advance preparation at the emergency center in handling for the trauma further accentuates the delay.

While many mobile solutions have been created to address this issue, they all suffer from some infirmity or the other that has precluded their widespread use. This paper explains the functioning of REDAlert+, a mobile application solution whose objective is to reduce delays in receiving medical care, by analyzing the shortcomings of some existing applications and creating a solution that addresses these issues.

Consider a typical scenario where a road accident has taken place. The user places an emergency call to a hospital, which may or may not be nearest or equipped to handle the emergency, to request for an ambulance. After having made the request the user keeps on waiting, having no means of knowing when and where the ambulance is likely to arrive. With no real time data at hand, he is also not in a position to guide the ambulance to the accident spot. The ambulance driver on the other hand, with no outside help and lack of terrain knowledge, ends up losing precious time to arrive at the accident site. Furthermore, the lack of a common communication platform between the user and the hospital hinders making advance preparations to receive the patient.

The authors conducted a detailed analysis of the steps required to ensure speed and ease of use both by the user in distress as well as the other stakeholders in the treatment cycle i.e. the driver of the ambulance and the medical supervisors receiving the victim in the emergency ward. Using the application developed, the user can quickly locate the nearest hospital, inform it about the emergency and ensure that an ambulance will be deployed to the user's location. Concurrently the user can track the ambulance on a map after making the request. This application not only allows the user to estimate the likely arrival time of the ambulance but also provides the ability to guide the ambulance to the accident spot using the shortest possible route using a map. In the meantime, the user's medical profile is forwarded to the hospital en route so the hospital staff is better prepared to receive the patient. This application positively impacts the life of millions of people that face medical emergencies and suffer due to delayed medical response.

The remainder of this paper is organized as follows. Section II presents the relevant related work. Section III describes the system architecture, the functioning, the technologies used. Section IV presents the testing results under various emergency scenarios. Section V explains the findings and discusses the future work. Section VI concludes the paper.

RELATED WORK

Various mobile applications and IT solutions dealing with coordination, communication and tracking during emergencies have been developed in the last lustrum. The pervasiveness of mobile devices has obviated the need for using costly equipment and the fast expanding universe of mobile apps has helped ease creation of solutions that address specific issues. However only a few of these solutions have been successful in streamlining communication in times of emergency.

Chang et al. (2012) proposed to store critical information like observations of earthquake, debris flow, abnormal weather, river pan abuse, abnormal weather, etc. in an online web emergency database system, thereby developing an Android-based emergency SMS broadcasting application where people of the region could receive real-time messages in case of any natural disasters. They identified a design, which included requirement specification of three functional subsystems, namely, web application subsystem (WAS), an emergency database subsystem (EDS) and an embedded mobile application subsystem (EMAS).

Hariprasath et al. (2013) proposed an emergency alerts system where they developed certain efficient mathematical techniques to avoid network congestion while broadcasting SMS alerts. They also calculated the minimum time required for the delivery of those bulk messages using GSM network in smartphones.

Applications like IPROB (Kumar & Rajkumar, 2014) have also been developed that tackle the issue of safety. This application, specially designed for women makes use of the tri-axial accelerometer in the smartphone as a result of which the victim simply needs to shake the phone to send a location aware emergency SMS alert. This application was made for android-based smartphones with requirements including a GPS tracking service, a network provider and a SMS Manager Module.

The downside of these solutions is that they use GSM connectivity and network provider based SMS alerts, which makes uninterrupted network connectivity imperative to receive real time alerts. Such connectivity may not always be available during emergencies.

There have also been numerous discussions on Technology and Innovation that addressed the issues relating to medical emergencies. West and Valentini (2013) have stated how there has been a transformation in public safety and disaster relief with the help of mobile devices in recent years. They have presented example of Japan's EEW (earthquake early warning systems), where Mobile Ad-hoc Networks (MANETs) work efficiently in the absence of Wi-Fi or cellular networks. They also talked about scenarios where citizens and first responders have been provided with the necessary tools and services, which have significantly reduced the chances of loss of lives.

Monares et al. (2011) have highlighted the need of a proper communication system for the fire fighters of Latin America. They proposed a solution to overcome any communication problem by developing a collaborative low cost mobile application called MobileMap. The application uses an ad-hoc communication infrastructure and proves to be useful for the purpose of coordination between the fire fighters and supporting decisions in emergencies. The advantage of this solution is that the application can switch between Wi/Fi/GSM for communication depending upon the availability. However, the application has a complex and a cluttered user interface that renders it difficult to operate during an emergency.

Baykal (2013) has discussed the basic application of ad-hoc networking for Android devices where image and audio data can be transferred once the connection gets established through peer-to-peer protocol. He has also stated that establishment of an ad-hoc network using phone's Wi-Fi can solve many problems that arise due to temporary disconnections to network access points or 3G networks.

Koshmak (2011) proposed an android-based monitoring and alarm system for patients suffering from chronic disease. The system provided remote access to monitor various physiological health parameters of patients. It becomes very convenient for the professionals to create a medical review when data collection related to oxygen saturation and heart rate is performed and transferred to the responsible authorities for subsequent evaluation of the health of the patient. This system involved connection between a pulse oxymeter (worn by the patient) and an android phone used by the medical officer. It has, by far, been an excellent application dealing with data processing to the algorithms of anomaly detection and activity correlations. If the risk data exceeds some threshold value, it sends alert to the corresponding medical officer to take some immediate action. However, the application depends a lot on sensors worn by patient and the user interface of this highly functional application is found to be extremely sophisticated and impractical. Kim et al. (2012) proposed a performance evaluation to determine which cellular network is most suitable for Vehicular Ad-hoc Networks (VANETs) further explaining Vehicle-to-Infrastructure communication and Vehicle-to-Vehicle communication. Drive testing has been used to evaluate the performance of several cellular networks. They have also stated that many organizations and groups working to achieve Intelligent Transport System (ITS) have been proceeding with certain protocols like WAVE for standardizing and specializing VANETs. In case of cellular networks, the results of delay variations at different driving speeds show that 4G LTE network takes up less delay when compared to 3G HSUPA (High Speed Uplink Packet Access) networks being more efficient to adopt for VANETs.

Table 1. Related work

Author Names Reference	Name of the Article	Connectivity Requirements	Technologies and Services Ssed	Services Offered	Limitations
Chang et al. (2012)	Android based emergency broadcasting system for natural hazards	Cellular Networks	SQL Server 2008 Web Database, SMS broadcasting	Emergency SMS boradcasting of natural hazards	Dependant on availability of a network provider to broadcast SMS alerts
Kumar et al. (2014)	IPROB- emergency application for women	Cellular Networks	GPS, SMS Manager Module, tri-axial accelerometer sensors	Send location aware emegency alerts by shaking the phone	
Hariprasath et al. (2013)	EAS using android	Cellular Networks like GSM and CDMA	SMS services for sending alerts	Congestion management algorithms for emergency SMS broadcasts	
Monares et al. (2011)	Mobile Computing in Urban Emergency systems	Wi-Fi/GSM/ MANETs	Maps, GPS, XML database	Facilitate coordination and communication for fire fighters	Complex and cluttered user interface making navigation difficult during emergencies
Koshmak (2011)	Android based monitoring and alarm system for patients with chronic obtrusive diseases	Local connectivity to pulse oxymeter (via Bluetooth)	Smartphone's accelerometer, Fingertip Oxymeter technology	Health monitoring of the patient and triggers to send alerts to doctors	

Shaukat (2014) shows that peer-to-peer communication can be used in an effective manner by application of Wi-Fi Direct protocol for networking in android devices. He explains a part of the implementation of the wireless peer-to-peer network model using Wi-Fi Direct. Santos et al. (2013) have presented a paper on handling emergencies that is efficient but lacks data load balancing and the use of cloud technology. Table 1 presents an overview of the related work.

The work done while commendable, suffers from limitation on account of either the communication technology used, the platform used for deployment or the complex user interface. It was therefore felt that a solution carved on Wi-Fi/GSM technologies for the ubiquitous Android, coupled with an intuitive user interface would be most apt. This paper presents REDAlert+, an android application developed for handling emergencies that is adaptive enough to work with Wi-Fi and mobile data networks for sending emergency alerts. For cell phones that do not have GPS, the user's location can be alerted using the Location Area Code (LAC). With the unique collaboration of such an application with the VANETs technology that broadcasts warnings to vehicles in close vicinity, the authors of this paper have also addressed traffic management and road safety.

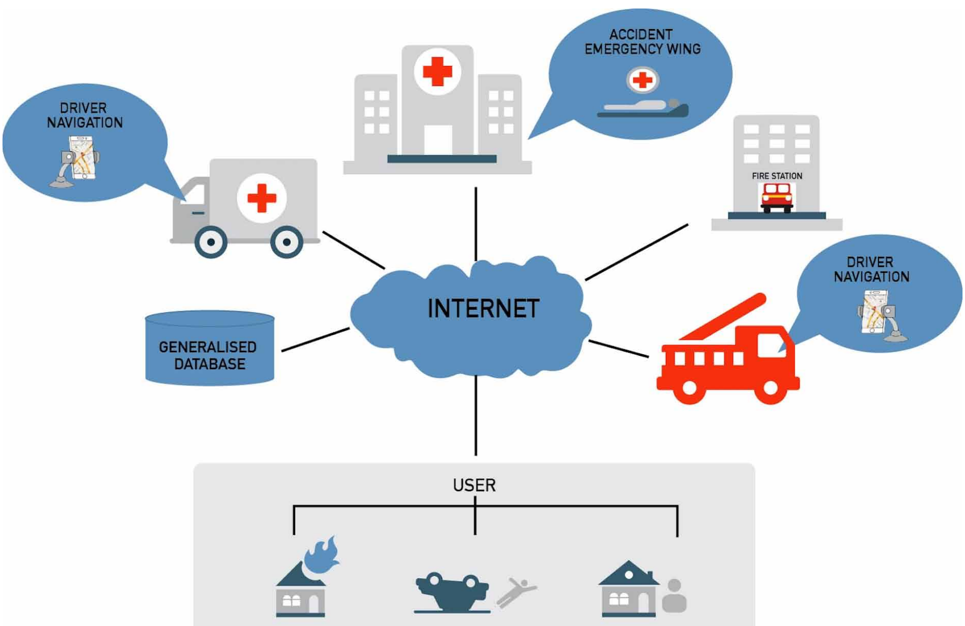
PROPOSED SOLUTION: REDAlert+

The absence of a proper system for managing medical and fire emergencies paves a way for a proficient solution that is quick and responsive. This application enables the user to deal with an emergency in an organized and efficient manner.

This section shows the overall system architecture, the modular architecture of the application and the used technologies. The system architecture is presented in figure 1. The main entities are the

- REDAlert+ App Users
- Hospitals and Fire Stations
- Ambulances
- Centralized Database

Figure 1. System Architecture of REDAlert+



The users of the application connected to the Internet through Wi-Fi or GSM/CDMA send information across all the entities. The connection is encrypted with TKIP that uses the RC4 stream cipher along with a 128-bit per-packet key. The communication between the user, the hospital/fire station, and the ambulance is done using Python client-server scripting. All the relevant information including the Medical IDs, user and ambulance locations, and the record of all the hospitals and fire stations are stored and centrally managed in the online central SQL database. The exchange of information is facilitated using PHP scripting and the data sent and received is parsed with JSON.

The REDAlert+ android application has been developed in four standalone application versions.

- **User Application – REDAlert+:** This is designed for the user who will access this application in times of distress. Through heavy code optimization, this application has achieved a very small footprint of approximately12MB that would make it affordable to a wide spectrum of users. (Figure 2)

Figure 2. User Application REDAlert+

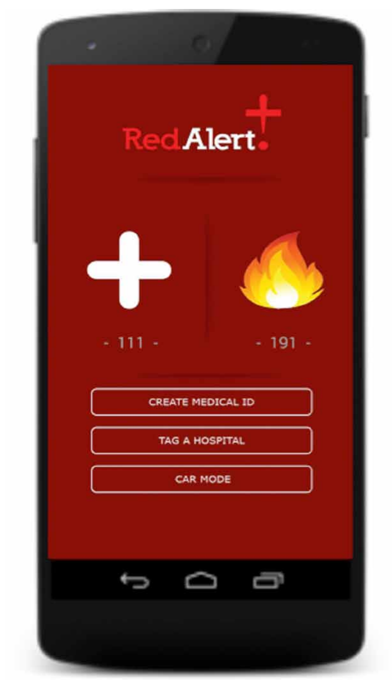


Figure 3. Hospital App

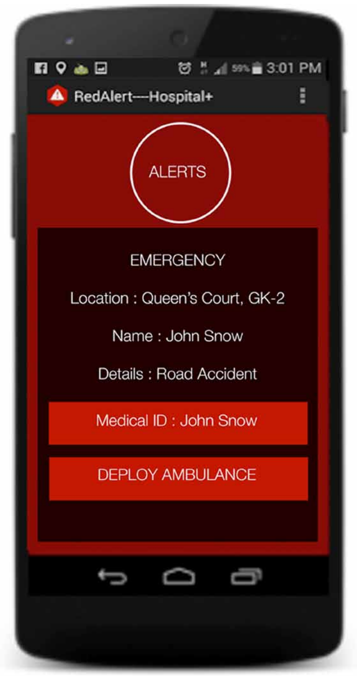
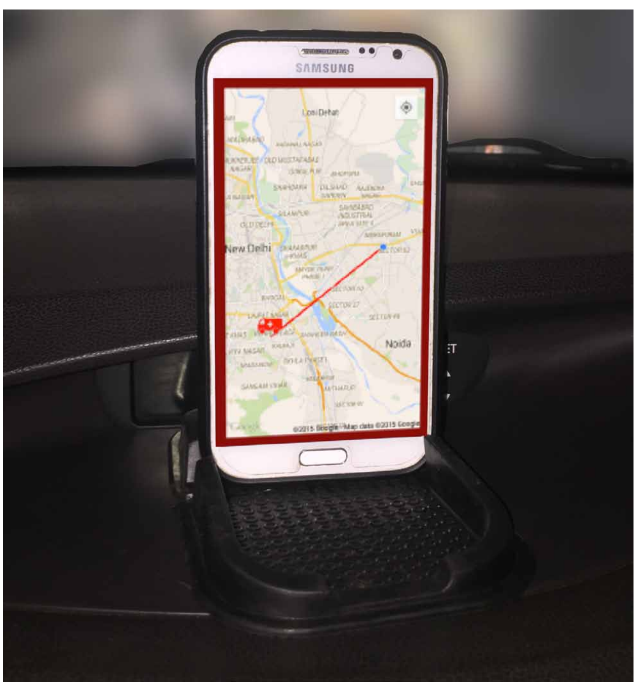


Figure 4. Ambulance App



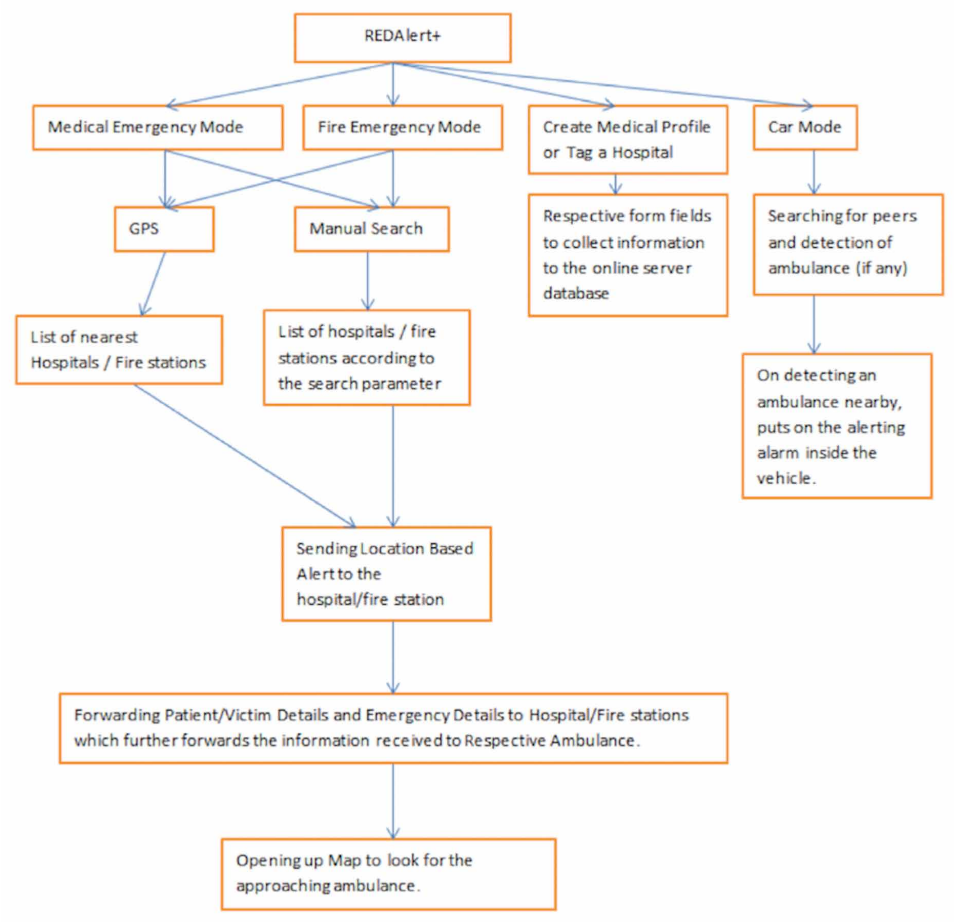
- **Hospital/Fire Station Application:** This application is used by the A&E (Accident and Emergency) department of the hospitals and fire stations to receive the emergency alerts. (Figure 3)
- **Ambulance Application:** This application is used by the ambulance driver to spot the user in distress and navigate to his location accurately and timely. (Figure 4)
- **Car Mode:** This application is designed for receiving alerts and warnings while the user is driving the vehicle so the user can react properly if an ambulance is in vicinity.

The overall representation of the functional architecture of all the modules related to this android application in the form of a flowchart is given in Figure 5.

This application mainly constitutes of three modes:

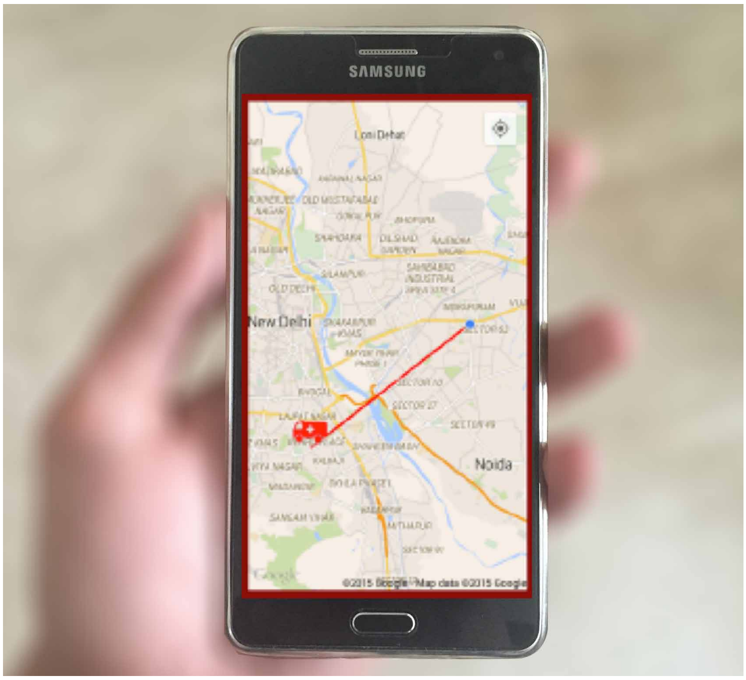
1. **The Medical Emergency Mode:** In this mode, the user has the functionality to locate the three nearest hospitals by using the GPS (Global Positioning System). The user also has the option to manually search hospitals on the basis of various parameters like hospital name, hospital address, hospital zip code, hospital city or country. After selection of the desired hospital, a location based alert is sent to the hospital notifying it about the emergency at the user's location. Meanwhile the user can forward his Medical ID recorded while registering on the application along with any additional details regarding the emergency that may be required at the time of admission at the hospital. Valuable time would be saved since the hospital would be prepared in advance and all the formalities would be completed. The hospital will deploy an ambulance to the user's location and the necessary information received by the hospital is forwarded to the ambulance. The user can track the ambulance in real time on a map within the application, which will enable him to know precisely where the rescue vehicle has reached (Figure 6). The ambulance driver can also navigate to the user's location with ease by using the map. The application also has a provision through which the triage nurse present in the ambulance can assign a triage color code (Red, Yellow, Green, Black) based on the 'ABCDE' resuscitation system [11].
2. **The Fire Emergency Mode:** Similar to medical emergencies, here the user can retrieve the list of the three nearest fire stations, or alternatively has the functionality to search fire stations manually on the basis of above listed parameters like the name, city, zip code etc. After selection of the fire station, a location based alert is sent to that fire station. The fire station deploys a fire ambulance to the user's location and the user and fire ambulance driver can track each other on a map.

Figure 5. Flowchart for REDAlert+ Android Application



3. **Car Mode:** In this mode, using the application of VANETs, the vehicles act as mobile nodes creating their own ad-hoc network. In this setup, all vehicles in the range of the user's vehicle can exchange information. The vehicles can drop out of the network and new ones are added according to the range. This application uses the Wi-Fi-Direct technology, which has a typical range of approx. 200m [12]. Each vehicle using the application is alerted as soon as an ambulance is in the range of the user's network. Using this concept, the user can form proper corridors and the emergency vehicle can reach its destination smoothly with minimal delay. This mode is further explained using some real time scenarios in the next section.

Figure 6. User Tracking the Ambulance



The java code for plotting the ambulance's location on a map is shown in figure 7. The ambulance's marker is created using the ambulance's location stored in the variable *latLng*.

Figure 8 shows the way the PHP script is called from the java application. The PHP script interacts with the online stored database and returns the results back to the java application. The result is parsed using JSON.

The tools required for the implementation of this application are given in table 2 and the system requirements for setting up the infrastructure and implementing this solution are presented in table 3.

The proposed solution: REDAlert+ is designed keeping practicality and functionality in focus. The next section presents the performance testing under few scenarios.

Figure 7. Plotting the ambulance on a map

```
@Override
public void onLocationChanged(Location location) {
    TextView tvLocation = (TextView) findViewById(R.id.tv_location);
    // Getting latitude of the current location
    double latitude = location.getLatitude();
    // Getting longitude of the current location
    double longitude = location.getLongitude();
    // Creating a LatLng object for the current location
    LatLng latLng = new LatLng(latitude, longitude);
    // Showing the current location in Google Map
    googleMap.moveCamera(CameraUpdateFactory.newLatLng(latLng));
    // Zoom in the Google Map
    googleMap.animateCamera(CameraUpdateFactory.zoomTo(15));
    googleMap.addMarker(new MarkerOptions()
            .position(latLng)
            .title("Ambulance Location")
            .snippet(st2)
            .icon(BitmapDescriptorFactory.fromResource(R.drawable.redam)));
    // Setting latitude and longitude in the TextView tv_location
    tvLocation.setText("Latitude:" +  latitude  + ", Longitude:"+ longitude );
    gps = new GPSTracker(rev.this);
    Polyline line1 = googleMap.addPolyline(new PolylineOptions()
            .add(new LatLng(latitude,longitude),
                    new LatLng(gps.getLatitude(),gps.getLongitude()))
            .width(5)
            .color(0xFFFF0000));
```

Figure 8. Connecting to PHP script

```
public void getData(String text,String latitude, String longitude) {
    String result = "";
    InputStream isr = null;
    try {
        List<NameValuePair> nameValuePairs = new ArrayList<>(1);
        nameValuePairs.add(new BasicNameValuePair("text", text));
        HttpClient httpclient = new DefaultHttpClient();
        HttpPost httppost = new HttpPost("http://redalert.site90.net/medid.php");
        httppost.setEntity(new UrlEncodedFormEntity(nameValuePairs));
        HttpResponse response = httpclient.execute(httppost);
        HttpEntity entity = response.getEntity();
        isr = entity.getContent();
    } catch (Exception e) {
        Log.e("log_tag", "Error in http connection " + e.toString());
        m7.setText("Couldn't connect to database");
    }
}
```

Table 2. Implementation tools

S. No.	Tool	Version	Description
1	Android Studio	Beta 0.86	For designing the android applications.
2	Eclipse with ADT	Juno 4.2	For coding the android applications in Java.
3	Adobe Photoshop	CS6	For designing the UI/UX of the applications.
4	Sublime Text	2.2	For coding the Python and PHP scripts.
5	Atom	Stable Release	For coding the UI

Table 3. System requirements

S. No.	Requirement
1	Android OS for running the REDAlert+ Applications
2	MySQL database on the cloud for storing all the data in a centralised hosted location
3	Python for Android (PY4A) Release 6 for compiling python scripts (included in the REDAlert+ Bundle)
4	Scripting Layer for Android (SL4A) Release 6 for running the python scripts (included in the REDAlert+ Bundle)

RESULTS

To test the practicality and usage of this application, a series of tests were carried out. To test the first scenario, in which a user has a medical emergency, a fleet of three private vehicles tagged as A1, A2 and A3 with the REDAlert+ Ambulance app on board were requisitioned. These vehicles were deployed in close proximity to three hospitals in New Delhi. Three members of the testing team marked as H1, H2, and H3 stood outside the hospitals with the REDAlert+ Hospital app on their phones. The user U represents the location of the victim who was randomly placed at a location within a 5-10 kilometer radius of the three medical centers. This is depicted in figure 9.

Using the REDAlert+ app on the mobile phone, U simulated a medical emergency. On launching the app, the three phones H1, H2 and H3 representing three hospitals in the vicinity appeared on the screen of the user (Figure 10). The user selected one of the hospitals (in this case H2) and an emergency alert was sent to the hospital H2. The hospital H2 then sent the alert to ambulance marked A2, which was then guided by the app to the location of the distress call.

Figure 9. Emergency Simulation

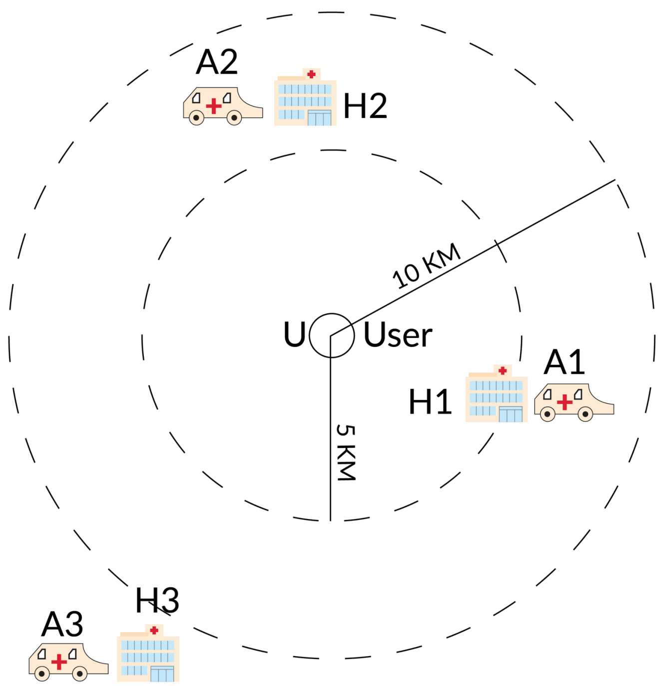


Figure 10. Hospitals in proximity

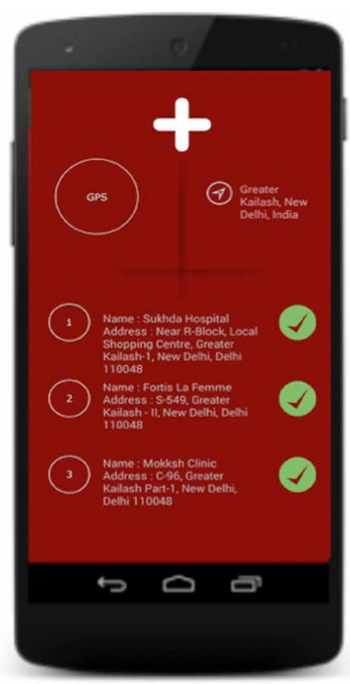


Table 4. Total call time

Hospital Selected	Approx. distance of patient location from hospital (km)	Site Response Time (SRT) (hh:mm:ss)	Hospital Response Time (HRT) (hh:mm:ss)	Total Call Time (TCT) (hh:mm:ss)
H1	5.5	00:12:34	00:11:27	00:24:01
H2	8.1	00:15:11	00:14:40	00:29:51
H3	10.3	00:19:22	00:17:10	00:36:32

The site response time (SRT), i.e. the time taken from the initiation of the call to the arrival of the ambulance A2 at the accident scene was recorded as 15 minutes 11 seconds. The hospital response time (HRT), i.e. the time taken from the accident site to the original location of the hospital H2 was recorded as 14 minutes 40 seconds. The total call time (TCT) to handle the emergency was 29 minutes and 51 seconds.

This experiment was repeated several times by varying the hospital selected by U (among H1, H2 and H3) and the observations were tabulated in Table 4.

In a study, Centralized Accident and Trauma Services (CATS), Dept. of Hospital Administration, All India Institute of Medical Sciences (AIIMS), New Delhi, India,

Figure 11. Ambulance approaching from behind

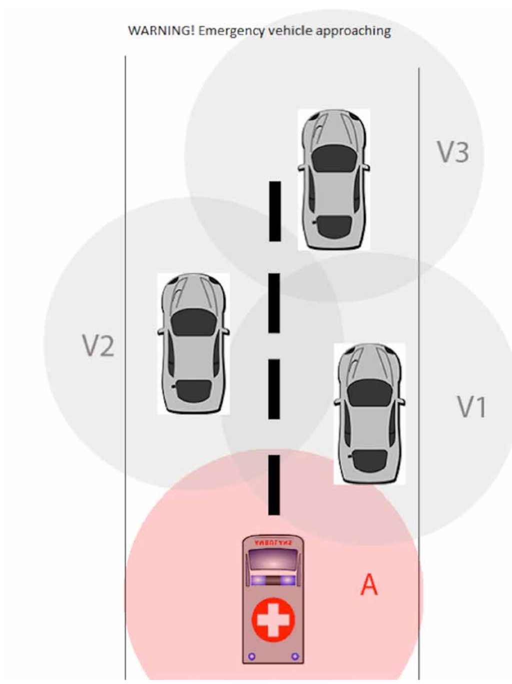
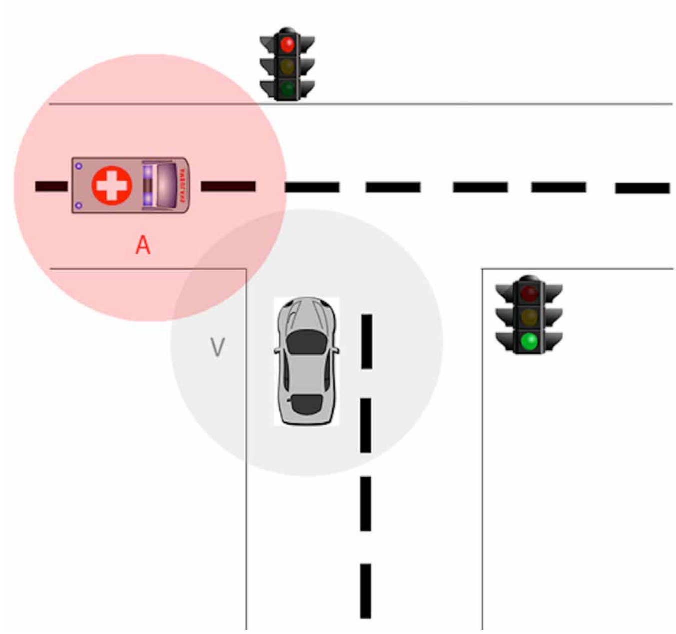


Figure 12. Ambulance skipping a red light



reported that the average SRT, HRT and TCT was approximately 10 minutes, 30 minutes and 57 minutes respectively.

On interaction with the team responsible for the CATS study, it was learned that the above figures were for hospitals within a 5-kilometer radius of the site of emergency.

To evaluate the REDAlert+ Car mode, our proposed system was further tested under the following two scenarios. Four vehicles A, V1, V2 and V3 were used for simulating these common scenarios. Vehicle A was tagged as the ambulance while vehicles V1, V2 & V3 depicted traffic on the road.

- Ambulance (A) on the road approaching the user (V3) from behind (Figure 11)

The user in vehicle V1 was alerted of an ambulance (A) approaching from behind. This information was propagated to the vehicle V2 since it was also in the range of the ambulance. Vehicle V3 was alerted by vehicle V1/V2. In this way, all vehicles were alerted about the approaching ambulance, which would subsequently lead to proper traffic corridor formation and allow the emergency vehicle (A) reach its destination quickly without losing time.

- Ambulance (A) skipping a red light to reach its destination

Many accidents on road occur as the emergency vehicles skip the stoplight in order to reach the hospital. Figure 12 depicts the scenario where the ambulance (A) is skipping the red light in the event of an emergency. The user in vehicle (V) was alerted by the ambulance crossing the red light and warned him to let the emergency vehicle pass. This would help avoid accidents and increase road safety. The time taken by a vehicle to broadcast the alert to all the vehicles in its range was less than a second.

The next section analyses, interprets and explains the findings along with the observed anomalies.

DISCUSSION

This study found that the average TCT for a hospital selected within a 10-kilometer radius was 30 minutes and 08 seconds. The figures obtained by the CATS study cited approximately 57 minutes, which yields a clear benefit of approximately 26 minutes when using the REDAlert+ app.

An anomaly on the CATS timings was discovered in which their HRT was higher than the SRT. This is due to the exclusion of the time spent in transferring the patient into the ambulance after the ambulance has reached the emergency site, which is a limitation of this study.

Another factor that influences the SRT, HRT and the TCT are the real world traffic conditions. While conducting the experiments, peak traffic conditions as well as medium density locations were chosen. Therefore, the data obtained is a fair representation of actual ground realities and the obtained results are accurate.

In a simulated environment, it is difficult to quantify the time advantage accrued on account of the patient's medical history being available with the medical staff prior to arrival at the casualty, which is an important feature of the app. The app permits the patient's medical data, already available on the cloud server, to be shared with the emergency team at the hospital in addition to sharing the nature of the trauma while en-route. It is safe to assume that this advance information will hasten the medical prepping which will further reduce delays in administering treatment.

The car mode of this application solves the monumental problem of corridor formation and road accidents. An alert can be propagated to all the vehicles on the road with the app within a few seconds educating them of the advancing ambulance thereby reducing chaos, accidents and time wastage.

Future work would include a performance evaluation in a real and unpredictable scenario. Additionally, there is also room for the integration with personal monitoring devices and sensors that collect relevant data in real time and help in alerting emergency care to respond to a situation.

CONCLUSION

This paper presented REDAlert+, a medical/fire emergency and warning system for android devices that helps speed up transport and care of trauma victims. This application is aimed at connecting hospitals, ambulances and patients by reducing the time wastage and providing ease of usability so that emergency services can be provided to the user in an efficient manner. Greater reliability is achieved by switching between Wi-Fi/GSM depending on the availability to send alerts to all stakeholders in the emergency response team. The usage of Wi-Fi Direct technology in providing peer-to-peer connectivity through VANETs is a unique attempt to promote the creation of emergency road corridors that hasten medical attention to the trauma victim and help reduce the overall call time.

REFERENCES

Baykal, E. (2013). Adhoc Data Transfer for Android Devices. Linnaeus University, Center for Technology Innovation's Mobile Economy Project event.

Chang, K. T., Lo, B. C., Teng, M. C., & Jiang, Y. Y. (2012). *Developing an android-based emergency broadcasting system for natural hazards. Ming-hsin University of Science and Technology, National Science and Technology Center for Disaster Reduction*.

Gupta, S.K., Kumar, N., Thergaonkar, A., Singh, A.R., Singh, S.K.V., Mehta, S.P., Parmar, S.C., & Mishra, S.B.N. (n. d.). Report of the Working Group on Emergency Care in India. Retrieved from http://healthmarketinnovations.org/sites/default/files/Centralized%20Ambulance%20Trauma%20Services%20Supporting%20Document%202.pdf

Hariprasath, L., Dhivya, R., & Adithya, S. (2013). Emergency Alert System using Android. *IJREAT International Journal of Research in Engineering & Advanced Technology*, 1(1).

Hu, S., Liu, H., Su, L., Wang, H., Abdelzaher, T.F., Hui, P., Zheng, W., Xie, Z., … Stankovic, J.A. (2014). Towards Automatic Phone-to-Phone Communication for Vehicular Networking Applications. *IEEE INFOCOM*.

Kim, H.Y., Kang, D.M., Lee, J.H., & Chung, T.M. (2012). A Performance Evaluation of Cellular Network Suitability for VANETs. *World Academy of Science, Engineering and Technology,* 64.

Koshmak, G. (2011). *An Android Based Monitoring and Alarm System for Patients with Chronic Obtrusive Disease*. Department of Technology at Örebro University.

Kumar, M. S., & Rajkumar, M. (2014). IPROB – Emergency Application for Women. *International Journal of Scientific and Research Publications*, *4*(3).

Monares, A., Ochoa, S., Pino, J., Herskovic, V., Covili, J., & Neyem, A. (2011). Mobile Computing in Urban Emergency Situations. *Expert Systems with Applications: An International Journal*.

Mur, D. C., Saavedra, A. G., & Serrano, P. (2013). Device to device communications with Wi-Fi Direct. *IEEE Wireless Communications*, *20*(3), 96–109. doi:10.1109/MWC.2013.6549288

Santos, B. D. M., Rodrigues, J. J. P. C., & Silva, B. M. C. (2013). EmergenSIG: An Integrated Location-based System for Medical Emergencies. *Paper presented at the 9th International Conference on Multimedia Information Technology and Applications (MITA '13)*, Bali, Indonesia. http://patient.info/doctor/trauma-triage-and-scoring

Shaukat, N.K. (2014). Wi-Fi Direct in Android Using Peer-to-Peer Communication. *International Journal for Research in Applied Science and Engineering Technology*, 2(1).

West, D., & Valentini, E. (2013). How mobile devices are transforming disaster relief and public safety. Center for Technology Innovation's Mobile Economy Project event.

This research was previously published in the International Journal of E-Health and Medical Communications (IJEHMC), 8(1); edited by Joel J.P.C. Rodrigues; pages 37-51, copyright year 2017 by IGI Publishing (an imprint of IGI Global).

Chapter 3
Predicting Medical Resources Required to be Dispatched After Earthquake and Flood, Using Historical Data and Machine Learning Techniques:
The COncORDE Emergency Medical Service Use Case

Homer Papadopoulos
National Center for Scientific Research Demokritos, Greece

Antonis Korakis
National Center for Scientific Research Demokritos, Greece

ABSTRACT

This article presents a method to predict the medical resources required to be dispatched after large-scale disasters to satisfy the demand. The historical data of past incidents (earthquakes, floods) regarding the number of victims requested emergency medical services and hospitalisation, simulation tools, web services and machine learning techniques have been combined. The authors adopted a twofold approach: a) use of web services and simulation tools to predict the potential number of victims and b) use of historical data and self-trained algorithms to "learn" from these data and provide relative predictions. Comparing actual and predicted victims needed hospitalisation showed that the proposed models can predict the medical resources required to be dispatched with acceptable errors. The results are promoting the use of electronic platforms able to coordinate an emergency medical response

DOI: 10.4018/978-1-7998-2535-7.ch003

since these platforms can collect big heterogeneous datasets necessary to optimise the performance of the suggested algorithms.

1. INTRODUCTION

Demand prediction and forecasting after natural disasters are especially critical in emergency health management (Ardalan et al., 2009). According to WHO (World Health Organization, 2007), large-scale disaster situations causing mass casualty incidents are characterised among the others by:

- Large numbers of patients, which require the mobilisation of increased hospital personnel and equipment;
- Large numbers of the same type of injury (e.g. skin damage in fire or breathing problems in a gas leakage) that may require equally large amounts of the same type of medical supplies and specialists;
- Injuries that require immediate and simultaneous highly specialised intervention;
- Ambulances availability to deliver several patients;
- Stress and panic situations and, very often, inaccurate estimates of the number of injured people who need treatment.

Preparing essential parts of the healthcare system such as hospitals to prevent, respond, and rapidly recover from these threats is critical for protecting and securing the entire health infrastructure. Incidents such as the 2009 H1N1 influenza pandemic (Shrestha et al., 2010), the Fukushima tsunami (Bachev, 2014) and the hurricane Sandy (Kryvasheyeu et al., 2015) highlighted the importance of preparedness for hospitals against potential threats and their consequences in the community. We should also note that these threats, are added to the considerable multiple challenges faced by trauma centres operating in hospitals and healthcare systems on a daily basis. However, during the emergency response process, in reality, it is difficult to obtain an accurate estimation and prediction of commodities demand after natural disasters because traditional statistic methods such as time-series forecasting methods seem to be ineffective (Zhao and Cao, 2015).

Recent years, aiming at this problem, new technological advancements (Web 2.0 services, broadband communications, and the ability to process, and analyse big heterogeneous data-streams) have been applied to get an insight into the fast-changing situation and help drive an effective disaster response. More specifically Haiti earthquake motivated ICT usage driven crisis since big data collected during the crisis (Meier, 2014) helped to find information about the affected population.

After this disaster, data and technology-driven disaster response have become a norm leading to the emergence of a new kind of distributed intelligence (Crowley and Chan, 2011). The 2013 World Disasters Report[1] highlighted the importance of disaster response in the perspective of big data and technology.

However, still, large-scale disasters and emergency situations expose the lack of integration and collaboration among all the involved organisations revealing challenges for useful decision support tools. The COncORDE as a technology research project (www.concorde-project.eu) tried to cope with the gaps mentioned above. The project developed a platform of ICT tools that make the best use of existing and emerging technologies for healthcare emergency management and a Decision Support System (DSS) to improve preparedness and interoperability of medical services during emergencies and mass disaster events. The aim of this study, which conducted within the realm of the COncORDE project, is to integrate and experiment with existing tools and techniques to predict victims that need Emergency Medical Service and hospitalisation after earthquake and floods within acceptable errors. This paper describes the architectural design of the generated decision support service which integrates simulation tools, web services, historical data and machine learning techniques (regression modelling framework, Natural Language Process models, deep neural networks) and provides and discusses some first promising results.

The following section presents the background and related work of similar systems and studies. Section 3 describes the architecture of the prediction service for all the use cases while Section 4 presents and discusses some first results of the models, followed by the conclusions part in Section 5.

2. BACKGROUND AND RELATED WORK

In recent years, software platforms[2] and information management systems are used to collect data, to provide situational awareness and actionable insights for decision-makers and increase and improve information exchange in emergency situations (Garret et al., 2003; Shen and Shaw, 2004; Demchak et al., 2006; Chua et al., 2007; Chen et al., 2009; FAO, 2011; Balfour, 2012).

Furthermore, online social media, like Twitter and Facebook, have matured into prominent communication platforms and provide an unprecedented opportunity to record and analyse vast amounts of information (Lazer et al., 2009). The potential of these networks is already leveraged during natural disasters (Watts et al., 2013), with applications in situation awareness (Caragea et al., 2011), event detection (Earle et al., 2012), search/locating persons (Rahwan et al., 2013) and others (Balana, 2012; Blanchard et al., 2012).

Following this trend, scholars (Chapman and Ciravegna, 2013) stress the need to combine semantic Web with natural language processing to apply data and text mining techniques and extract useful data for decision support in emergency response. Within this realm, new applications and techniques of data mining support in building situation awareness and real-time threat assessment and in facilitating information sharing have been developed (Li Zheng et al., 2013).

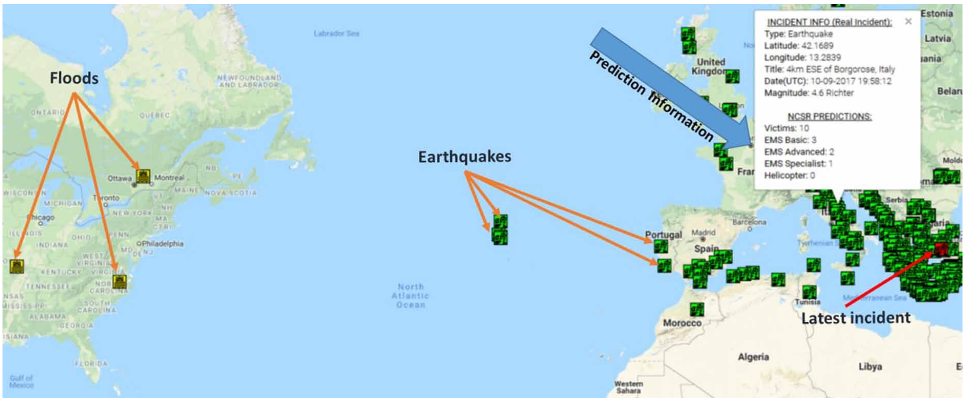
Above all, information management technologies and decision support systems and techniques can be used to analyse information on how emergency response activities are being implemented and make predictions about additional activities and the resources that are required (FAO, 2011). These methods include artificial intelligence model (e.g. Neural Networks) and time-series (Xu et al., 2010), advanced knowledge models for aggregating the knowledge of geographically separate experts (Mendonça et al., 2000), case-based reasoning (Deng et al., 2014) and information entropy theory (Sheu, 2010).

However, using state of the art machine learning systems to predict for example the necessary medical resources required to be dispatched and relief to populations devastated by the effects of a disaster-producing event, involves challenges. These challenges include among the others the identification of historical datasets to train the machine learning algorithms. Although there are many open Public Datasets[3456] which are made available to research communities to advance research on crisis computing and can be used to train machine learning algorithms necessary for different kind of decision support systems these are not always helpful.

Following the difficulties as mentioned earlier and challenges to identify suitable historical datasets, researchers have applied alternatives to generate Artificial Corpus using Artificial Intelligence planners, synthetic big data techniques that can generate data based on a specified schema using open source tools[7] and Monte-Carlo simulation (Agre and Horswill, 1992; Beckman et al., 1993; Lesh 1998; Blaylock and Allen, 2005; Grinberger et al., 2015).

Within the framework of the COncORDE project, we adopted a blended approach where we found a real historical data from past events and from which we derived a basic model that we used for the generation of further synthetic data in such a way that some relevant properties have been satisfied.

Figure 1. The Emergency Medical Service prediction web platform



3. IMPLEMENTATION OF THE EMERGENCY MEDICAL SERVICE PREDICTION MODEL

3.1. The architecture of the Emergency Medical Service Prediction Model

The Emergency Management System[8] of the COncORDE platform incorporates different subsystems, methods, tools and algorithms to generate estimations of the medical resources required to be dispatched after large-scale disasters. The system produces predictions for medical vehicles that are required to be dispatched after earthquake and flood as shown in Figure 1.

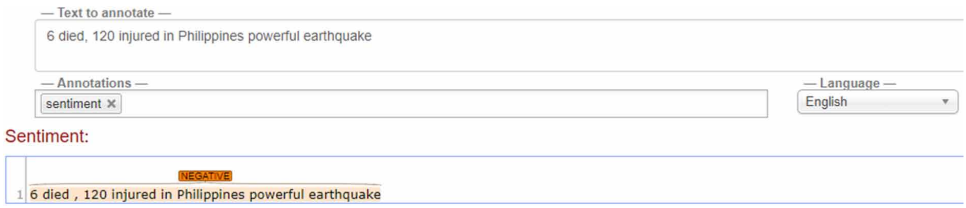
Within the following sections, we describe the architecture design of this system.

3.2. The Architecture of the Emergency Medical Service Prediction Service for Earthquakes

The Emergency Medical Service algorithm for earthquakes is following (see Figure 2):

- Every five minutes search the US Geological Survey Service9 for new earthquake incidents;
- If there is new incident, then it searches for Tweets[10] related to the new earthquake (search for earthquake's location and time) and trigger the Stanford CoreNLP tool to do a sentiment analysis to all identified tweets;
- The Earthquake Loss Estimation Routine (ELER11) analyses the earthquake's geographical data (longitude, latitude, depth) and earthquake's magnitude of the new incidents and predict potential victims;

Figure 2. The architecture of the Emergency Medical Service prediction module for earthquakes



- Three machine learning algorithms process the incidents' data, the predicted victims and the Twitter sentiment analysis to predict the medical resources required to be dispatched;
- The predicted medical resources and victims are saved into the COncORDE platform and compared with the "real world" data (actual earthquakes' victims and medical resources);
- The "real world" data in the COncORDE platform feed the machine learning algorithms to train them further increasing their accuracy-precision.

3.3. The Architecture of the Emergency Medical Service Prediction Service for Floods

The Emergency Medical Service algorithm for floods is following (see Figure 3):

- Every five minutes send a request to the Global Disaster Alert and Coordination System Service for new floods incidents;
- If there is new incident, then it searches for Tweets[12] related to the new flood (search for flood's location and time) and trigger the Stanford CoreNLP tool to do a sentiment analysis to all identified tweets;
- It triggers the Stanford CoreNLP tool to do a sentiment analysis to all identified tweets and predict victims;
- Three machine learning algorithms process the flood's magnitude, time, the predicted victims and the Twitter sentiment analysis to predict the medical resources required to be dispatched;
- The predicted medical resources and victims are saved into the COncORDE platform and compared with the "real world" data (actual floods' victims and medical resources);
- The "real world" data in the COncORDE platform feed the machine learning algorithms to train them further increasing their accuracy-precision.

Figure 3. The architecture of the Emergency Medical Service prediction module for floods

3.4. Platforms and Open Tools Utilised for the Emergency Medical Service in COncORDE

3.4.1. United States Geological Survey Service

To retrieve real-time or near real-time data and detail information on current earthquakes we used the United States Geological Survey (USGS) platform and its relevant Application Programming Interface13 (APIs) also, its ShakeMap14 the product which provided to us near-real-time maps of ground motion and shaking intensity for significant earthquakes.

3.4.2. Earthquake Loss Estimation Routine

To generate a rapid estimation of earthquakes' victims and losses in the Euro-Mediterranean region we used the Earthquake Loss Estimation Routine[15] (ELER) working with the following levels of Analysis:

- Level 0 analysis estimates casualties based on magnitude and intensity information. The casualty estimation is done utilising regionally adjusted intensity casualty or magnitude-casualty correlations based on the Landscan population distribution inventory (Dobson et al., 2000);

- Level 1 analysis estimates casualties and building damages based on intensity information. The intensity-based empirical vulnerability relationship is employed to find the number of damaged buildings;
- Level 2 analysis estimates casualties and building damages based on ground motion and spectral parameters. The spectral acceleration-displacement-based vulnerability assessment methodology is utilised for the building damage estimation. The casualty estimation is done through the number of damaged buildings using HAZUS99 (FEMA, 1999)16 and HAZUS-MH (FEMA, 2003)17 methodologies.

3.4.3. Global Disaster Alert and Coordination System

To retrieve real-time or near real-time data and detail information on current floods we use the disaster event feeds of the Global Disaster Alert and Coordination System18 (GDACS). We analyse Twitter, based on the retrieved data, to predict potential victims, and then we estimate the number of Emergency Medical Service vehicles that are required to be dispatched using the forecasting methodology (machine learning models) as we describe below.

3.4.4. "Twitter Search API"

We use Twitter Search API19 to retrieve tweets relevant to current earthquakes and floods. We analyse these tweets to predict victims in floods and do a sentiment analysis in both earthquake and floods to identify the significance of the incident. Twitter Search API is part of Twitter's REST API[20] and it allows queries against a sampling of recent Tweets published in the past seven days.

For the earthquake events, first, we perform simulation in the Earthquake Loss Estimation Routine tool for all the incidents that the Global Disaster alert system provides –even the small-scale earthquake signals. If the output of the simulation tool (predicted victims) is different from zero, then we search and analyse the relevant tweets.

3.4.5. Stanford CoreNLP for Sentiment Analysis

We use Twitter Search API to collect and filter tweets that are referring to earthquakes and floods and Stanford CoreNLP21 tool to do sentiment analysis on the identified tweets and identify the significance of the incident. We use the result of the sentiment analysis as a variable in the machine learning algorithms to increase our confidence on the estimated number of the Emergency Medical Service vehicles that are required to be dispatched after earthquakes and floods. Stanford CoreNLP (the instance we used in COncORDE project can be found in http://143.233.247.63:9000/) integrates many of Stanford's Natural Language Processing tools, including the sentiment analysis tool and the open information extraction tools and it provides model files for the analysis of well-edited English. Within the realm of the COncORDE project, we used only English language tweets.

3.4.6. Machine-Learning Frameworks Used for Emergency Medical Resources Estimation

- H2O[22] is a Java machine learning framework, which seamlessly integrates with the most popular open source products like Apache Hadoop and Spark providing the flexibility to solve the most challenging data problems. A machine learning model can be trained on complete data sets in real-time with H2O's rapid in-memory distributed parallel processing;
- The Accord.NET Framework[23] is a .NET machine learning framework combined with audio and image processing libraries wholly written in C#. It is a complete framework for building production-grade computer vision, computer audition, signal processing and statistics applications.

3.5. Algorithm Developments for the Emergency Medical Service

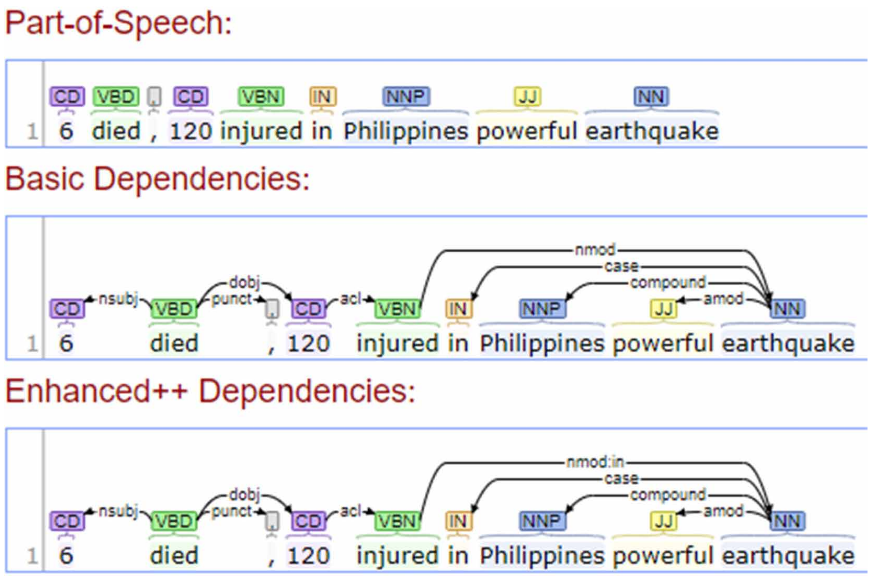
3.5.1. Sentiment Analysis and Twitter to Estimate Victims and Increase the Confidence of Predictions

We use Twitter Search API to find tweets that are referring to victims, injured, casualties and others, we analyse these tweets using Natural Language Processing tools, and we estimate the number victims in floods and the significance of earthquakes or floods. We use these values as additional inputs in the Emergency Medical Service to increase the confidence of the produced estimations. Figures 4 and 5 shows the COncORDE Prediction Service.

Figure 4. The architecture of the Twitter module in the COncORDE Prediction Service

```
tweet date:  Sat Feb 11 23:56:13 EET 2017
tweet likes:  0
sentence:  6 die, 120 injured in Philippines powerful earthquake
```

Figure 5. Example of Twitter search in the COncORDE Prediction Service



More specifically we use the Twitter Search API to retrieve a sampling of recent Tweets and those published in the past seven days following two different methods. The first method searches for tweets using only keywords like the type of incident (flood) and incident's country, City and Date while the second method filters the tweets using the incident's geographical data (longitude, latitude) and the type of incident (e.g. earthquake) and incidents date. We are using both methods since it is very difficult to retrieve tweets based on their geographical data (longitude, latitude).

We use Stanford's deep learning model (Stanford CoreNLP) that builds up a representation of whole sentences based on the sentence structure to do sentiment analysis of the identified tweets. We compute the sentiment based on how words compose the meaning of longer phrases. Tweets are short messages, restricted to 140 characters in length. Due to the nature of this microblogging service (quick and short messages), people use acronyms, make spelling mistakes, use emoticons and other characters that express special meanings. We follow the following steps for the data preprocessing for all the identified tweets:

- Remove those keywords we used to search (e.g. earthquake) to neutralise the sentiment analysis score from these keywords;
- Tokenization - A tokeniser divides the text into a sequence of tokens, which roughly correspond to "words";
- Remove targets - usernames (words starting with @);

- Remove URLs;
- Replace emoticons with their emotional state;
- Normalization: For the normalisation process, the presence of abbreviations within a tweet is noted, and then abbreviations are replaced by their actual meaning (e.g., idk – I do not know). We replaced all instances of repeated characters with a single character (e.g. my gooood – my god).

We do a Sentiment analysis with the processed data to cluster each tweet in one of the following categories:

- Negative (1)
- Neutral (2)
- Positive (3)

An example of the sentiment analysis of a particular tweet is shown in Figure 6.

For example, in an earthquake in the Philippines, we retrieved 34 tweets, and the results of the sentiment analysis are shown in Table 1.

The Sentiment Analysis classified most of the tweets as Negative (1). We used this value in the machine learning process to increase the confidence of the estimated emergency medical vehicles.

Figure 6. The format of sentiment analysis of a tweet in the COncORDE Prediction Service

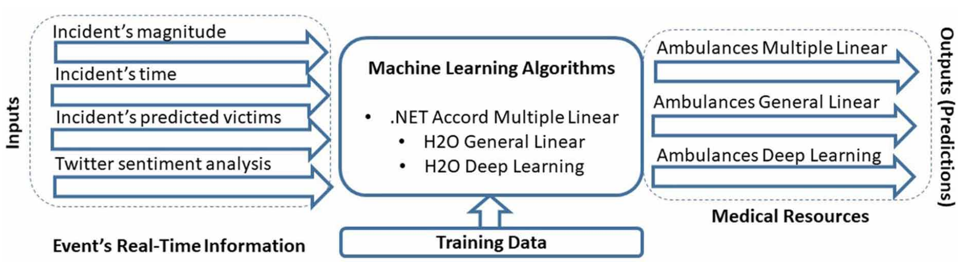


Table 1. Example of the analysis of the Tweets for the Philippines earthquake

Categories	Number of Tweets Classified
Negative (1)	26
Neutral (2)	6
Positive (3)	2

3.5.2. Twitter Victims Prediction

We analyse tweets with Stanford's CoreNLP tool to estimate the number of victims in a flood incident. To do the analysis, we have created a vocabulary containing all words that could refer to victims in case of an incident (such as die, deaths, deads, injured and others). The procedure of creating the vocabulary started by a small number of words and extended by recursively finding and adding synonyms and similar meaning words. To form the vocabulary to work with we used WORDNET[24]; a large lexical database of English. Nouns, verbs, adjectives and adverbs that we grouped into sets of cognitive synonyms (synsets), each expressing a distinct concept.

We then follow the following procedure for each of the tweets:

- **Normalization:** In the normalisation process, we find and replace words that represent numbers with their respective number (e.g. fifty-five -> 55);
- **Sentence Tokenize using CoreNLP Tokenizer:** Sentence Tokenize also was known as Sentence breaking is the problem in natural language processing of deciding where sentences begin and end;
- **Part-of-speech tagging using CoreNLP Speech Tagger:** Part-of-speech tagging is assigning the correct part of speech (noun, verb, and others.) to words. Any token that we have assigned to CD that represents Cardinal number is likely referring to victims. The English taggers use the Penn Treebank tag set;
- **Using CoreNLP to extract the dependencies:** Dependencies provide a representation of grammatical relations between words in a sentence. We are interested in the dependencies of the CD's found earlier. We consider as an estimation any of the dependencies that are an NN (Noun, singular or mass), or an NNS (Noun, plural), or a VBD (Verb, past tense) or a VBN (Verb, past participle) and are part of the vocabulary we have created.

One of the tweets that we received from the Twitter API for the earthquake in the Philippines is shown in Figures 7-9.

The normalisation of the tweets in Figure 7 replaces the "Six" word with the number 6 as shown in Figure 8.

The analysis of this simple one sentence tweet with the CoreNLP tool to get the parts-of-speech produces the result shown in Figure 9.

There are 2 CD's (Cardinal numbers) in the sentence, so we proceed to the dependencies. The dependency of the CD (Cardinal Number) "6" is an NN (Noun, singular or mass - "die") and contained in our vocabulary. Furthermore, the dependency of the CD "120" is a VBN (Verb, past participle) and also contained

Figure 7. Example of Tweets for the Philippines earthquake

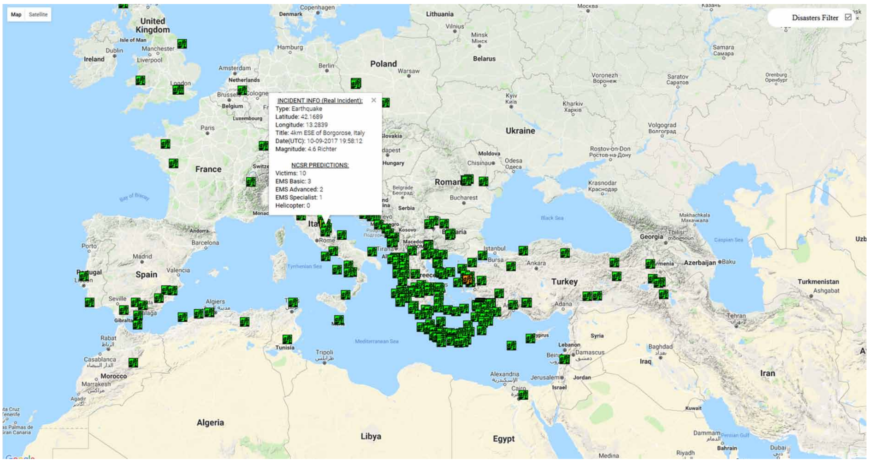


Figure 8. The normalised Tweet for the Philippines earthquake

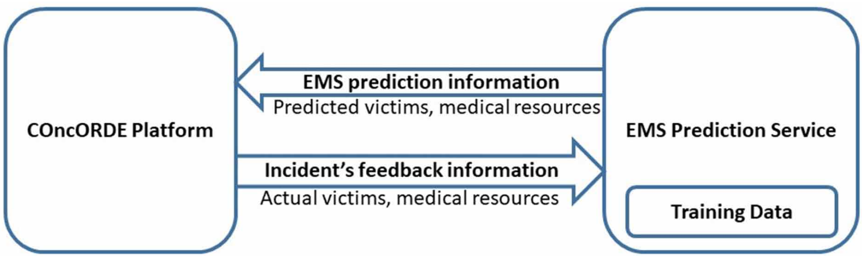
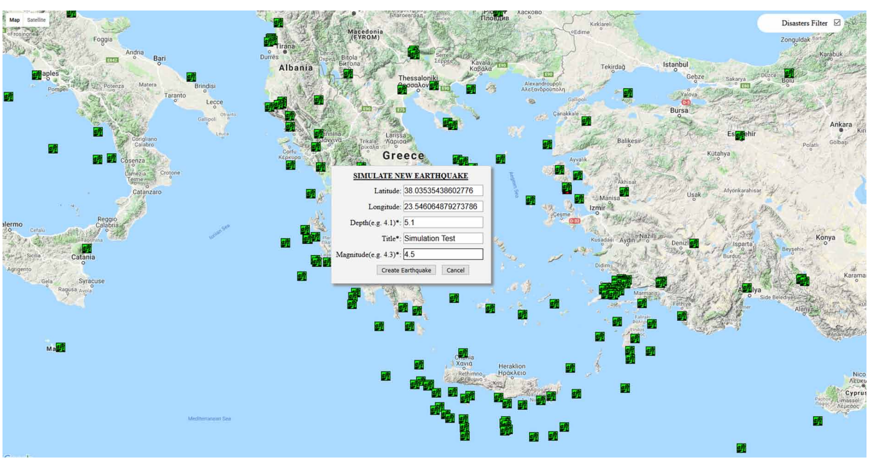


Figure 9. Example of the language analysis with the CoreNLP tool for the Philippines earthquake



in our vocabulary. So, both numbers are used to calculate the number of victims (in this sentence) which is 126.

We follow this procedure for all the identified tweets, and the estimation of the number of victims is the value that appears most often. In our example (earthquake in the Philippines), multiple sources are referring to 126 victims, so this is the final estimation for this event. We use this number as an input in the COncORDE Emergency Medical Service Prediction Service to predict the emergency medical vehicles.

3.6. Machine Learning Algorithms Used to Predict Emergency Medical Vehicles

Multiple linear regression analysis methods and artificial neural networks (ANN) have been widely applied to forecast demand in disasters (Smith and Gupta, 2002; Hayati and Karami, 2005; Zhang and Xu, 2010; Kargar and Charsoghi, 2014). Although studies have demonstrated that in some cases artificial neural networks provide accurate time series forecasts (Kandananond, 2011) we believe that the traditional statistical models, as well as the artificial neural networks models, have their shortcomings. To minimize defects, we applied both regression and deep learning neural networks where multiple linear regression models were chosen as the benchmark forecasting methods as shown in Figure 10.

Figure 10. Machine Learning architecture adopted in the Emergency Medical Service prediction service

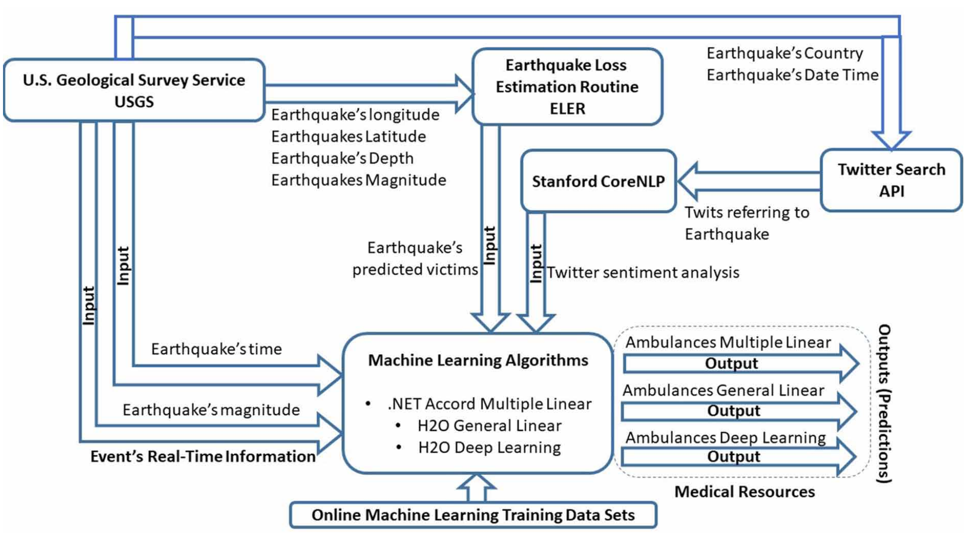


Table 2. Independent and dependent variables used in the machine learning models

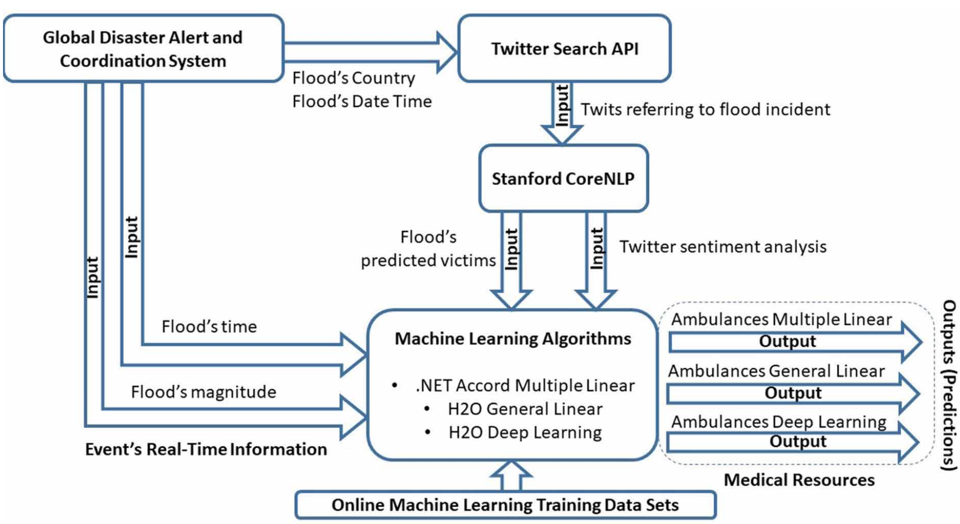
Independent Variables (Inputs) for the Machine Learning Models	Dependent Variables (Outputs)
Earthquake's magnitude (provided from USGS Service)	Emergency Medical Service Basic
Earthquake date time (provided from USGS Service) Flood date time (provided from GDACS Service)	Emergency Medical Service Advanced
Earthquake's predicted victims (calculated from ELER) Flood's predicted victims (calculated from twitter's analysis using Stanford CoreNLP's Named Entity Recognition, Tokenizer, Part of speech tagging and dependencies).	Emergency Medical Service Specialist
Incident's (both earthquake and flood incidents) twitter sentiment analysis using Stanford CoreNLP	Helicopter

We used three machine learning models (Multivariate Linear, General Linear model and Deep Learning), all of which support multiple inputs (four-4) and outputs (three-3), to estimate the emergency medical vehicles.

To train the machine learning models, we adopted a blended approach:

- We used real historical data from past events from National Centers for Environmental Information25, and we derived a model and a probability distribution that best described these datasets;

Figure 11. Example of the machine learning results in the web portal of the Emergency Medical Service



- Based on this model and the probability distribution we generated further synthetic data in such a way that some relevant properties have been satisfied.

We used four independent variables (inputs) to estimate the number of four categories of Emergency Medical Service vehicles (dependent variables) as shown in Table 2.

The picture shown in Figure 11 presents the inputs and outputs of the machine learning tools.

A description of the configuration of the machine learning models is shown in the following section.

3.6.1. Multivariate Linear (ACCORD) and Generalized (H2O) Linear Models

Multiple and Generalized Linear Models can estimate regression models for outcomes following Gaussian regression exponential distribution.

The linear regression model we experimented with corresponds to the Gaussian family model. The link function g is the identity, and density f corresponds to a normal distribution. It is the purest example of a Generalized Linear Model but has many uses and several advantages over other families. Specifically, it is faster and requires more stable computations.

The Generalized Linear Model (GLM) beyond the Gaussian (i.e. normal) distribution, can include Poisson, binomial, and gamma distributions. Each serves a different purpose, and depending on distribution and link function choice can be used either for prediction or classification. A detail description of the parameters of the Generalized Linear Model we experimented with is shown in Table 3.

3.6.2. Deep Learning Model (H2O) Adopted in COncORDE

We believe that within the realm of the business exploitation phase of the COncORDE project we will work with big datasets having to implement complex nonlinear models. Therefore, we tried to experiment with deep networks to forecast the number of emergency medical vehicles, since we can add significant complexity to these algorithms. We used a multi-layer feed-forward artificial neural network that is trained with stochastic gradient descent using back-propagation. A detail description of the parameters of the Deep Learning Model we experimented with is shown in Table 4.

To increase the Emergency Medical Service predictions' accuracy, we adopted an online learning method approach, since we updated our machine learning models for every new real-world data-point. More specifically the COncORDE platform provides real world data whenever these become available (real victims, Emergency

Table 3. The parameters of the Generalized Linear Model

General Liner Model Parameter	Option
number of folds for cross-validation	0
random number generator (RNG) seed for algorithm components dependent on randomisation	-1
model type	Gaussian
solver to use (AUTO, IRLSM, L_BFGS, COORDINATE_DESCENT_NAIVE, COORDINATE_DESCENT, GRADIENT_DESCENT_LH, or GRADIENT_DESCENT_ SQERR)	AUTO
enable lambda search	False
standardise the numeric columns to have a mean of zero and unit variance	False
force coefficients to have non-negative values	False
Enable this option to score during each iteration of the model training	False
Request computation of p-values	False
automatically remove collinear columns during model-building	False
number of training iterations	-1
link function (Identity, Family_Default, Logit, Log, Inverse, Tweedie, Ologit, Oprobit, and Ologlog)	family_default
handle missing values (Skip or mean imputation)	Mean Imputation
include a constant term in the model	True
threshold for convergence.	-1
beta epsilon value	0.0001
Specify a threshold for convergence	-1
prior probability for p(y==1)	-1
maximum number of active predictors during computation	-1
Search criteria	Cartesian

Medical Service resources actual needed, etc.). The system retrieves these real-world data via an authenticated POST request and continuously updates the training datasets providing more accurate predictions as shown in Figure 12.

3.7. Communication Protocols

The emergency medical vehicles estimation service supports two communication protocols:

1. Restful API (on demand requests);
2. Websockets (real-time notifications).

Table 4. The parameters of the Deep Learning Model

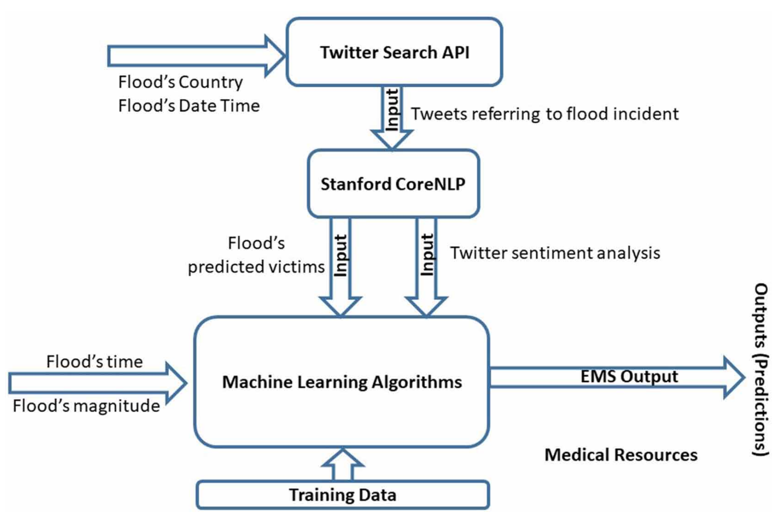
Deep Learning Model Parameter	Option
number of folds for cross-validation	0
activation function	Rectifier
ignore constant training columns	True
hidden layer sizes	200,200
number of times to iterate the dataset	10
compute variable importance	False
score during each iteration of the model training	False
oversample the minority classes to balance the class distribution	False
maximum number (top K) of predictions to use for hit ratio computation	0
use all factor levels in the possible set of predictors	True
automatically standardize the data	False
number of global training samples per MapReduce iteration	-2
enable the adaptive learning rate	True
input layer dropout ratio to improve generalization	0
L1 regularization to add stability and improve generalization	0
L2 regularization to add stability and improve generalization	0
loss function (Automatic, Cross Entropy, Quadratic, Huber, Absolute)	Automatic
distribution	Gaussian
quantile to be used for Quantile Regression	0.5
shortest time interval (in seconds) to wait between model scoring	5
number of training set samples for scoring	10000
maximum duty cycle fraction for scoring	0.1
Maximum allowed runtime in seconds for model training	0
enable the Deep Learning autoencoder	False
encoding schemes for handling categorical features	Auto
overwrite the final model with the best model found during training	True
target ratio of communication overhead to computation	0.05
random number generator (RNG) seed for algorithm components dependent on randomization	-1
adaptive learning rate time decay factor	0.99
adaptive learning rate time smoothing factor to avoid dividing by zero	1e-8&
enable the Nesterov Accelerated Gradient	True
initial weight distribution (Uniform Adaptive, Uniform, or Normal)	Uniform Adaptive
Specify the stopping criterion for regression error (MSE) on the training data	0.000001

continued on following page

Table 4. Continued

Deep Learning Model Parameter	Option
compute the variable importance for input features (using the Gedeon method)	True
enable fast mode, a minor approximation in back-propagation	True
force extra load balancing to increase training speed for small datasets and use all cores	True
run on a single node for fine-tuning of model parameters	False
shuffle the training data	False
handle missing values (Skip or MeanImputation)	Mean Imputation
display less output in the standard output	False
enable sparse data handling, which is more efficient for data with many zero values	False
use a column major weight matrix for the input layer	False
average activation for the sparse autoencoder	0
sparsity-based regularization optimization	0
maximum number of categorical features enforced via hashing	2147483647
force reproducibility on small data	false
export the neural network weights and biases as H2O frames	False
value for the mini-batch size	1
enable elastic averaging between computing nodes, which can improve distributed model convergence	False
Search criteria	Cartesian

Figure 12. Online learning method approach adopted in the Emergency Medical Service prediction service



3.7.1. Restful Webservice

The client can send a GET request to the Restful service located in http://143.233.247.63:8000/incidentpredictions, using the HTTP Basic authentication standard with the below-mentioned credentials:

username: concorde
password: testdemokritos

The authenticated client receives a JSON formatted response containing the below-mentioned incident's information:

- Incident's Type (earthquake, Flood);
- Incident's unique ID;
- Simulation (in case that this is a simulation incident);
- Incident's Date Time (in ms);
- Incident's Date Time (in readable format);
- Incident's magnitude (0 for flood);
- Map's URL (If available);
- Incident's Title;
- Incident's Country;
- Incident's Coordinates;
- Predicted Victims;
- Medical resources Prediction using Multivariate Linear algorithm;
- Medical resources Prediction using the Generalized Linear algorithm;
- Medical resources Prediction using Deep Learning Model algorithm;
- Supported information for validation (if available).

3.7.2. Web Sockets Client

The WebSockets client needs to subscribe to the WebSockets server located in: ws://143.233.247.63:800/incidentpredictions, using the HTTP Basic Authentication standard (similar to the restful webservice) with the below-mentioned credentials:

username:concorde
password: testdemokritos

Then the client will receive predictions when an event occurs real time. The client does not need to send requests to the server. The client needs to be subscribed to the

WebSockets server. The authenticated client receives a JSON formatted response similar to the Restful webservice response.

4. RESULTS AND DISCUSSION

To validate the performance of the three machine learning models we compared the predictions of these models with the real number of victims and emergency medical vehicles following the press release. The comparison of the predicted versus the real numbers concerns a time horizon of the seven first months of the year 2017.

For example according to the press release[26], the earthquake in Lesvos Island in Greece (12-06-2017, Magnitude: 6.3, http://earthquake.usgs.gov/earthquakes/eventpage/us20009ly0#shakemap) caused one dead woman and fifteen (15) injured victims.

The COncORDE Emergency Medical Service, predicted within the first minutes of the event-Earthquake 25 victims and 15 ambulances (mean values), which is quite close to the real numbers.

We have to notice that the models did not perform well and cannot be expected to perform well in incidents that concern floods. These events usually last many days, and a prediction of the number of victims and the requested medical resources should consider more parameters, e.g. performance of the first responders and others.

In Table 5, we present the predictions from all models, i.e., regression, deep neural network and a simple average of these three forecasts. Estimations coming from the deep learning models often exhibit average numbers while the regression models perform surprisingly well. A simple aggregation (or averaging) of predictions obtained from different procedures may or may not yield better accuracy.

Although the usability of these predictions at the moment is under question, we expect soon the use of more sophisticated tools, methods and algorithms and more large historical data to help us generate more accurate and rich predictions.

The scope of the study was to develop an integrated methodology to predict emergency medical vehicles in real events. However, our tools can also be used to simulate an earthquake and predict within this virtual event the expected victims and necessary medical vehicles that should be dispatched. We can use this extra feature for prevention and preparedness projects in the field of civil protection and medical agencies exercise programs (see Figure 13).

Table 5. Indicative comparison of the predicted values versus the actual numbers of victims in earthquakes and floods

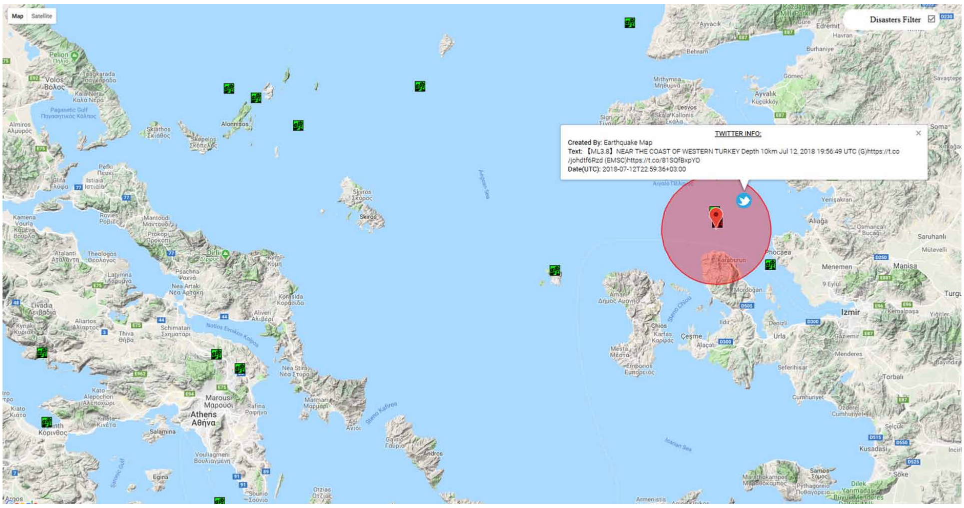
Type	Country	Coordinates (Lat, Lon)	Data Time (UTC) DD-MM-YYYY HH:mm:ss	Magnitude	Predicted Vehicles	Predicted Victims and EMS Vehicles (Mean Values)	Real World Victims
Earthquake	Greece	36.9485 27.4577	20-07-2017 22:31:12	6.7	**MultivariateLinearRegression:** "EMS_Basic": 18, "EMS_Advanced": 10, "EMS_Specialist": 6, "Helicopter": 0 **GeneralLinear:** "EMS_Basic": 18, "EMS_Advanced": 10, "EMS_Specialist": 6, "Helicopter": 0 **DeepLearning:** "EMS_Basic": 21, "EMS_Advanced": 4, "EMS_Specialist": 5, "Helicopter": 1	51 victims – 33 EMS vehicles	27
Earthquake	Greece	38.8251 26.4665	22-06-2017 02:48:53	4.8	**MultivariateLinearRegression:** "EMS_Basic": 5, "EMS_Advanced": 3, "EMS_Specialist": 2, "Helicopter": 0 **GeneralLinear:** "EMS_Basic": 5, "EMS_Advanced": 3, "EMS_Specialist": 2, "Helicopter": 0 **DeepLearning:** "EMS_Basic": 7, "EMS_Advanced": 3, "EMS_Specialist": 0, "Helicopter": 0	16 victims – 10 EMS vehicles	11
Earthquake	Italy	42.601 13.227	18-01-2017 10:14:10	5.7	**MultivariateLinearRegression:** "EMS_Basic": 112, "EMS_Advanced": 63, "EMS_Specialist": 36, "Helicopter": 0 **GeneralLinear:** "EMS_Basic": 112, "EMS_Advanced": 64, "EMS_Specialist": 36, "Helicopter": 0 **DeepLearning:** "EMS_Basic": 113, "EMS_Advanced": 60, "EMS_Specialist": 37, "Helicopter": 0	305 victims – 211 EMS vehicles	299
Flood	China	28.741 108.766	01-07-2017 21:00:00		**MultivariateLinearRegression:** "EMS_Basic": 10, "EMS_Advanced": 6, "EMS_Specialist": 4, "Helicopter": 0 **GeneralLinear:** "EMS_Basic": 10, "EMS_Advanced": 5, "EMS_Specialist": 3, "Helicopter": 0 **DeepLearning:** "EMS_Basic": 8, "EMS_Advanced": 5, "EMS_Specialist": 4, "Helicopter": 0	27 victims – 19 EMS vehicles	56

continued on following page

Table 5. Continued

Type	Country	Coordinates (Lat, Lon)	Data Time (UTC) DD-MM-YYYY HH:mm:ss	Magnitude	Predicted Vehicles	Predicted Victims and EMS Vehicles (Mean Values)	Real World Victims
Flood	Bangladesh	22.283 92.089	11-06-2017 21:00:00		**MultivariateLinearRegression:** "EMS_Basic": 34, "EMS_Advanced": 20, "EMS_Specialist": 12, "Helicopter": 0 **GeneralLinear:** "EMS_Basic": 34, "EMS_Advanced": 19, "EMS_Specialist": 11, "Helicopter": -1 **DeepLearning:** "EMS_Basic": 26, "EMS_Advanced": 16, "EMS_Specialist": 4, "Helicopter": 0	93 victims – 59 EMS vehicles	158
Flood	Sri Lanka	6.59 80.614	24-05-2017 21:00:00		**MultivariateLinearRegression:** "EMS_Basic": 61, "EMS_Advanced": 34, "EMS_Specialist": 20, "Helicopter": 0 **GeneralLinear:** "EMS_Basic": 60, "EMS_Advanced": 34, "EMS_Specialist": 19, "Helicopter": -1 **DeepLearning:** "EMS_Basic": 52, "EMS_Advanced": 18, "EMS_Specialist": 23, "Helicopter": 5	164 victims – 33 EMS vehicles	103
Flood	Peru	-11.904 -75.423	02-03-2017 22:00:00		**MultivariateLinearRegression:** "EMS_Basic": 28, "EMS_Advanced": 16, "EMS_Specialist": 9, "Helicopter": 0 **PredictedResourcesGeneralLinear:** "EMS_Basic": 27, "EMS_Advanced": 15, "EMS_Specialist": 9, "Helicopter": 0 **PredictedResourcesDeepLearning:** "EMS_Basic": 31, "EMS_Advanced": 17, "EMS_Specialist": 5, "Helicopter": 0	75 victims – 32 EMS vehicles	90

Figure 13. Example of an earthquake simulation in the Emergency Medical Service web portal



5. CONCLUSION

This study presents a modelling method to predict emergency medical resources (vehicles) required to be dispatched after large-scale disasters to satisfy the demand. The results showed that the use of historical data of the number of victims requested medical assistance (Emergency Medical Service and hospitalisation) after earthquakes and floods, together with simulation tools, web services, Natural Language Processing techniques, linear regression and deep learning models can predict emergency medical vehicles within acceptable errors. One of the challenges we have to overcome to increase the accuracy of our methods is to get more accurate historical data sets in an acceptable period to train the models. Since emergency management platforms like the COncORDE one can collect and process digital data, we expect more heterogeneous and rich large datasets soon to become available, helping us to train the algorithms better and get more accurate predictions.

ACKNOWLEDGMENT

European Commission funded the research under the 7th Framework ICT Research Programme. Further details can be accessed at http://www.concorde-project.eu/.

REFERENCES

Agre, P., & Horswill, I. (1992). Cultural support for improvisation. In *Proceedings of the Tenth National Conference on Artificial Intelligence*, San Jose, CA (pp. 363-368).

Bachev, H. (2014, December 13). Impacts of Match 2011 Earthquake, Tsunami and Fukushima Nuclear Accident in Japan. doi:10.2139srn.2538949

Balana, C. D. (2012). Social media: Major tool in disaster response. *Inquirer Technology*, *5*, 3.

Balfour, R. E. (2012). Next generation emergency management common operating picture software/systems (COPSS). In *2012 IEEE Systems, Applications and Technology Conference (LISAT)*, Long Island, NY, May 4.

Beckman, R. J., Baggerly, K. A., & McKay, M. D. (1996). Creating synthetic baseline populations. *Transp. Res. Part Policy Pract.*, *30*(6), 415–429. doi:10.1016/0965-8564(96)00004-3

Blanchard, H., Carvin, A., Whitaker, M. E., Fitzgerald, M., Harman, W., & Humphrey, B. (2012). The case for integrating crisis response with social media (White Paper). American Red Cross.

Blaylock, N., & Allen, J. (2005). Generating artificial corpora for plan recognition. In *User Modeling 2005, LNAI* (Vol. 3538, pp. 179-188). Springer. 10.1007/11527886_24

Caragea, C., McNeese, N., Jaiswal, A., Traylor, G., Kim, H. W., Mitra, P., ... & Yen, J. (2011). Classifying text messages for the Haiti earthquake. In *Proceedings of the 8th International Conference on Information Systems for Crisis Response and Management (ISCRAM2011)*.

Chapman, M. S., & Ciravegna, P. F. (2006). Focused data mining for decision support in emergency response scenarios. *Management*, *4*, 6–14.

Chen, R., Coles, J., Lee, J., & Rao, H. R. (2009). Emergency communication and system design: The case of Indian Ocean Tsunami. In *Proceedings of the 3rd International Conference on Information and Communication Technologies and Development (ICTD)* (pp. 300-309). 10.1109/ICTD.2009.5426699

Chua, A. Y. K., Kaynak, S., & Foo, S. S. B. (2007). An analysis of the delayed response to Hurricane Katrina through the lens of knowledge management: Research Articles. *Journal of the American Society for Information Science and Technology*, *58*(3), 391–403. doi:10.1002/asi.20521

Crowley, J., & Chan, J. (2011). Disaster Relief 2.0: The Future of Information Sharing in Humanitarian Emergencies. UN Foundation & Vodafone Foundation Technology Partnership. Retrieved from http://goo.gl/PylRL

Demchak, B., Chan, T. C., Griswold, W. G., & Lenert, L. A. (2006). Situational awareness during mass-casualty events: Command and control. *AMIA ... Annual Symposium Proceedings - AMIA Symposium. AMIA Symposium*, *2006*, 905. PMID:17238524

Ardalan, A., Masoumi, G., Gouya, M. M., Ghafari, M., Miadfar, J., Sarvar, M. R., ... & Khankeh, H. R. (2009). Disaster Health Management: Iran's Progress and Challenges. *Iranian Journal of Public Health*, *38*, 93–97.

Dobson, J. E., Bright, E. A., Coleman, P. R., Durfee, R. C., & Worley, B. A. (2000, July). LandScan: A Global Population Database for Estimating Populations at Risk. *Photogrammetric Engineering and Remote Sensing*, *66*(7), 849–857.

Earle, P. S., Bowden, D. C., & Guy, M. (2012). Twitter earthquake detection: Earthquake monitoring in a social world. *Annals of Geophysics*, *54*, 708–715.

Food and Agriculture Organization of the United Nations (FAO). (2011). Good Emergency Management Practices: The Essentials. FAO Animal Production and Health Manual No. 11.

Garrett, N. Y., Yasnoff, W. A., & Kumar, V. (2003). Emergency implementation of knowledge management system to support a bioterrorism response. *AMIA ... Annual Symposium Proceedings - AMIA Symposium. AMIA Symposium*, *2003*, 849. PMID:14728354

Grinberger, A. Y., Felsenstein, D., & Lichter, M. (2015). Simulating urban resilience: Disasters, dynamics and (synthetic) data. In S. Geertman, J. Stillwell, J. Ferreira, & R. Goodspeed (Eds.), *Planning Support Systems and Smart Cities* (pp. 99–119). Cham, Switzerland: Springer. doi:10.1007/978-3-319-18368-8_6

Hayati, M., & Karami, B. (2005). Application of Neural Networks In Short-Term Load Forecasting. In *7th WSEAS International Conference on Mathematical Methods and Computational Techniques in Electrical Engineering*.

Kandananond, K. (2011). Forecasting electricity demand in Thailand with an artificial neural network approach. Energies, 4(8), 1246-1257.

Kargar, M. J., & Charsoghi, D. (2014). *Predicting annual electricity consumption in Iran using artificial neural networks (NARX). Indian J. Sci. Res, 5(1), 231-242.*

Kryvasheyeu, Y., Chen, H., Moro, E., Van Hentenryck, P., & Cebrian, M. (2015). Performance of Social Network Sensors during Hurricane Sandy. *PLoS One*, *10*(2), e0117288. doi:10.1371/journal.pone.0117288 PMID:25692690

Lesh, N. (1998). Scalable and Adaptive Goal Recognition [PhD thesis]. University of Washington.

Lazer, D., Pentland, A. S., Adamic, L., Aral, S., Barabasi, A. L., Brewer, D., ... & Jebara, T. (2009). Life in the network: The coming age of computational social science. *Science*, *323*, 721–723. doi:10.1126cience.1167742 PMID:19197046

Meier, P. (2014). Digital Humanitarians: How Big Data Is Changing the Face of Humanitarian Response. CRC Press.

Mendonça, D., Rush, R., & Wallace, W. A. (2000). Timely knowledge elicitation from geographically separate, mobile experts during emergency response. *Safety Science*, *35*(1-3), 193–208. doi:10.1016/S0925-7535(00)00031-X

Deng, S. C., Wu, Q., Shi, B., Chen, X. Q., & Chu, X. M. (2014). Prediction of Resource for Responding Waterway Transportation Emergency Based on Case-Based Reasoning. *China Safety Science Journal*, *24*, 79–84.

Rahwan, I., Dsouza, S., Rutherford, A., Naroditskiy, V., McInerney, J., Venanzi, M., ... Cebrian, M. (2013). Global Manhunt Pushes the Limits of Social Mobilization. *Computer*, *46*(4), 68–75. doi:10.1109/MC.2012.295

Shen, S. Y., & Shaw, M. J. (2004). Managing coordination in emergency response systems with information technologies. In *Proceedings of the Tenth Americas Conference on Information Systems*, New York, NY.

Sheu, J. B. (2010). Dynamic relief-demand management for emergency logistics operations under large-scale disasters. *Transportation Research Part E, Logistics and Transportation Review*, *46*(1), 1–17. doi:10.1016/j.tre.2009.07.005

Shrestha, S. S., Swerdlow, D. L., Borse, R. H., Prabhu, V. S., Finelli, L., Atkins, C. Y., ... Meltzer, M. I. (2011). Estimating the burden of 2009 pandemic influenza A (H1N1) in the United States (April 2009– April 2010). *Clinical Infectious Diseases*, *52*(Suppl. 1), S75–S82. doi:10.1093/cid/ciq012 PMID:21342903

Smith, K. A., & Gupta, J. N. (2002). *Neural networks in business: techniques and applications*. Idea group publishing. doi:10.4018/978-1-930708-31-0.ch001

Watts, D., Cebrian, M., & Elliot, M. (2013). Dynamics of social media. *Public Response to Alerts and Warnings Using Social Media: Report of a Workshop on Current Knowledge and Research Gaps.* Washington, DC, USA: The National Academies Press.

World Health Organization (WHO). (2007). Mass Casualty Management Systems: Strategies and Guidelines for Building Health Sector Capacity. In *Health Action in Crises Injuries and Violence Prevention* (p. 38). Geneva: WHO Publications.

Xu, X. Y., Qi, Y. Q., & Hua, Z. S. (2010). Forecasting Demand of Commodities after Natural Disasters. *Expert Systems with Applications*, *37*(6), 4313–4317. doi:10.1016/j.eswa.2009.11.069

Zhang, H., & Xu, J. (2010). Research on Emergency Material Demand Forecasting Model in Disaster Based on MLR-CBR. In *International Conference of Logistics Engineering and Management (ICLEM)*. doi:10.1061/41139(387)404

Zhao, J. N., & Cao, C. J. (2015). Review of Relief Demand Forecasting Problem in Emergency Logistic System. *Journal of Service Science and Management*, *8*(1), 92–98. doi:10.4236/jssm.2015.81011

Zheng, L., Shen, C., Tang, L., Zeng, C., Li, T., Luis, S., & Chen, S. C. (2013). Data mining meets the needs of disaster information management. *IEEE Transactions on Human-Machine Systems*, *43*(5), 451–464. doi:10.1109/THMS.2013.2281762

ENDNOTES

1 http://www.ifrc.org/en/publications-and-reports/world-disasters-report/world-disasters-report-2013/
2 www.oneconcern.com
3 https://wtcdata.nist.gov/
4 http://crisisnlp.qcri.org/
5 https://kdd.ics.uci.edu/
6 https://www.cs.toronto.edu/~delve/data/datasets.html
7 https://github.com/tdunning/log-synth
8 https://webservices.iwelli.com/concorde/
9 www.usgs.gov
10 https://twitter.com/
11 http://www.koeri.boun.edu.tr/News/NERIES%20ELER%20V3.1_16_177.depmuh
12 https://twitter.com/

[13] https://www.usgs.gov/products/data-and-tools/apis

[14] https://earthquake.usgs.gov/data/shakemap/

[15] http://www.koeri.boun.edu.tr/News/NERIES%20ELER%20V3.1_16_177.depmuh

[16] http://www.disastersrus.org/emtools/earthquakes/FEMA366.pdf

[17] http://lee.civil.ntua.gr/pdf/mathimata/eidika_themata_texnikis/simeioseis/HAZUS-MH-MR1.pdf

[18] http://www.gdacs.org

[19] https://dev.twitter.com/rest/public/search

[20] https://developer.twitter.com/en/docs

[21] https://stanfordnlp.github.io/CoreNLP/

[22] https://www.h2o.ai/h2o/h2o-flow/

[23] Accord.NET Framework

[24] https://wordnet.princeton.edu

[25] https://www.ngdc.noaa.gov/hazard/earthqk.shtml

[26] www.keeptalkinggreece.com/2017/06/13/vrisa-the-ghost-village-lesvos-greece-earthquake/

This research was previously published in the International Journal of Interactive Communication Systems and Technologies (IJICST), 8(2); edited by Rosanna E. Guadagno; pages 13-35, copyright year 2018 by IGI Publishing (an imprint of IGI Global).

Chapter 4
TEEM:
Technology-Enhanced Emergency Management for Supporting Data Communication During Patient Transportation

Massimo Canonico
University of Piemonte Orientale, Italy

Stefania Montani
University of Piemonte Orientale, Italy

Diego Gazzolo
Neonatal Intensive Care Unit of Alessandria Children Hospital, Italy

Mariachiara Strozzi
Neonatal Intensive Care Unit of Alessandria Children Hospital, Italy

Manuel Striani
University of Turin, Italy

ABSTRACT

In this article, the authors describe a client-server architecture, designed for supporting data recording and transmission during emergency patient transportation by ambulance. The clients are a set of mobile apps, interfaced to the monitoring devices in the ambulance, that automatically send all the recorded data to a server at the destination center. One additional app enables the travelling personnel to input and transmit further significant patient data, or comments. At the destination center, the specialist physician logs onto the server, receives the data in real time, and is allowed to plot/analyze them, assessing the patient's situation, and possibly sending

DOI: 10.4018/978-1-7998-2535-7.ch004

immediate feedback to the operators in the ambulance. The system is currently under evaluation at the Neonatal Intensive Care Unit (NICU) of Alessandria Children Hospital, Italy. The system, by allowing real time data communication, is able to provide clear advantages from the organizational and economical viewpoint.

1. INTRODUCTION

Patients experiencing a medical emergency (e.g., stroke patients, pre-term born babies, or accident victims) are normally taken to the closest hospital structure. Peripheral hospitals might be insufficiently equipped, in terms of human or instrumental resources. In these situations, patients need to be stabilized, and then carried to a larger and more suitable health care center (i.e., a “hub” center), where specialized physicians, as well as more advanced diagnostic/therapeutic devices, are available.

During patient transportation by ambulance, a specialist physician (e.g., a neurologist) is typically not present; paramedics and/or emergency medicine doctors usually provide assistance. The travelling personnel continuously monitors the patient by means of proper devices available on the ambulance (such as a saturation meter, or a blood pressure monitor). However, the monitored data, at least in Italy, are not automatically recorded. Therefore, they cannot be inspected/analyzed a posteriori. Moreover, they are not accessible in real time by the specialist physician at the hub center. At most, the travelling personnel register a few key values on a paper log, and provide them to the specialist physician as soon as the ambulance arrives. However, information is necessarily partial and incomplete, and the specialist needs to re-asses the patient condition before starting the proper treatment.

In this paper, we propose a technological support to data communication and data access, during patient transportation by ambulance. Our approach is organized as a client-server architecture, where different mobile apps, running on smartphones/ tablets in the ambulance, act as clients, and send monitoring data to a server, residing at the hub center.

The architecture is composed of one different app for each monitoring device in the ambulance (e.g., the saturation meter), plus an additional app to send further data. The device apps have a very simple interface, just allowing the user to activate the connection to the server. Typically, the devices record a set of monitoring parameters in the form of time series, with a device-dependent sampling frequency; each app is adapted in order to be interfaced to a specific device. The additional app, meant to be manually adopted by the travelling personnel, has a more complete interface, which allows to introduce relevant patient data, not recorded by the machines (e.g., temperature), as well as comments and notes. This app also receives possible feedback from the specialist at the hub center.

The server component of the architecture receives the data sent by all the apps, and stores them in a database. It has a textual and graphical user interface, which enables the specialist physician to immediately visualize all the data received from the ambulance, and to assess the patient's situation in real time. Patient's assessment takes advantage of the possibility of reading/plotting the monitoring time series, and of running simple data analysis facilities (such as trend calculation). This allows the specialist physician to have a more complete understanding of the patient's situation already during transportation. In case of need, s/he is also able to communicate with the ambulance personnel and supervise the management of possible critical needs.

The architecture has been designed to be secure, but also extremely user friendly in the design of the interfaces, since both the travelling personnel and the expert physician at the hub center must not be distracted from more critical tasks (i.e., patient management).

As already observed, our approach not only supports real time communication, but also permits the users to store all monitoring data. Data availability over time is certainly fundamental for medico-legal purposes; moreover, monitoring data constitute a very useful source of operative knowledge, that can be exploited a posteriori, for a more complete patient characterization, or for comparison among different patients (e.g., for prediction goals, or for a global quality assessment of the medical center).

In its current implementation, the system has been specifically designed for pre-term born baby transportation (however, it could be easily adapted to different application domains as well), and it is currently under evaluation at the Neonatal Intensive Care Unit of Alessandria Children Hospital, Italy.

The paper is organized as follows: Section 2 describes the client-server architecture we have designed; Section 3 reports on evaluation results; finally, Section 4 presents concluding remarks, and delineates future work directions.

2. METHODS

In this section, we first illustrate related work; then, we describe the details of our architecture, referring to the client side (and thus to the device apps and to the operator app), and to the server side.

2.1. Related Work

Recently, architectures for storing and analyzing medical data in cloud computing (Li et al., 2013) have been proposed in combination with the usage of mobile devices, which allow the user to send/receive data in real time without any particular equipment and/or knowledge. This new computing paradigm is called Mobile Cloud Computing (MCC) (Fernando, Loke, & Rahayu, 2013) MCC integrates the cloud computing into the mobile environment and overcomes obstacles related to performance (e.g., battery life, storage, and bandwidth), environment (e.g., heterogeneity, scalability, and availability), and security (e.g., reliability and privacy) issues, discussed in mobile computing. In particular, the approaches in the research from Jin and Kwok, (2011), and Misra, Das, Khatua, and Obaidat (2014) deal with bandwidth issues. They propose solutions to share the limited bandwidth among mobile users. As for security/integrity/confidentiality issues, a classical solution (Zhou & Huang, 2013) consists of three main components: a mobile device, a web and storage service and a trusted third party. This third party is in charge of running a trusted crypto co-processor which generates a Message Authentication Code (MAC). Thanks to the MAC, every request from the user to read/write data on cloud storage is properly authenticated and, at any time, it is possible to validate the integrity of any file, collection of files or the whole file system stored in the cloud.

In our approach, we have adopted the technological solutions illustrated above.

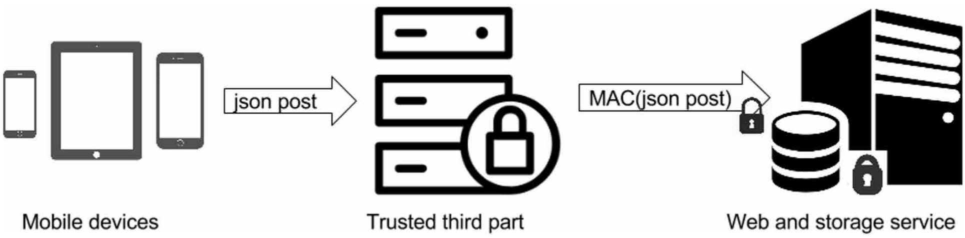
As regards the application domain of emergency patient transportation, a few apps addressing the problem are available. Among them, Stat (http://www.stat.com/about.html) allows the user to find the nearest idle ambulance with appropriate equipment to manage the emergency at hand. Stat currently operates in Philadelphia and Austin. Call Ambulance (http://timesofindia.indiatimes.com/city/jaipur/Calling-an-ambulance-to-get-easier-with-App/articleshow/50423415.cms) is a very recent app developed to support ambulance services in India. Through the app, the user obtains assistance in compiling her/his health and insurance records, and in sending them to a preferred hospital, which will then dispatch an ambulance. Flare (http://disrupt-africa.com/2016/07/kenyan-startup-to-launch-uber-for-ambulances-app/), to be deployed in Africa, allows patients and hospitals to see available ambulance options, and request help quickly. Ambulance Tasmania (http://www.ambulance.tas.gov.au/smartphone_apps) has also published a set of apps, to help callers in requesting emergency assistance, or to provide information about the caller's location to the emergency service organization.

Interestingly enough, these apps typically deal with ambulance dispatch, while, to the best of our knowledge, no previous contribution to support real time data transmission during ambulance transportation, and to maintain monitoring data over time, has been published.

2.2. System Architecture

To adopt MCC in our scenario, we had to address both low bandwidth issues from the mobile communication side, and security/integrity/confidentiality issues on

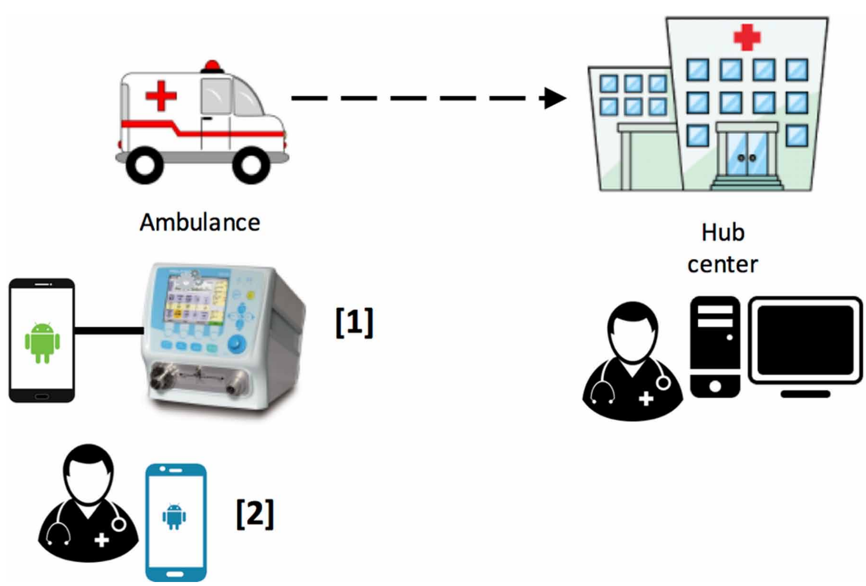
Figure 1. System architecture



storing medical data from the cloud computing side. To address bandwidth issues, we have resorted on the already cited approaches in (Jin & Kwok, 2011; Misra, Das, Khatua, & Obaidat, 2014), while for security/integrity/confidentiality issues, we have resorted to the three-component architecture described in (Zhou & Huang, 2013). Figure 1 illustrates the overall system architecture.

Our system is organized according to the client-server paradigm (see Figure 2), where different mobile apps, running on smartphones/tablets in the ambulance, act as clients, and send monitoring data to a server, residing at the hub center. The power supply for these devices is guaranteed by the various components (such as inverters/chargers, battery chargers and portable backup power products) able to supply constant power even when the vehicle (partly) breaks down or does not get to its destination.

Figure 2. Client server paradigm in the system



When the vehicle is in transit, the data transmission between client and server may incur in disconnections or low bandwidth availability. In order to overcome these problems, we have implement a solution based on TCP as the transmission protocol, since it provides mechanisms to detect network problems and to automatically re-transmit lost packets. Over TCP, we have also implement the techniques suggested in (Jin & Kwok, 2011; Misra, Das, Khatua, & Obaidat, 2014) in order to address bandwidth issues.

More specifically, the set of mobile apps we have implemented can be subdivided into two groups:

1. the device apps;
2. the operator app.

The device apps, directly connected to the medical monitoring devices in the ambulance (e.g., the saturation meter), are used by default, to send all the automatically recorded data to the server side. A smartphone or a tablet, physically connected to the medical monitoring device via RS-232, perform data transmission.

The operator app, where data have to be inserted manually by the personnel, is meant to be adopted only when:

- A medical monitoring device is not working or not available in the specific ambulance. In this case, monitoring data normally collected by the device can be entered manually, and the personnel is significantly helped in data entry, thanks to the availability of pre-defined value ranges and value correctness checks implemented in the operator app itself (see Section 2.3.2 for details);
- Additional data have to be provided, which are not measured by the medical devices (also in this case, data entry is facilitated by the supports and correctness checks illustrated in Section 2.3.2);
- Personnel wants to send textual notes and comments.
- Manual data entry is therefore possible, but is not used by default.
- The server side of the architecture, on the other hand, is based on three main components: (1) a web server (provided by Apache HTTP or Microsoft Windows Server) with (2) a PHP module enabled and (3) a database server (provided by MySQL). The following Sections illustrate all details.

2.3. Client Side: The Mobile Apps

2.3.1. Device Apps

Within our architecture, we have implemented a collection of device apps. Each device app is meant to be interfaced to a specific monitoring device, and is run on a smartphone or tablet, directly connected to the device via RS-232. Typically, the ambulance is equipped with three devices: Acutronic Medical System™ device for neonatal ventilation, Radical 7™ saturimeter, and Burke&Burke™ transportation cradle. The transportation cradle sends its monitoring data to the Acutronic Medical System™ device, therefore we have currently implemented one app for the Acutronic Medical System™ device and another one for the Radical 7™ saturimeter.

Figure 3 shows the Acutronic Medical System™ device; Figure 4 shows the Burke&Burke™ transportation cradle; Figure 5 shows the Radical 7™ saturimeter. In all pictures, our app, being used on a tablet, is also visible.

Figure 3. Acutronic Medical System™ device

Figure 4. Burke&Burke™ transportation cradle

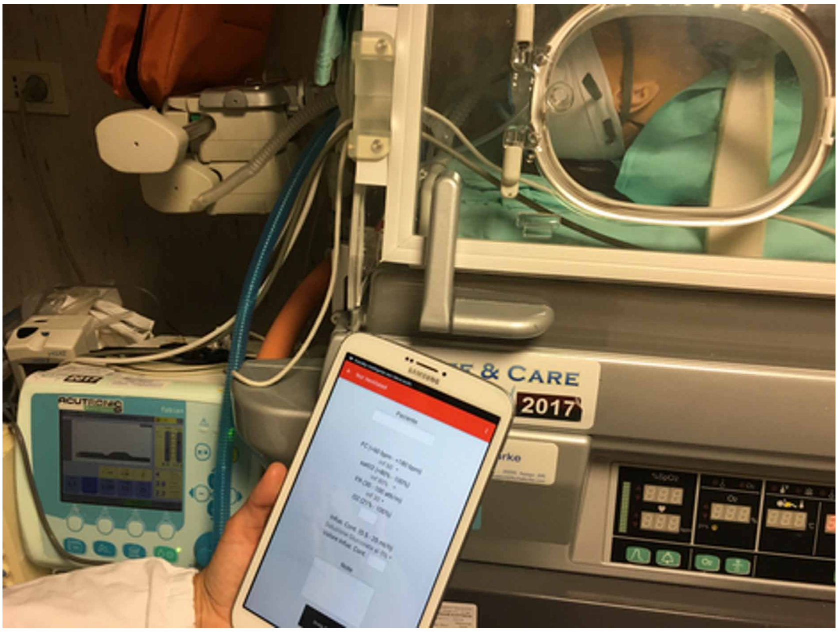


Figure 5. Radical 7™ saturimeter

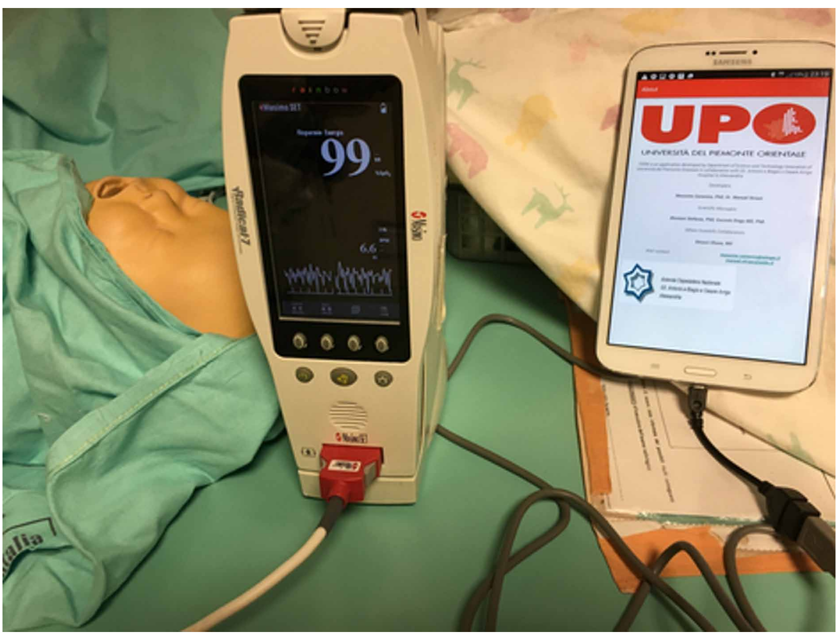


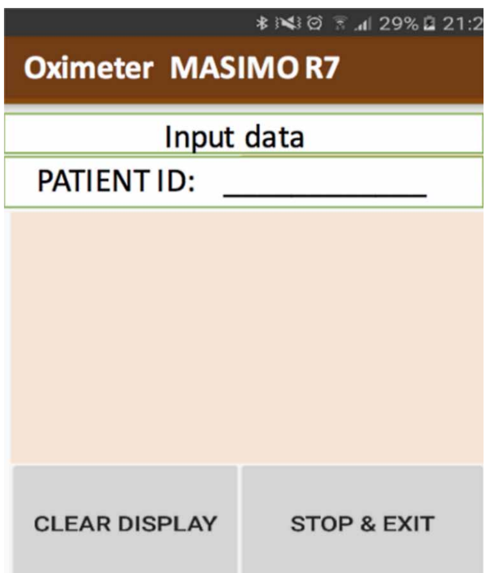
Figure 6. Acutronic Medical System RS-232 specifications

Type	RS-232, 9 Pin Sub D (female)
Pins:	Pin 2: TxD Pin 3: RxD Pin 5: Gnd
Note:	Hardware Handshake is not supported

Figure 7. Acutronic Medical System RS-232 settings

Typ	RS-232
Baudrate	38400 Baud
Parity	none
Stopbits	1
Data bits	8
Handshake	no

Figure 8. Interface of a device app



The only functionality of a device app is the one of reading the monitoring data produced by the device, and of sending them to the server. However, every device produces data in a different format, and requires transmission at a different baud rate (being the baud rate the number of distinct symbol changes - signaling events - made to the transmission medium per second in a digitally modulated signal). The various device apps are therefore very similar, but customized to the single device characteristics, in order to correctly read the data, correctly parse them, and correctly serialize them in a JSON string, to be posted to the server (see Figure 1).

As an example, the Acutronic Medical System™ devices for neonatal ventilation have a standard built-in RS-232 interface with no hardware or software flow control (handshaking). The serial port RS-232 has the specifications and settings illustrated in Figures 6 and 7. These settings are factory-provided and the user cannot adjust them.

The device app interface towards the ambulance personnel is extremely simple: it just allows the user to input the patient's identifier, and then to activate the connection towards the server side of the architecture. The data being sent are visualized in real time on the smartphone/tablet display (but no action is required to the user); the display can be cleared on demand by pressing a dedicated button; another dedicated button allows the operator to stop the data transmission and to exit the app (see Figure 8).

2.3.2. Operator App

Our architecture also provides the ambulance personnel with an additional app, meant to be directly used by the human operator. The operator app allows to input additional data with respect to the ones automatically sent by the device apps, or to substitute a device app in sending the information, if the device is not in use.

The operator app is obviously meant to be exploited in very critical situations, where the user has higher priorities with respect to data entry. Given these goals, the app has been designed to be very user friendly, very clear, and essential in its graphical design.

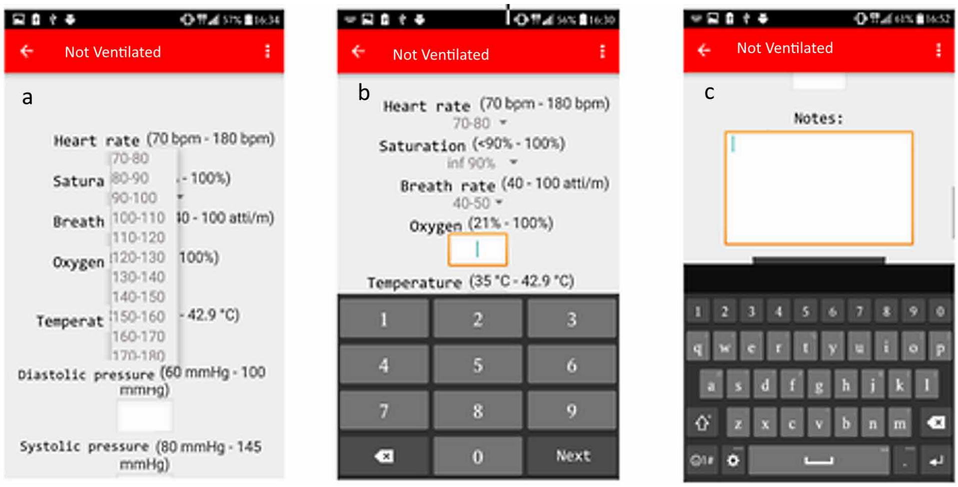
The parameters to be inputted have been selected by our medical collaborators, resorting to domain knowledge.

In particular, every data entry operation has been customized based on the type of parameter being inputted, in order to make it as fast and simple as possible, as illustrated in Figure 9. The figure presents three different activities of the operator app, which allow the user to input some data for a non-ventilated newborn patient transportation.

Figure 9(a) shows how to insert heart frequency. In our application domain, the exact value of heart frequency is not of interest: only the range needs to be specified. To this end, a set of pre-defined ranges are shown to the user, who will just have to choose one of them without digitizing any number. Pre-defined ranges have been defined, based on medical knowledge as well.

In the second activity (Figure 9[b]), the user inserts oxygen saturation. The admissibility range (21%-100%) is reminded to the user, but s/he has to insert a specific numeric value. To this end, a numeric keyboard is activated.

Figure 9. Snapshots of 3 activities in the operator app



It is worth noting that consistency controls are also executed in this case, since, obviously, transportation data always need to be correct. If the digitized number is outside the admissibility range, an error message will appear, in order to allow the user to introduce the correct value.

Finally, in the third case (Figure 9[c]), additional textual notes can be inserted. In this case, an alpha-numeric keyboard with auto-completion is activated.

When data have been sent to the server, the user is notified by a toast message, i.e., a notification message that shows for a few seconds and then fades away.

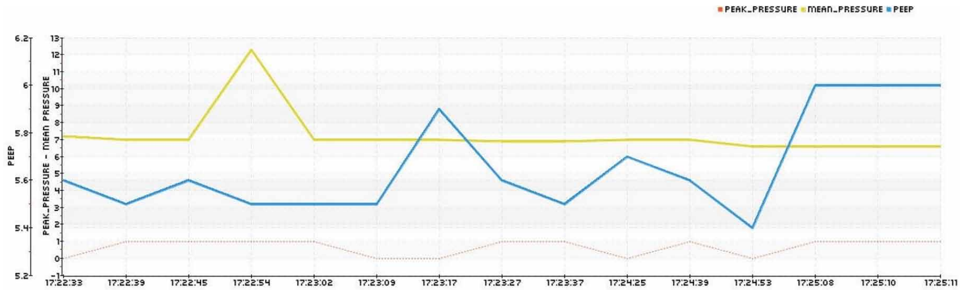
2.4. Server Side

The server side is based on three main components: (1) a web server (provided by Apache HTTP or Microsoft Windows Server) with (2) a PHP module enabled and (3) a database server (provided by MySQL). All components are very easy to install and configure (in Canonico, Montani, and Striani we provide all technical details for the sake of reproducibility of our system). Once the server-side components are up and running, the tool is ready to receive data from mobile devices.

All the data inputted through the mobile apps are serialized as a JSON string, which is posted to the server (see Figure 1). At the server side, data have then to be de-serialized, stored in the database, and shown to the user through a web interface.

The textual interface web page is automatically refreshed every five seconds, in order to always show the most recent data during transportation. Indeed, an updated measurement can be sent several times during the journey.

Figure 10. Parameter plotting on the server side

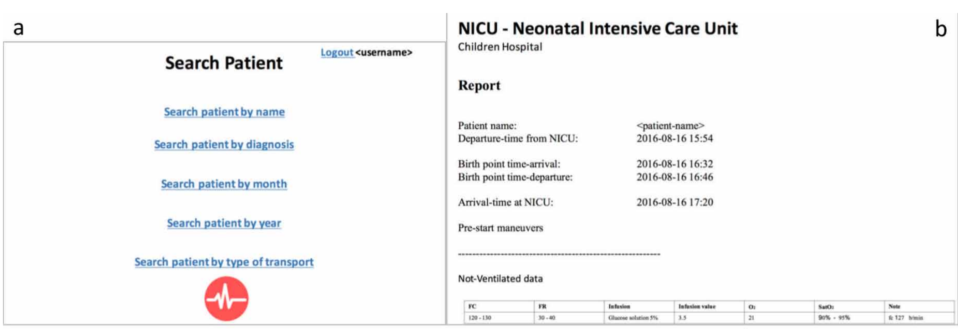


Upon the expert physician's request, some monitoring data can also be plotted, to be easily inspected by means of a graphical interface. Figure 10 shows, as an example, the plot of three parameters recorded by the neonatal ventilation device. Plots are automatically refreshed every five seconds as well.

As mentioned above, the data received from the apps are stored in a database, which maintains all the measured information over time. The advantages of this choice from the medico-legal viewpoint are obvious: indeed, by recording all monitoring data, we solve a very critical issue that affected patient transportation up to now, given that only a part of the data was logged on paper. In that way, monitoring information was often incomplete, and possibly incorrect. This critical limitation is overcome by the use of our system.

The immediate availability of monitoring data in the electronic format also allows physicians to have them accessible for data analysis, both during transportation, and a posteriori. Several ways to query the data (e.g., by patient, by diagnosis type, etc. – see Figure 11[a]) are provided to this end. An overall report of the transportation data can also be generated in pdf format (see Figure 11[b]).

Figure 11. Data querying and data report generation



By now, we have focused on the transportation phase, and we have provided the expert physician with a few, simple statistical facilities, such as trend calculation, to allow her/him to have clear indications on the patient's clinical conditions in real time. We will consider more complex analyses, able to predict the patient's clinical evolution, or to support therapeutic decisions, on the basis, e.g., of the comparison among similar patients, in our future work (see Section 4).

3. RESULTS

The client-server architecture described in this paper, in its current version, has been realized to monitor the transportation of pre-term born babies. The facility is currently under evaluation at the Neonatal Intensive Care Unit (NICU) of Alessandria Children Hospital, Italy. In the following, we quickly illustrate the application domain specificities, and present the results of the evaluation phase.

3.1. Pre-Term Born Baby Transportation

Pre-term born babies are very often critical patients, who need intensive care. If a baby is born at an insufficiently equipped hospital, s/he has to be moved to a hub center, equipped with a NICU (http://apps.who.int/iris/bitstream/10665/183037/1/9789241508988_eng.pdf?ua=1). Transportation may also be required if the baby, possibly already cared at the NICU, needs a specific intervention, that can be performed only at a larger or more specialized clinical center.

The clinical conditions of the baby to be transported may require ventilation assistance during the journey. Different types of mechanical ventilations exist, each of them relying on a specific device, and requiring specific parameter settings. Additional monitoring devices, such as the saturation meter, are also routinely adopted to track patient clinical conditions during the journey.

3.2. Evaluation Phase Results

The personnel of the NICU of Alessandria Children Hospital, Italy has currently been using our facility for six months. The NICU has 7 beds, and usually performs more than 150 transportations a year. During these first months of usage, the framework has always shown reliability and timeliness of data transmission from the client to the server side.

It is difficult to assess an improvement of clinical outcomes due to exploitation of our tool. Indeed, the number of patients being transported by the personnel of Alessandria is relatively small (47 in the period at hand); secondly, the majority of babies experienced very serious pathologies, whose effects cannot be easily mitigated just by a prompt and correct data transmission – which is important, but often not sufficient to ameliorate their clinical conditions.

On the other hand, we were able to identify a clear advantage from the organizational and economical viewpoint. In particular, knowing the details of the patient condition in real time (i.e., during transportation) allowed the NICU team an early and optimal bedside set-up, thus reducing the time-window for bedside preparation and the extra-costs in terms of un-needed equipment, such as respiratory support. Bearing in mind that the costs for a respiratory set for invasive/non-invasive ventilation can vary from 700 to 2000 euros, the capability of choosing the adequate equipment set-up permitted the NICU to avoid time and money waste. Specifically, in the period under examination, the NICU was able to save about 6000 euros.

3.3. System Usability

In addition to the impact on hospital practice from the economical and organizational viewpoint, we need to consider usability issues, in order to understand the real applicability of the proposed tool in day-by-day clinical work. Indeed, only a simple and user-friendly access to the provided functionalities can enable a regular adoption of the system in the long run, especially considering that it is meant to be exploited in very critical situations, where the user has higher priorities with respect to data entry. Usability considerations basically apply to the operator app, since the other apps are directly connected with the medical devices.

As already observed, the operator app was designed to be very clear, and essential in its graphical interface. In order to verify how this simplicity of use was actually perceived, we formally evaluated usability.

In our usability study, we first asked the NICU travelling personnel (three users) to execute three tasks by means of the operator app, namely:

1. Enter patient data that cannot be recorded by the medical devices;
2. Enter patient data that can be recorded by the medical devices (simulating the situation where a device is unavailable);
3. Enter a set of predefined additional comments and notes.

In the study, the users run the app first by means of a smartphone (LG Electronics G6) and then by means of a tablet (Samsung Galaxy Tab 3 7.0 3G T211 8GB).

Given the goals of the app, all tasks were obviously related to data input. We opted for laboratory experiments, since they are more indicated for testing data input mechanisms for mobile devices, with respect to field studies (Zhang & Adipat, 2005). Of course, more usability considerations might emerge after a longer routine field usage of the system: in this case, we will possibly define a revised version of the app, if needed.

In our usability study, in accordance to ISO 9241-11 standard, we aimed at measuring *effectiveness* (i.e., the ability of users to complete tasks using the system), *efficiency* (i.e., the level of resource consumed in performing tasks), and *satisfaction* (i.e., users' subjective reactions to using the system) (Zhang & Adipat, 2005; Brooke, 1996). The types of task carried out with the system obviously determine the measures of effectiveness and efficiency (Brooke, 1996).

In the case of the operator app, we could measure efficiency as task execution time. When working on the smartphone, average execution time was 36.98 seconds for task 1, 22.65 seconds for task 2 and 10.32 seconds for task 3. When using the tablet, average execution time was 22.02 seconds for task 1, 14.40 seconds for task 2 and 10.20 seconds for task 3.

We measured effectiveness as the reception of the inputted data at the server side (which were always correctly recorded in our study, with no errors).

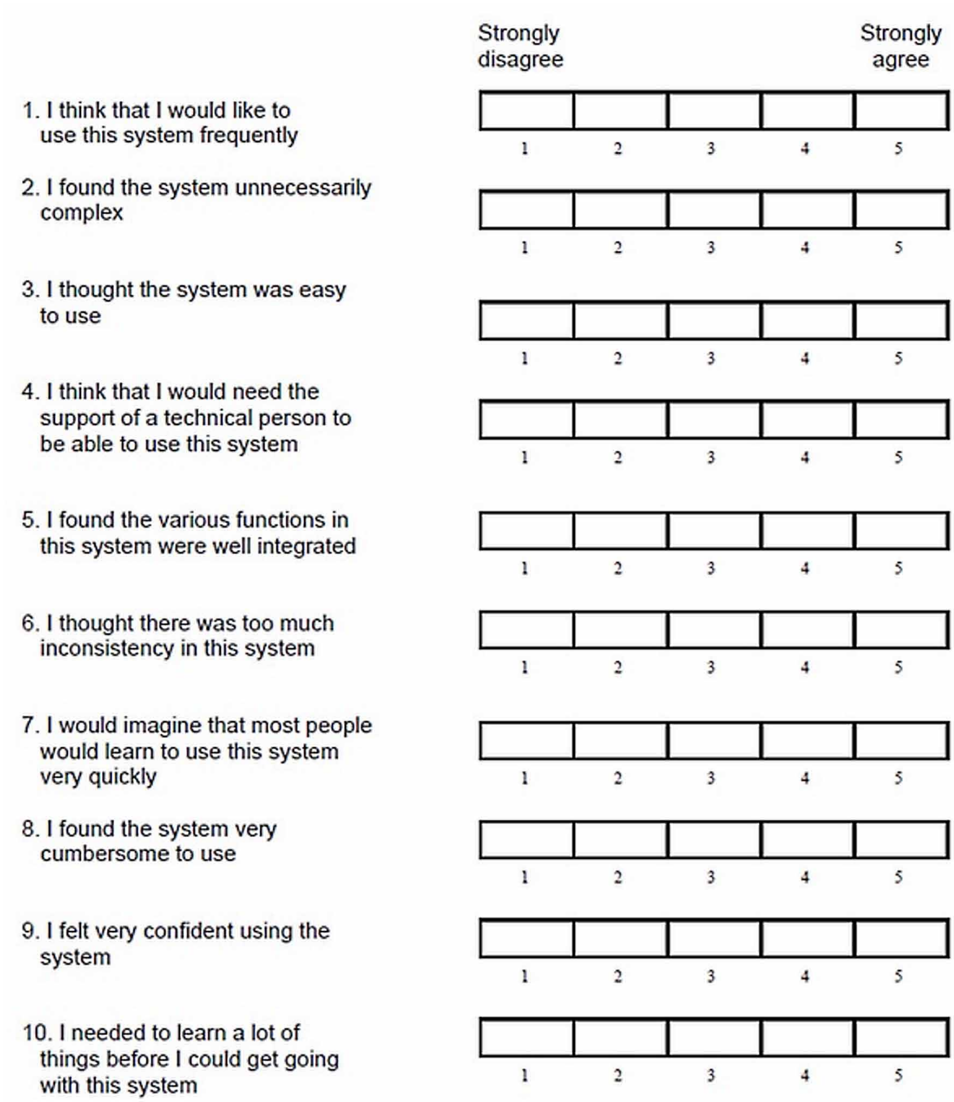
As regards satisfaction, we asked the users to compile the SUS usability questionnaire (Brooke, 1996). The SUS questionnaire, reported in Figure 12, is a simple, ten-item attitude Likert scale, giving a global view of subjective assessments of usability, by actually covering a variety of aspects, such as the need for support and training (*learnability*), and *complexity* (Zhang & Adipat, 2005). Specifically, questions 1, 2, 5, 6, 8 and 9 are basically aimed at measuring the perceived system complexity, while questions 3, 4, 7, 10 are mainly related to learnability.

The average scores registered in the questionnaire were very positive (top score was reached in 9 out of 10 questions), with the only exception of question 5, rated 4/5 by one of the user.

We also carried out an interview after task completion. Running the app on the tablet proved to be a bit easier (probably due to the larger monitor). Anyway, the users did not signal any particular difficulty in using the app. However, one of them provided two suggestions. One was about the opportunity of highlighting anomalous patient values by means of a red background. The second suggestion was not directly related to usability, since it was about allowing the insertion of some additional patient characterization data (namely, the "Transport Risk Index of Physiologic Stability" and the "Mortality Index for Neonatal Transportation" scores), not originally considered in the data input design. Both features have now been implemented in the operator app.

In synthesis, the users found the system easy to learn and to exploit, without requiring any previous experience, and without unnecessarily complex steps.

Figure 12. The SUS questionnaire (Brooke, 1996)



	Strongly disagree				Strongly agree
1. I think that I would like to use this system frequently	1	2	3	4	5
2. I found the system unnecessarily complex	1	2	3	4	5
3. I thought the system was easy to use	1	2	3	4	5
4. I think that I would need the support of a technical person to be able to use this system	1	2	3	4	5
5. I found the various functions in this system were well integrated	1	2	3	4	5
6. I thought there was too much inconsistency in this system	1	2	3	4	5
7. I would imagine that most people would learn to use this system very quickly	1	2	3	4	5
8. I found the system very cumbersome to use	1	2	3	4	5
9. I felt very confident using the system	1	2	3	4	5
10. I needed to learn a lot of things before I could get going with this system	1	2	3	4	5

4. CONCLUSION

In this paper we have described a client-server architecture, studied to support data communication and assessment during patient transportation by ambulance. The system resorts to a set of apps, which send all the monitoring data to a server at the destination center, thus substituting the extremely incomplete paper log typically deployed (in Italy) up to now. By means of this architecture, the expert physician can access and evaluate all the data, have a very clear picture of the patient's situation in real time, and thus start proper treatment as soon as the patient arrives at the hospital. Moreover, the system maintains all monitoring data over time. Interestingly, we are not aware of any other similar approach in the field of emergency patient transportation.

From the technological viewpoint, our choice has been the one of relying as much as possible on already available medical instruments, and on cheap data connection devices. Most medical instruments currently installed in ambulances, in fact, do not provide any data transmission capability, other than a RS-232 port for data download. We operate by fully resorting on such medical equipment for data monitoring, and on extremely diffused and cheap commercial devices for data transmission. In particular, we have opted for Android smartphones and tablets, being Android a recognized and hardware independent standard. Our apps are so light that they can run on these low-cost devices without requiring any specific hardware addition.

In our system, we guarantee confidentiality and privacy by adhering to existing Italian regulations (D.L. 196 30/6/2003). In particular, the system meets standard hospital procedures to protect patient privacy. These include the designation of a privacy officer to be responsible for developing and implementing all required policies and procedures; the restriction of access to electronic protected health information to only those employees who have a need for it to complete their job function; the control on access to computer systems. Patient data are maintained in the hospital database by using SQLite with SQLCiper (https://www.zetetic.net/sqlcipher/about/), an open source library that provides transparent and secure 256-bit AES encryption. With SQLCipher, an application exploits the standard SQLite API to manipulate tables using SQL. Behind the scenes the library silently manages the security aspects, making sure that data pages are encrypted and decrypted as they are written to and read from storage. Access to the software requires users to provide login/password information and is thus limited to authorized personnel. Finally, research on collected data can be conducted only after anonymizing them.

Our framework is currently in use at the NICU of Alessandria Children Hospital, Italy, where it has already provided organizational and economical improvements. The data available so far are not quantitatively sufficient to draw statistical tests. Indeed, the system has been used for a few months, and the number of patient transportations in our application domain is rather limited. A statistical study is foreseen as a future work, as soon as more deployment data will be collected.

We are making the apps available through Google Play Store. Obviously, the apps are customized to the specific hospital needs, and, in order to be used, backend configuration is needed. Therefore, even though, in line of principle, the apps will be downloadable by any hospital (and a technical note providing details for the backend configuration is provided in [Canonico, Montani, & Striani]), we are currently resorting to Google Play Store basically to facilitate and accelerate the installation of newer versions of the apps by all the Alessandria NICU personnel. However, we will consider customization for different hospitals in the future.

We also plan to extend our work along different additional directions.

As regards the operator app, we will take into account voice-based communication, as a more user-friendly approach with respect to manual data entry. Indeed, since the traveling personnel must not be distracted from critical tasks during patient transportation by ambulance, we plan to replace the manual data insertion of the operator app by exploiting the speech recognition API library available for Android. In particular, Google Cloud Speech (GCS) (https://cloud.google.com/speech/?gclid=CLKyq7HWqNACFRG6GwodbPIE7A) enables to convert audio to text by applying powerful neural network models in an API. With GCS, the traveling personnel can dictate data concerning the patient health without typing anything. Moreover, all data dictated can be sent to the server by using a vocal command.

As for the server side, on the other hand, we would like to enrich the data analysis capabilities of the tool. Up to now, we have focused on real time support during the transportation phase, but more complex (and possibly time-consuming) analyses, not well suited for the emergency phase, may be useful a posteriori. In particular, the clinical conditions of a specific patient may be compared to the ones of other patients in the database: similar patients may have similar outcomes, or may require similar therapies. Indeed, we plan to exploit the transportation database as a source of experiential knowledge, and adopt it as the knowledge base of a Case-Based Reasoning (CBR) (Aamodt & Plaza, 1994) tool. CBR is an artificial intelligence methodology, which takes advantage of past experience, and retrieves past situations similar to the current one, to get advice on the current problem solution. The current solution may be built by reusing or adapting the solutions of the retrieved examples. Our application could certainly benefit of this approach, even though it requires the treatment of non-trivial issues, such as representation and comparison of data in the form of time series. We will therefore consider time series comparison, and, more generally, time series analysis, in our future work too, resorting both to classical mathematical transforms, such as the Discrete Fourier Transform (Agrawal, Faloutsos, & Swami, 1993), and to more advance artificial intelligence techniques, such as Temporal Abstractions (Shahar, 1997). Temporal Abstractions are a knowledge-based approach to time series dimensionality reduction and interpretation, which operate by converting consecutive points, sharing a common behavior persistent over time, into a single interval, mapped to a symbol, which identifies the behavior at hand. Temporal Abstractions have already been adopted in CBR systems, particularly when dealing with medical applications (Montani & Portinale, 2006; Montani, Leonardi, Bottrighi, Portinale, & Terenziani, 2013).

Note that patient comparison can also be useful to assess the overall quality of care in a given medical center, identifying similarities as well as outlying situations.

As a further step, we plan to integrate the data collected by means of our tool within the Electronic Patient Record (EPR) of the hospital. This improvement is along the lines discussed in (Martinelli et al., 2011) - however, it is worth noting that, in (Martinelli et al., 2011), transportation data were integrated in the EPR, but had to be inputted manually in the system at the end of the transportation: they were not automatically recorded in real time.

Finally, we will integrate our work within a larger telemedicine project, which will enable the specialist physician at the hub center to supervise the stabilization process as well, before patient transportation begins. Patient stabilization will take place at the peripheral hospital, but the specialist physician at the hub center will constantly help the local physicians. Communication will be made possible and very quick by exploiting the recent paradigm called Fog Computing (Shane et al., 2015) which will enable the transmission of several types of data, including patient videos recorded by webcams and streaming media. Concerning the server side, many techniques able to implement the server consolidation (Anglano, Canonico, & Guazzone, 2015) and energy savings (Albano, Anglano, Canonico, & Guazzone, 2013) can be applied in our system in order to improve efficiency and usability. We believe that the overall telemedicine project will really enhance the quality of care of emergency patients, regardless of the location of their initial admission.

ACKNOWLEDGMENT

This research is original and has a financial support of the University of Piemonte Orientale. On behalf of all authors, the corresponding author states that there is no conflict of interest.

REFERENCES

Aamodt, A., & Plaza, E. (1994). Case-based reasoning: Foundational issues, methodological variations, and system approaches. *AI Communications*, *7*(1), 39–59.

Agrawal, R., Faloutsos, C., & Swami, A. (1993). Efficient similarity search in sequence databases. In *Proceedings of the International Conference on Foundations of Data Organization and Algorithms* (pp. 69-84). 10.1007/3-540-57301-1_5

Albano, L., Anglano, C., Canonico, M., & Guazzone, M. (2013). Fuzzy-Q&E: achieving QoS guarantees and energy savings for cloud applications with fuzzy control. In *Proc. of the 3*rd *International Conference on Cloud and Green Computing (CGC 2013)*. 10.1109/CGC.2013.31

Ambulance Tasmania. (2016). Smartphone Apps. Retrieved November 8 2016 from http://www.ambulance.tas.gov.au/smartphone_apps

Anglano, C., Canonico, M., & Guazzone, M. (2015). FC2Q: Exploiting Fuzzy Control in Server Consolidation for Cloud Applications with SLA Constraints. *Concurrency and Computation*, *27*(17), 4491–4514. doi:10.1002/cpe.3410

Brooke, J. (1996). SUS: a "quick and dirty" usability scale. In *P. W. Jordan, B. Thomas, B. A. Weerdmeester, & A. L. McClelland (Eds.), Usability Evaluation in Industry*. London: Taylor and Francis.

Canonico, M., Montani, S., & Striani, M. (2016). Supporting data communication and patient assessment during emergency transportation (Technical Report TR-INF-2016-09-03-UNIPMN). DiSIT, Computer Science Institute Universita del Piemonte Orientale.

Fernando, N., Loke, N. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. *Future Generation Computer Systems*, *29*(2), 84–106. doi:10.1016/j.future.2012.05.023

Google. (2016). Cloud speech API. Retrieved November 8 2016 from https://cloud.google.com/speech/?gclid=CLKyq7HWqNACFRG6GwodbPIE7A

Jackson, T. (2016). Kenyan startup to launch "Uber for ambulances" app. Disrupt Africa. November 8 2016 http://disrupt-africa.com/2016/07/kenyan-startup-to-launch-uber-for-ambulances-app/

Jin, X., & Kwok, Y. K. (2011). Cloud assisted P2P media streaming for bandwidth constrained mobile subscribers. In *Proceedings of the 16th IEEE International Conference on Parallel and Distributed Systems (ICPADS).*

Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Transaction on Parallel and Distributed Systems*, *24*(1).

Martinelli, S., Vergani, P., Zanini, R., Bellù, R., Farina, C, & Tagliabue, P. (2011). Transport as a system: reorganization of perinatal assistance in Northern Lombardy. *The Journal of Maternal-Fetal and Neonatal Medicine*, *24*(1), 122-125.

Misra, S., Das, S., Khatua, M., & Obaidat, M. S. (2014). QoS-Guaranteed Bandwidth Shifting and Redistribution in Mobile Cloud Environment. *Transactions on Cloud Computing*, *2*(2), 181–193. doi:10.1109/TCC.2013.19

Montani, S., Leonardi, G., Bottrighi, A., Portinale, L., & Terenziani, P. (2013). Supporting flexible, efficient and user-interpretable retrieval of similar time series. *IEEE Transactions on Knowledge and Data Engineering*, *25*(3), 677–689. doi:10.1109/TKDE.2011.264

Montani, S., & Portinale, L. (2006). Accounting for the temporal dimension in Case-based retrieval: A framework for medical applications. *Computational Intelligence*, *22*(3-4), 208–223. doi:10.1111/j.1467-8640.2006.00284.x

Montani, S., Portinale, L., Leonardi, G., Bellazzi, R., & Bellazzi, R. (2006). Case-based retrieval to support the treatment of end stage renal failure patients. *Artificial Intelligence in Medicine*, 37(1), 3731–3742. PMID:16213692

Shahar, Y. (1997). A Framework for Knowledge-Based Temporal Abstraction. *Artificial Intelligence*, *90*(1-2), 79–133. doi:10.1016/S0004-3702(96)00025-2

Stat.com. (2016). About. Retrieved November 8 2016 from http://www.stat.com/about.htmlccessed

Times of India. (2016). Calling an ambulance to get easier with App. Retrieved November 8 2016 from http://timesofindia.indiatimes.com/city/jaipur/Calling-an-ambulance-to-get-easier-with-App/articleshow/50423415.cms

WHO. (2015). WHO recommendations on interventions to improve preterm birth outcomes. Retrieved September 22nd 2016 from http://apps.who.int/iris/bitstream/10665/183037/1/9789241508988_eng.pdf?ua=1

Yi, S., Li, C., & Li, Q. (2015). A Survey of Fog Computing: Concepts, Applications and Issues. In *Proceedings of the Workshop on Mobile Big Data*. ACM.

Zetetic. (2016). About. Retrieved November 8 2016 from https://www.zetetic.net/sqlcipher/about/

Zhang, D., & Adipat, B. (2005). Challenges, Methodologies, and Issues in the Usability Testing of Mobile Applications. *International Journal of Human-Computer Interaction*, *18*(3), 293–308. doi:10.120715327590ijhc1803_3

Zhou, Z., & Huang, D. (2013). Efficient and Secure Data Storage Operations for Mobile CloudComputing. In *Proceedings of the 8th International Conference on Network and Service Management*.

This research was previously published in the International Journal of Mobile Computing and Multimedia Communications (IJMCMC), 8(4); edited by Agustinus Waluyo; pages 49-65, copyright year 2017 by IGI Publishing (an imprint of IGI Global).

Chapter 5
Live Video Communication in Prehospital Emergency Medicine

Camilla Metelmann
Greifswald University, Germany

Bibiana Metelmann
Greifswald University, Germany

ABSTRACT

Prehospital emergency medicine treats time-critical diseases and conditions and aims to reduce morbidity and mortality. The progression of emergency medicine is an important topic for governments worldwide. A problem occurs when paramedics need assistance at the emergency site by emergency doctors, who cannot be present. Video-communication in real-time from the emergency site to an emergency doctor offers an opportunity to enhance the quality of emergency medicine. The core piece of this study is a video camera system called "LiveCity camera," enabling real-time high quality video connection of paramedics and emergency doctors. The impact of video communication on emergency medicine is clearly appreciated among providers, based upon the extent of agreement that has been stated in this study's questionnaire by doctors and paramedics. This study was part of the FP7-European Union funded research project "LiveCity" (Grant Agreement No. 297291).

DOI: 10.4018/978-1-7998-2535-7.ch005

INTRODUCTION

Prehospital emergency medicine is a crucial part of all health care systems worldwide. The goal of emergency medicine is to treat time-critical diseases or conditions and thus reduce preventable disabilities and deaths. Citizens often judge their government by the quality of critical infrastructure regarding for instance security and emergency medicine (Hsia, Razzak, Tsai, & Hirshon, 2010; Razzak & Kellermann, 2002). One approach to further improve emergency medicine is to balance existing healthcare disparities by using telemedicine (Brokmann et al. 2015). Telemedicine are ICTs (information and communication technologies) in medicine enabling diagnostics and treatment of diseases over geographical distances (Kazley, McLeod, & Wager, 2012; WHO, 2011).Telemedicine is an important future topic as described in the "Global Observatory for eHealth" by the World Health Organization, and the implementation of telemedicine is one of the goals of the European Union (Economic and Social Committee, 2008; WHO, 2011). Telemedicine devices, using a high-definition video communication in realtime, offer the highest amount of information-transfer currently available (Metelmann & Metelmann, 2016).

This chapter is based on findings of the FP7- European Union funded research project LiveCity (Grant Agreement No. 297291). The LiveCity Project studied how high-definition video communication in real time can positively contribute to the quality of life of citizens or communities within the European Union in many different areas (Chochliouros, Stephanakis, Spiliopoulou, Sfakianakis, & Ladid, 2012; Weerakkody, El-Haddadeh, Chochliouros, & Morris, 2012). A special video camera, called "LiveCity camera" was developed to connect the different providers of emergency medicine in the European Union - the paramedics at the emergency site and a (remote) emergency doctor.

This chapter focuses on the impact of video communication on prehospital emergency medicine. In the first part the medical emergency systems worldwide and in Germany in particular are introduced, followed by a paragraph on the use of telemedicine in emergency medicine and the concept of a tele emergency doctor. In the next section the methodology of the study is described with information regarding the "LiveCity camera". A selection of results is presented. The discussion reflects on the results and how governments worldwide could benefit from implementing telemedicine in prehospital emergency medicine. Finally conclusions are drawn concerning the impact of video communication on emergency medicine.

BACKGROUND OF STUDY

Medical Emergency System Worldwide

Medical emergency systems are different constitutively or to some extent in every country worldwide (T. E. Callese et al., 2015). Sometimes even within one country there are different emergency systems, for example China had seven different emergency systems in 2007 (Huiyi, 2007). In some countries the urban areas can provide a higher developed system than rural areas (Vaitkaitis, 2008). And in many low- and middle-income-countries the existing emergency systems are used only insufficiently (Choi et al., 2017). To categorize the variety of systems four different types might be differentiated: (a) no organized structure, (b) basic life support, (c) advanced life support with paramedics and (d) advanced life support with physicians(Roudsari et al., 2007).

(a) Some developing countries in Sub-Saharan Africa or parts of Asia have no organized prehospital emergency system, for example Malawi (Chokotho et al., 2017). However in line with population growth, urbanization and industrialization there is an ongoing shift from infectious diseases towards medical conditions like cardiovascular diseases and vehicle accidents. Due to medical reasons this calls for a higher need of medical emergency systems (Suryanto, Plummer, & Boyle, 2017; WHO, 1996). One approach to improve the quality of emergency medicine in those countries is to teach volunteers of the community high quality first aid (Chokotho et al., 2017).

(b) Basic life support works without trained medical professionals at the emergency site and focuses on fast transport to a hospital and keeping the patient alive during transport, which is for instance the case in Kenya (Nielsen et al., 2012). Advanced life support systems in comparison work on a more sophisticated level of care at the emergency site and during the transport to a hospital, but depend upon well-educated and medically qualified providers (Roudsari et al., 2007).

(c) Advanced life support with paramedics as single providers at the emergency site is also called the Anglo-American model. It was developed in the United States of America (Wandling, Nathens, Shapiro, & Haut, 2016) and is also used e.g. in Ireland (Masterson et al., 2015), the United Kingdom (Clawson et al., 2017), Australia (Nehme, Andrew, Bernard, & Smith, 2014), Singapore (Lateef, 2006), and the Netherlands (Dib, Naderi, Sheridan, & Alagappan, 2006).

(d) Advanced life support with paramedics working together with physicians at the emergency site is called Franco-German model (Al-Shaqsi, 2010). It is for example used in Germany (Luiz, Dittrich, Pollach, & Madler, 2017), Finland (Kupari, Skrifvars, & Kuisma, 2017), Israel (Ellis & Sorene, 2008), Brazil (Timerman, Gonzalez, Zaroni, & Ramires, 2006), and in the urban areas of Lithuania (Vaitkaitis, 2008).

The main difference between the two advanced life support models is that the Anglo-American model brings the patient to the doctor and in the Franco-German model the doctor is brought to the patient (Dick, 2003).

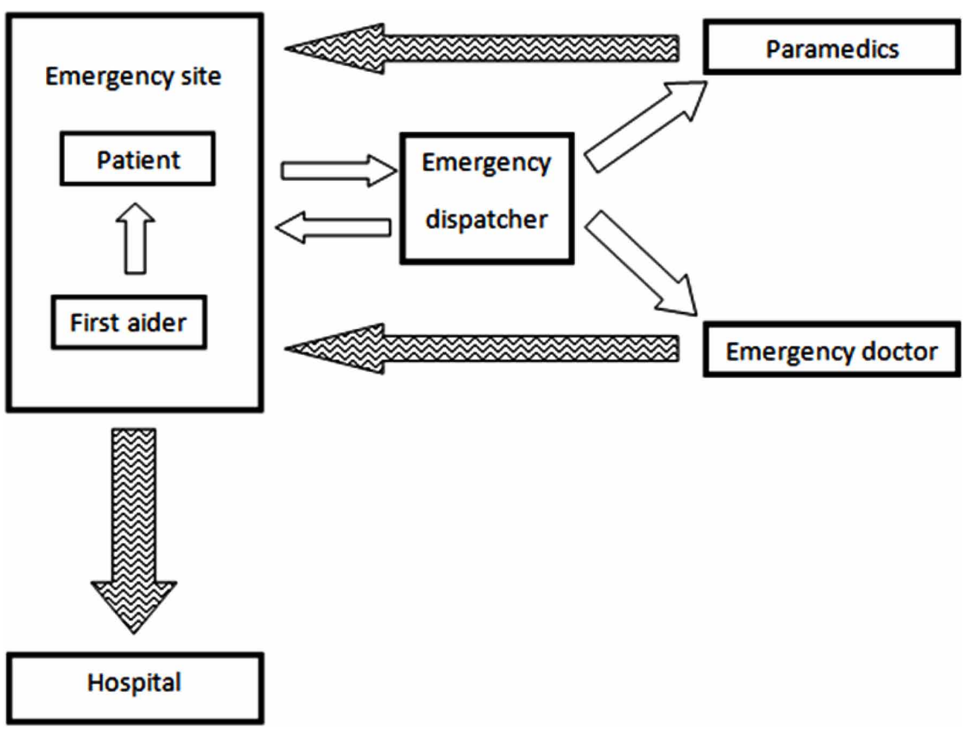
Medical Emergency System in Germany

The German Medical Emergency System as an example of the Franco-German model is a dual system with two partners, i.e. paramedics and emergency doctors (Harding et al., 2013). Paramedics receive a one- to three-year education in handling emergency situations (Becker, Hündorf, Kill, & Lipp, 2006). Emergency doctors are medical doctors with a special training in intensive care medicine and qualification in emergency medicine(Bundesärztekammer, 2011b).

Figure 1 shows the pathway of a patient, who experiences an emergency and alerts the medical emergency system.

The emergency call is answered by the emergency dispatcher, who will assess all relevant details. Based on that, the dispatcher will alert the paramedics and additionally an emergency doctor in cases of (potentially) life-threatening conditions.

Figure 1. Pathway of medical emergency system in Germany



Approximately only one out of three to one out of four emergency situations require an emergency doctor (Roessler & Zuzan, 2006).

Because the paramedics are alerted in every emergency, there are more paramedics than emergency doctors. This allows a wider geographical spread of paramedics, which places the paramedics closer to potential sites of emergencies. The paramedics and the emergency doctors approach the emergency with different cars and meet only at the emergency site(DeutscherBundestag17.Wahlperiode, 2010; Schmiedel & Behrendt, 2011). This allows a high flexibility and leads to a substantial decrease in the time it takes for the first team of emergency personnel to arrive at the emergency site(Ellinger, 2011). Every federal state government in Germany is obliged by law to organize the required infrastructure for the emergency personnel to arrive within a predefined time(Becker et al., 2006; Binder, 1993). On average the paramedics in Germany arrive at the emergency site after 8.7 minutes and the emergency doctor after 12.3 minutes (Schmiedel & Behrendt, 2011).

At the emergency site doctor and paramedics establish a preliminary diagnosis and start the treatment. The treatment could be either completed at the emergency site, so that the patient can be left at home, which is the case in approximately 5% (Schmiedel & Behrendt, 2011). Or the patient has to be brought to the hospital. The transport of the patient to the hospital is done by the paramedics, often together with the emergency doctor. Once the patient is in the hospital, the hospital staff will continue the diagnostics and treatment and the paramedics and emergency doctor return to their different bases becoming available for the next emergency patient.

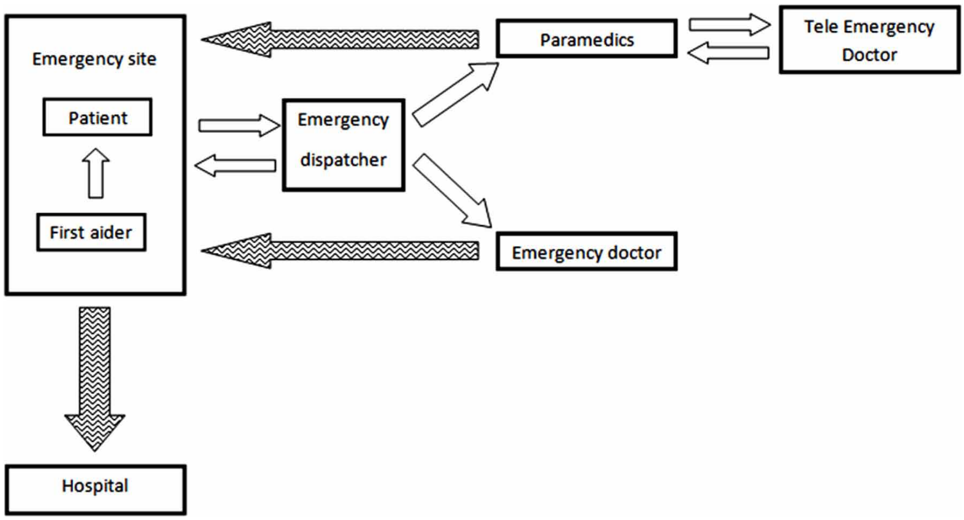
Tele Emergency Doctor

There are special situations, when this system could benefit from support by telemedicine, e.g. by a tele emergency doctor. Figure 2 is introducing a tele emergency doctor as an auxiliary partner. The tele emergency doctor is an emergency doctor with special training, who works from a central dispatch place distant from the emergency site. The paramedics can get in contact with the doctor via telemedicine.

Telemedicine offers an opportunity to balance uneven allocation of infrastructure and resources including human resources (Sood et al., 2007). It has huge advantages in emergency medicine, where the transfer of knowledge in short time is critical and potentially lifesaving (Amadi-Obi, Gilligan, Owens, & O'Donnell, 2014).

Telemedicine looks especially promising and supportive, when paramedics are without an emergency doctor at the emergency site but would like to consult one. The absence of the emergency doctor could have several reasons. For example, as mentioned above, in general the emergency doctor arrives at the emergency site some minutes after the paramedics. Although in most cases, this is just a short time, in life-threatening situations, these early minutes are especially crucial. Another

Figure 2. Pathway of medical emergency system in Germany with addition of a tele emergency doctor



reason might be that in the initial assessment the severe extent of the emergency was not identifiable, so that the emergency dispatcher only alerted the paramedics. And in some emergencies the situation can worsen very quickly and unexpectedly, so that it develops into a situation, where an emergency doctor would be needed. Additionally there are emergencies, which are not life-threatening, but in which paramedics would like to have guidance by an emergency doctor. Those situations might be, for example, rare diseases or special circumstances, e.g. difficulties during pregnancy.

In all situations, in which paramedics are without an emergency doctor at the emergency site, but would like to consult one, telemedicine might be the solution. The prerequisite for that is that there is a real time connection for live communication between the paramedics and the tele emergency doctor.

For this contact to be efficient, helpful and according to legal regulations in medicine, the distant consultation has to transport more information than a mere telephone call can perform. The "Model Professional Code for Physicians in Germany" obligates physicians to an individual and direct treatment of patients also in telemedicine(Bundesärztekammer, 2011a; Katzenmeier & Schrag-Slavu, 2010).

Several different concepts of tele emergency doctors are currently under study or already implemented. One example is Telenotarzt in Aachen, Germany, where an ambulance car is equipped with a video camera, which sends high-definition videos in real-time to the tele emergency doctor. This concept was implemented as part of the medical emergency system in the city of Aachen in April 2014 (Felzen et al., 2016)(Brokmann et al. 2016a; Brokmann et al. 2016b; Brokmann et al. 2017a; Brokmann et al. 2017b)(Stevanovic et al. 2017). Based on these findings the tele emergency concept will be implemented and further analyzed within the project Land|Rettung in the northern part of Germany. Another progressive project is PreSSUB in Brussels, Belgium (Yperzeele et al. 2014; Valenzuela Espinoza et al. 2017; Valenzuela Espinoza et al. 2016a; Valenzuela Espinoza et al. 2016b).

METHODOLOGY

LiveCity Camera

The central communicational device in this study is a special video camera with software and hardware newly developed by LiveCity Project-partners in Greece, Portugal and Ireland (Goncalves, Cordeiro, Batista, & Monteiro, 2012; Palma et al., 2013). This camera enables a video connection via internet in real time. The emergency doctor gives instructions based on all the information he got, observes the realization of the instructions, evaluates the actions and improves them, if needed. Hence a time lag is a huge hindrance and can result in such a poor communication, that no meaningful assistance by the emergency doctor is possible. At the same time the high legal standards regarding data security have to be met.

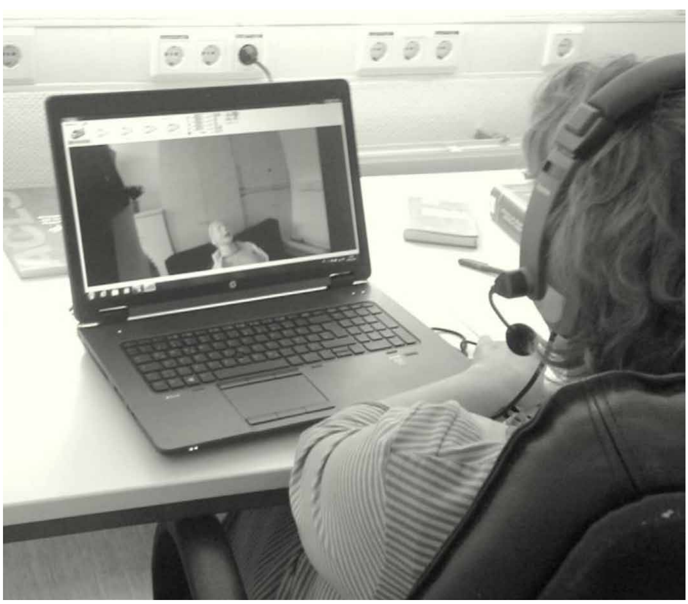
Figure 3. The LiveCity camera worn by a paramedic

The LiveCity camera as shown in figure 3 consists of the video-camera itself, worn with a headband above the right ear, a headphone with mouthpiece to enable audio connection in both ways and a microPC, which builds the internet connection. The position of the camera above the right ear was chosen to transmit the same perspective the paramedic has to the emergency doctor. The transmitted video is dynamic and follows the head movements of the paramedics. One major advantage of the position of the camera is also, that the paramedic still has both hands free to work.

Software of the LiveCity Camera

The transmitted video is received by the remote emergency doctor at a laptop provided with special software (Figure 4). This software allows the emergency doctor to adapt the transmitted video according to the particular needs, e.g. regarding light, contrast and sound level. A snapshot can be taken by the emergency doctor at any time and is a high definition photo transmitted independently from the video. Because of the high pixel count it allows the emergency doctor to analyze for instance a 12-lead-ECG in detail, where tiny elevations of lines can indicate a myocardial infarction. Because the interpretation of 12-lead-ECG is sometimes very challenging and needs a lot of experience, some authors state, that physicians have a higher success rate in detecting e.g. a heart attack than paramedics have (D. P. Davis et al., 2007).

Figure 4. Tele emergency doctor observing emergency site via LiveCity camera



Study Design

The aim of the study was to assess the impact of video communication on emergency medicine. The benefit of paramedics consulting a tele emergency doctor by use of the LiveCity camera was investigated in terms of professional work flow and outcome. To prevent potential harm for individuals the study was performed in the fully equipped medical simulation center of the Department of Anesthesiology at Greifswald University Medicine (Figure 5). A medical simulation center creates dynamic realistic routine or emergency scenarios with aid of computer-operated mannequins (Johannsson, Ayida, & Sadler, 2005). It is widely used in medicine for educational and research purposes (Cannon-Diehl, 2009; Kyle & Murray, 2010; Levine, DeMaria, Schwartz, & Sim, 2013).

Figure 5. Paramedics at the emergency site treating a "patient" in the simulation center by use of LiveCity camera

To evaluate the co-operation of paramedics and doctors close to reality, ten typical emergency scenarios from five different categories were standardized and structured for a randomized two-armed protocol. These categories are: “Trauma”, “Heart attack”, “Stroke”, “Rare diseases” and “Complications during pregnancy”. For each category two cases with similar level of difficulty in terms of diagnosis and treatment were created to allow a cross-over design. Cross-over design was achieved by comparing the results and opinions of paramedics in action at the simulated emergency site: (a) *without* doctor´s support and (b) the same paramedics in corresponding cases another time *with* video-based consultation and contact to a tele emergency doctor. According to usual guidelines in German emergency medicine two paramedics worked together as a team. The sequence of the case scenarios and the assignment to the two cross-over categories was randomized.

To assess the outcome in practical, technical and psychological aspects, paramedics and doctors were interviewed by use of structured questionnaires developed together with the Department for Medical Psychology, Greifswald University Medicine.

RESULTS

10 emergency doctors and 21 paramedics took part in a total of 110 simulated emergency scenarios. All participants (n =31) accomplished every scenario and completed all questionnaires. These are the results of the investigation in terms of “disagree”, “partly disagree”, “partly agree” or “agree” (ranked on a 4-point Likert scale) or concerning “yes” or “no” questions in the following sentences of the questionnaires:

“The scenarios were realistic.”

Considering the total number of 10 emergency doctors, 1 partly disagreed, 5 partly agreed, 4 agreed. Considering the total number of 21 paramedics, 1 partly disagreed, 11 partly agreed and 9 agreed. No emergency doctor or paramedic disagreed (Table 1).

Table 1.

	Agree	Partly agree	Partly disagree	Disagree
Doctors (10)	4	5	1	0
Paramedics (21)	9	11	1	0

Table 2.

	Agree	Partly agree	Partly disagree	Disagree
Doctors (10)	7	3	0	0
Paramedics (21)	14	7	0	0

Table 3.

	Diagnostics/Treatment	Practical/Manual	undecided
Paramedics (21)	13	6	2

Table 4.

	Agree	Partly agree	Partly disagree	Disagree
Paramedics (21)	15	6	0	0

Table 5.

	Yes	No
Paramedics (21)	14	7

"The scenarios were relevant."

Considering the total number of 10 emergency doctors, 3 partly agreed, 7 agreed. Considering the total number of 21 paramedics, 7 partly agreed,14 agreed. No emergency doctor or paramedic disagreed or partly disagreed (Table 2).

"What kind of support would you especially like to get in an emergency situation?"

The paramedics were asked to choose between "help with practical and manual skills" or "help with diagnostics and treatment". 6 of 21 paramedics wished for practical or manual help. 13 of 21 paramedics wished for help with diagnostics and treatment. 2 paramedics could not decide (Table 3).

"I consider the tele emergency doctor as helpful."

Considering the total number of 21 paramedics, 6 partly agreed and 15 agreed. No paramedic disagreed or partly disagreed (Table 4).

"Would you call a tele emergency doctor in cases you wouldn't normally call an emergency doctor?"

Considering the total number of 21 paramedics, 14 answered "yes" and 7 answered "no" (Table 5).

Table 6.

	Agree	Partly agree	Partly disagree	Disagree
Doctors (10)	3	7	0	0
Paramedics (21)	13	8	0	0

Table 7.

	Agree	Partly agree	Partly disagree	Disagree
Doctors (10)	3	6	1	0
Paramedics (21)	9	11	1	0

Table 8.

	Yes	No
Doctors (10)	2	8

Table 9.

	Yes	No
Doctors (10)	2	8

Table 10.

	Agree	Partly agree	Partly disagree	Disagree
Doctors (10)	4	5	1	0
Paramedics (21)	16	4	1	0

"A tele emergency doctor improves the quality of patient care."

Considering the total number of 10 emergency doctors, 7 partly agreed and 3 agreed. Considering the total number of 21 paramedics, 8 partly agreed and 13 agreed. No emergency doctor or paramedic disagreed or partly disagreed (Table 6).

"I perceive that the tele emergency doctor leads to a faster start of the therapy."

Considering the total number of 10 emergency doctors, 9 agreed (3 fully and 6 partly). 1 doctor disagreed partly, but no one to full extent. Of the paramedics, 20 of 21 agreed, in comparison more fully (11) than partly (9). 1 paramedic partly disagreed (Table 7).

"Is transmission of the vital signs without audio or video connection sufficient?"

Only emergency doctors were asked, 8 of 10answered "no" and 2 of 10 "yes" (Table 8).

"Is transmission of the vital signs with additional audio connection sufficient?"

Again only emergency doctors were asked, and again 8 of 10 answered "no" and 2 of 10 "yes" (Table 9).

"I can imagine working in a tele emergency doctor system."

Of the emergency doctors 9 of 10 agreed to the summarizing sentence of the study, 4 to full extent and 5 partly. Among the paramedics 16 of 21 agreed and 4 of 21 partly agreed. 1 paramedic and 1 emergency doctor partly disagreed (Table 10).

DISCUSSION

The impact of video communication on emergency medicine is very welcome among providers, based upon the amount of agreement of paramedics and emergency doctors in this study to a video-based consultation at the emergency site. This is an approach to increase quality of emergency treatment by applying telemedicine. The core piece of the concept is a special video camera, called LiveCity camera.

External Validity of the Study

As Ammenwerth and coworkers have explained, there are three ways of testing a new health information technology. The first way is to evaluate it in a laboratory. But the results are limited by a low external validity. The second way is a field evaluation test, but for this both software and hardware have to be sufficiently mature to not possibly harm any person. So the solution is often the middle way: a simulation study, which combines good internal and external validity (Ammenwerth et al., 2012).

Simulation studies offer the opportunity to conduct experimental cross-over trials with high internal validity. The external validity depends on how realistic the simulated scenarios are. The perception of how realistic a scenario in a simulation center is, is influenced by three different aspects: the equipment fidelity, the environment fidelity and the psychological fidelity(Fritz, Gray, & Flanagan, 2008). The equipment fidelity is characterized by the used hard- and software. In the LiveCity Project the Laerdal mannequin Resusci Anne was used and the vital signs were dynamically simulated with the monitor iSimulate. The environment fidelity is mostly created by the appropriate surrounding for every scenario. In the LiveCity Project every scenario had different characteristic accessories, e.g. in one case of simulated heart attack a patient was watching sports sitting on a sofa with a football flag while eating potato crisps. Psychological fidelity is the ability of the individual participant to immerse into the simulated situation. Psychological fidelity can be increased by enhancing equipment and environment fidelity (Bauman, 2013).

After finishing all scenarios all participants were asked, if they perceived the simulated cases as realistic. The majority of both emergency doctors and paramedics rated the scenarios as realistic. Thus, the possibility of the participants behaving in the study environment similar to their normal behavior is high. This implies a good external validity.

Relevance of the Selected Medical Emergencies

Furthermore, all emergency doctors and paramedics partly agreed or agreed that the chosen scenarios were relevant. This is also an indicator for a good external validity. To reflect the broad spectrum of emergencies, different scenarios were developed. The categories "Trauma", "Heart attack" and "Stroke" were chosen, because they belong to the "First Hour Quintet". This term was coined by the sixth European Resuscitation Council Meeting in Florence, Italy in 2002 and describes five emergencies, which are life-threatening diseases in which a fast treatment reduces morbidity and mortality (Krafft et al., 2003; Nilsen, 2012). Worldwide they belonged to the group of top 10 leading causes of death in 2004 and prognosis for 2030 predict them to be within the top 5 leading causes of death worldwide (WHO, 2010). Thus there are many approaches to improve the therapy, e.g. by telemedicine. The implementation of telemedicine in stroke treatment was recommended by the American Heart Association and American Stroke Association in 2009 (Schwamm et al., 2009). "Rare diseases" and "Complications during pregnancy" are a special challenge in medicine. Often there are no standard operating procedures and the paramedics might not have encountered a similar situation before, which increases the stress level. Another aspect in pregnancy is that the unborn child has to be considered, too e.g. in the application of drugs to manage the emergency. Therefore a video consultation of a tele emergency doctor might be helpful.

Since all paramedics and emergency doctors confirmed that the chosen scenarios were realistic and relevant, the simulation appears to be a suitable model and the findings of the LiveCity study might – at least partly – be transmitted from the simulation center into the existing medical emergency system.

Wish for Telemedical Support

To further assess the need for a tele emergency doctor, the paramedics, were asked, what kind of support they usually would like to get in a "normal" emergency. More than 2/3 of all paramedics answered, that they would want assistance in diagnostics and therapy. Because telemedicine enables the transfer of knowledge, this is the main area, where the tele emergency doctor can support.

One of the main purposes of the tele emergency doctor concept is that the emergency doctor supports and helps the paramedics at the emergency site by providing expertise (Czaplik et al., 2014). After completing all 10 scenarios in the LiveCity Project, all paramedics rated the tele emergency doctor as helpful. Hence they confirmed that knowledge can be transferred via telemedicine to the emergency site. This concept of the tele-consultation via video might be also expanded into other fields of emergency medicine. For example emergency doctors with limited experience, who are at the emergency site, might want to get support by a more experienced emergency doctor. Since some emergencies only occur rarely, the young emergency doctor might not have encountered a similar situation before (Gries, Zink, Bernhard, Messelken, & Schlechtriemen, 2006). And young emergency doctors often have a huge awareness of the responsibility they have and feel the difference between working in a hospital, where help by senior doctors is within reach and being the only doctor at the emergency site (Groos, 2011). Thus the young emergency doctor might also perceive an experienced tele emergency doctor as helpful.

Another advantage of the tele emergency doctor is that support by an emergency doctor is easily accessible without the expensive mobilization of many resources. Additionally this tele emergency support starts without time delay the moment the telemedicine connection is built. In the current German medical emergency system, the paramedic calls the emergency dispatcher, who then alerts the emergency doctor. The "normal" emergency doctor would now start to travel to the emergency site. This whole procedure takes some time, which directly leads to a later start of transport to the hospital. As explained earlier, this time difference could be crucial. Thus paramedics are more likely, to call an emergency doctor. This would presumable lead to a higher quality of emergency medicine.

Impact on Quality of Patient Care

Paramedics and emergency doctors were asked to rank the impact of a tele emergency doctor on the quality of patient care. All participants agreed or partly agreed that the tele emergency doctor improves the quality of patient care. Bashshur stated in 2002, that telemedicine has the potential to solve the existing problems in geographical differences in access to high standard medical care and might balance the uneven quality of care (Bashshur, 2002).So the improvement of patient care by the tele emergency doctor might be also used to enhance quality of diagnostics and therapies in geographical areas, where a high standard couldn't be achieved before. It would be very interesting to test the concept of a tele emergency doctor in countries outside of the European Union as well, which have not the medical emergency system of "advanced life support", but "basic life support" or "no organized structure". In these systems the transfer of expertise is even more important and can increase the quality of patient care immensely. Roughly 90% of all trauma-related death worldwide occur in low- and middle-income countries (Debenham, Fuller, Stewart, & Price, 2017). In these countries most trauma-related fatalities happen in the prehospital phase and some could be preventable through appropriate prehospital care (Anand, Singh, & Kapoor, 2013). The World Health Organization has published a manual in 2005 how prehospital trauma care management worldwide could be improved(Sasser, Varghese, Kellermann, & Lormand, 2005). One concept for countries without an organized medical emergency system or with a low-grade medical emergency system was to teach volunteer citizens principles of basic life support. These volunteers could then work together to improve the prehospital care. One of the problems in teaching laypersons, who had not received a medical education before, is the low level of literacy(Tyler E. Callese et al., 2014). Therefore there is a need for special curricula, which uses the existing resources. A review by Callese and coworkers showed that trained volunteers can reduce the mortality after trauma. If the volunteers could get help by a remote emergency doctor via telemedicine, this could lead to an even higher increase in quality of care.

As mentioned above, rapid start of treatment in an emergency is crucial. It is also often used as an indicator for the quality of the medical emergency system (DeutscherBundestag17.Wahlperiode, 2010). One demand on telemedicine therefore is to not delay the therapy. As Rogers and coworkers presented, the implementation of a tele emergency doctor can decrease the time to start of therapy (Rogers et al., 2017). In the development of the LiveCity camera huge emphasis was put on reducing the time needed to build the connectivity. After working with the LiveCity camera the majority of paramedics and emergency doctors partly agreed or agreed that they perceived, that this tele emergency doctor concept leads to an earlier start of therapy. It can be concluded for the LiveCity camera that the early availability of medical expertise regarding diagnostics and therapy leads to such an early start of therapy, that it can outbalance any delay due to technical reasons.

SPECIFIC CHALLENGES

As a consequence, one might argue, that reducing the technical complexity to a minimum might lead to a faster data transmission and thus to an earlier start of therapy. Additionally a complex system is often more failure-prone and requires a more stable and superior internet connection. To assess the possibility to eliminate expandable features, the emergency doctors were consulted, what information was necessary to evaluate the specific emergency situation. 80% of emergency doctors stated, that the sole transmission of vital signs (blood pressure, heart rate, oxygen saturation) would not have been enough. And even the addition of an audio connection would have not been enough for 80% of the emergency doctors to sufficiently treat the emergency patient. This means, that the telemedicine devise also needs to transmit video to enable the tele emergency doctor to successfully support the paramedics.

Despite great promises of telemedicine, the implementation of telemedicine projects into the existing medical systems is a huge challenge (Iakovidis, Maglavera, & Trakatellis, 2000; Zailani, Gilani, Nikbin, & Iranmanesh, 2014). Some very promising telemedicine projects were not as widely implemented as expected (Bont und Bal 2008). The reason for that is studied worldwide and several "enablers", e.g. well-working technology and training of the users, as well as "barriers", e.g. technical problems and lack of technical support, were discussed (Wade, Eliott, & Hiller, 2014). One main factor for successful implementation of telemedicine is a good acceptance of the idea and device by the users, e.g. doctors (Rho, Choi, & Lee, 2014). (Brewster et al. 2014). Wade and coworkers stated that acceptance by clinicians is the most important key factor and that if clinicians supported the telemedicine project, various technical problems were tolerated (Wade et al., 2014). The technology acceptance model (TAM) by Davis was applied to telemedicine and it could be shown that both the perceived usefulness and the perceived ease of use are significantly associated with the intention to use the system (F. D. Davis, 1989; Dünnebeil, Sunyaev, Blohm, Leimeister, & Krcmar, 2012; Kowitlawakul, 2011; Rho et al., 2014). In the LiveCity Project an impressive majority of emergency doctors and paramedics agreed, that they could imagine working in a tele emergency doctor system.

FUTURE OUTLOOK

This concept to transfer knowledge in real time through video communication to distant places can improve the quality of medical emergency systems. With the arrival of the first members of the medical emergency team at the emergency site, a high quality in diagnostics and treatment can be achieved. This leads to an earlier beginning of high quality medicine. Polls among citizens showed that the timely access to high quality medical care was rated as the most important quality feature of a health care system (Soroka, 2007). The perceived achievement of this goal, influences the appraisal of the current government and the wish for political change (Soroka, 2007). It is essential, that the implementation of telemedicine in prehospital emergency medicine is in direct collaboration with the government. In the German county Vorpommern-Greifswald the project Land|Rettung introduces a tele emergency doctor into the existing emergency system. The project is coordinated by the county government. There will be a scientific evaluation of medical, economically and organizational aspects to allow a transferability to other counties and regions.

To achieve the highest benefit of a video consultation in emergency medicine, policy makers worldwide should adapt the concept according to the existing medical emergency system of their specific country.

CONCLUSION

A common problem in emergency medicine worldwide is the lack of support by emergency doctors, when paramedics are at the emergency site without emergency doctors but need their assistance or back up. This chapter shows aim an approach to increase quality of emergency treatment by applying telemedicine. The core piece is a video camera system, enabling real time connection of paramedics and emergency doctors by high quality video. Emergency doctors and paramedics tested the work flow and outcome of this kind of communication in a medical simulation center with aid of computer-operated mannequins.

A structured questionnaire confirmed that, the majority of paramedics and emergency doctors considered the tele emergency doctor system (i) as helpful and (ii) an improvement regarding quality of patient care and could (iii) imagine working in a tele emergency doctor system. The impact of video communication on emergency medicine is clearly appreciated among providers, based upon the extent of agreement that has been stated in this study by doctors and paramedics. Thus, the concept of a video consultation of an emergency doctor is a good addition to the existing medical emergency system in Germany and the idea could be integrated into other medical emergency systems worldwide as well to enhance the quality of emergency medicine. Governments and policy makers play an integral role in introducing the benefits of live video communication in prehospital emergency medicine to their specific medical systems.

ACKNOWLEDGMENT

The present article has been structured in the context of the LiveCity ("Live Video-to-Video Supporting Interactive City Infrastructure") European Research Project and has been supported by the Commission of the European Communities - DG CONNECT (FP7-ICT-PSP, Grant Agreement No.297291).

REFERENCES

Al-Shaqsi, S. (2010). Models of International Emergency Medical Service (EMS) Systems. *Oman Medical Journal*, *25*(4), 320–323. doi:10.5001/omj.2010.92 PMID:22043368

Amadi-Obi, A., Gilligan, P., Owens, N., & O'Donnell, C. (2014). Telemedicine in pre-hospital care: A review of telemedicine applications in the pre-hospital environment. *International Journal of Emergency Medicine*, *7*(1), 29. doi:10.118612245-014-0029-0 PMID:25635190

Ammenwerth, E., Hackl, W. O., Binzer, K., Christoffersen, T. E., Jensen, S., Lawton, K., ... Nohr, C. (2012). Simulation studies for the evaluation of health information technologies: Experiences and results. *The HIM Journal*, *41*(2), 14–21. doi:10.1177/183335831204100202 PMID:22700558

Anand, L. K., Singh, M., & Kapoor, D. (2013). Prehospital trauma care services in developing countries. *Anaesthesia, Pain & Intensive Care*, *17*(1), 65.

Bashshur, R. L. (2002). Chapter 1: Telemedicine and health care. *Telemedicine Journal and e-Health*, *8*(1), 5–12. doi:10.1089/15305620252933365 PMID:12020402

Bauman, E. B. (2013). *Game-based Teaching and Simulation in Nursing and Healthcare*. Springer Publishing Company.

Becker, J., Hündorf, H-P., Kill, C., & Lipp, R. (2006). *Lexikon Rettungsdienst*. Stumpf + Kossendey Verlag.

Binder, G. (1993). *Hilfsfrist. In Rechtsbegriffe in der Notfallmedizin* (pp. 38–38). Springer Berlin Heidelberg. doi:10.1007/978-3-642-52350-2_38

Bundesärztekammer. (2011). *Übersicht Notarztqualifikation in Deutschland*. Retrieved from www.bundesaerztekammer.de

Callese, T. E., Richards, C. T., Shaw, P., Schuetz, S. J., Issa, N., Paladino, L., & Swaroop, M. (2014). Layperson trauma training in low- and middle-income countries: A review. *The Journal of Surgical Research*, *190*(1), 104–110. doi:10.1016/j.jss.2014.03.029 PMID:24746252

Callese, T. E., Richards, C. T., Shaw, P., Schuetz, S. J., Paladino, L., Issa, N., & Swaroop, M. (2015). Trauma system development in low- and middle-income countries: A review. *The Journal of Surgical Research*, *193*(1), 300–307. doi:10.1016/j.jss.2014.09.040 PMID:25450600

Cannon-Diehl, M. R. (2009). Simulation in healthcare and nursing: State of the science. *Critical Care Nursing Quarterly*, *32*(2), 128–136. doi:10.1097/CNQ.0b013e3181a27e0f PMID:19300077

Chochliouros, I., Stephanakis, I., Spiliopoulou, A., Sfakianakis, E., & Ladid, L. (2012). Developing Innovative Live Video-to-Video Communications for Smarter European Cities. In L. Iliadis, I. Maglogiannis, H. Papadopoulos, K. Karatzas, & S. Sioutas (Eds.), *Artificial Intelligence Applications and Innovations* (Vol. 382, pp. 279–289). Springer Berlin Heidelberg. doi:10.1007/978-3-642-33412-2_29

Choi, S. J., Oh, M. Y., Kim, N. R., Jung, Y. J., Ro, Y. S., & Shin, S. D. (2017). Comparison of trauma care systems in Asian countries: A systematic literature review. *Emergency Medicine Australasia*, *29*(6), 697–711. doi:10.1111/1742-6723.12840 PMID:28782875

Chokotho, L., Mulwafu, W., Singini, I., Njalale, Y., Maliwichi-Senganimalunje, L., & Jacobsen, K. H. (2017). First Responders and Prehospital Care for Road Traffic Injuries in Malawi. *Prehospital and Disaster Medicine*, *32*(1), 14–19. doi:10.1017/S1049023X16001175 PMID:27923422

Clawson, J. J., Gardett, I., Scott, G., Fivaz, C., Barron, T., Broadbent, M., & Olola, C. (2017). Hospital-Confirmed Acute Myocardial Infarction: Prehospital Identification Using the Medical Priority Dispatch System. *Prehospital and Disaster Medicine*, 1–7. doi:10.10171049023x1700704x PMID:29223194

Czaplik, M., Bergrath, S., Rossaint, R., Thelen, S., Brodziak, T., Valentin, B., ... Brokmann, J. C. (2014). Employment of telemedicine in emergency medicine. Clinical requirement analysis, system development and first test results. *Methods of Information in Medicine*, *53*(2), 99–107. doi:10.3414/ME13-01-0022 PMID:24477815

Davis, D. P., Graydon, C., Stein, R., Wilson, S., Buesch, B., Berthiaume, S., ... Leahy, D. R. (2007). The positive predictive value of paramedic versus emergency physician interpretation of the prehospital 12-lead electrocardiogram. *Prehospital Emergency Care*, *11*(4), 399–402. doi:10.1080/10903120701536784 PMID:17907023

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *Management Information Systems Quarterly*, *13*(3), 319–340. doi:10.2307/249008

Debenham, S., Fuller, M., Stewart, M., & Price, R. R. (2017). Where There is No EMS: Lay Providers in Emergency Medical Services Care - EMS as a Public Health Priority. *Prehospital and Disaster Medicine*, *32*(6), 593–595. doi:10.1017/S1049023X17006811 PMID:28797317

Deutscher Bundestag 17. Wahlperiode. (2010). *Bericht über Maßnahmen auf dem Gebiet der Unfallverhütung im Straßenverkehr 2008 und 2009 (Unfallverhütungsbericht Straßenverkehr 2008/2009)*. Author.

Dib, J. E., Naderi, S., Sheridan, I. A., & Alagappan, K. (2006). Analysis and applicability of the Dutch EMS system into countries developing EMS systems. *The Journal of Emergency Medicine*, *30*(1), 111–115. doi:10.1016/j.jemermed.2005.05.014 PMID:16434351

Dick, W. F. (2003). Anglo-American vs. Franco-German emergency medical services system. *Prehosp Disaster Med, 18*(1), 29-35.

Dünnebeil, S., Sunyaev, A., Blohm, I., Leimeister, J. M., & Krcmar, H. (2012). Determinants of physicians' technology acceptance for e-health in ambulatory care. *International Journal of Medical Informatics*, *81*(11), 746–760. doi:10.1016/j.ijmedinf.2012.02.002 PMID:22397989

Economic and Social Committee, Section for Transport, Energy, Infrastructure and the Information Society. (2008). Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society COM(2008) 689 final. Brussels: Author.

Ellinger, K. (2011). *Kursbuch Notfallmedizin: orientiert am bundeseinheitlichen Curriculum Zusatzbezeichnung Notfallmedizin*. Dt. Ärzte-Verlag.

Ellis, D. Y., & Sorene, E. (2008). Magen David Adom—The EMS in Israel. *Resuscitation*, *76*(1), 5–10. doi:10.1016/j.resuscitation.2007.07.014 PMID:17767990

Felzen, M., Brokmann, J. C., Beckers, S. K., Czaplik, M., Hirsch, F., Tamm, M., ... Bergrath, S. (2016). Improved technical performance of a multifunctional prehospital telemedicine system between the research phase and the routine use phase - an observational study. *Journal of Telemedicine and Telecare*. doi:10.1177/1357633x16644115 PMID:27080747

Fritz, P. Z., Gray, T., & Flanagan, B. (2008). Review of mannequin-based high-fidelity simulation in emergency medicine. *Emergency Medicine Australasia*, *20*(1), 1–9. doi:10.1111/j.1742-6723.2007.01022.x PMID:17999685

Goncalves, J., Cordeiro, L., Batista, P., & Monteiro, E. (2012). LiveCity: A Secure Live Video-to-Video Interactive City Infrastructure. In L. Iliadis, I. Maglogiannis, H. Papadopoulos, K. Karatzas, & S. Sioutas (Eds.), *Artificial Intelligence Applications and Innovations* (Vol. 382, pp. 260–267). Springer Berlin Heidelberg. doi:10.1007/978-3-642-33412-2_27

Gries, A., Zink, W., Bernhard, M., Messelken, M., & Schlechtriemen, T. (2006). Realistic assessment of the physican-staffed emergency services in Germany. *Der Anaesthesist*, *55*(10), 1080–1086. doi:10.100700101-006-1051-2 PMID:16791544

Groos, H. (2011). *Du musst die Menschen lieben: Als Ärztin im Rettungswagen, auf der Intensivstation und im Krieg*. Fischer E-Books.

Harding, U., Lechleuthner, A., Ritter, M. A., Schilling, M., Kros, M., Ohms, M., & Bohn, A. (2013). „Schlaganfall immer mit Notarzt?" – „Pro". *Medizinische Klinik, Intensivmedizin und Notfallmedizin*, *108*(5), 408–411. doi:10.100700063-012-0137-7 PMID:23010854

Hsia, R., Razzak, J., Tsai, A. C., & Hirshon, J. M. (2010). Placing emergency care on the global agenda. *Annals of Emergency Medicine*, *56*(2), 142–149. doi:10.1016/j.annemergmed.2010.01.013 PMID:20138398

Huiyi, T. (2007). *A Study on Prehospital Emergency Medical Service System Status in Guangzhou*. Hong Kong: University of Hong Kong.

Iakovidis, I., Maglavera, S., & Trakatellis, A. (2000). *User Acceptance of Health Telematics Applications: Education and Training in Health Telematics*. IOS Press.

Johannsson, H., Ayida, G., & Sadler, C. (2005). Faking it? Simulation in the training of obstetricians and gynaecologists. *Current Opinion in Obstetrics & Gynecology*, *17*(6), 557–561. doi:10.1097/01.gco.0000188726.45998.97 PMID:16258334

Katzenmeier, C., & Schrag-Slavu, S. (2010). *Einführung. In Rechtsfragen des Einsatzes der Telemedizin im Rettungsdienst* (Vol. 2, pp. 1–22). Springer Berlin Heidelberg. doi:10.1007/978-3-540-85132-5_1

Kazley, A. S., McLeod, A. C., & Wager, K. A. (2012). Telemedicine in an international context: Definition, use, and future. *Advances in Health Care Management*, *12*, 143–169. doi:10.1108/S1474-8231(2012)0000012011 PMID:22894049

Kowitlawakul, Y. (2011). The technology acceptance model: Predicting nurses' intention to use telemedicine technology (eICU). *Computers, Informatics, Nursing*, *29*(7), 411–418. doi:10.1097/NCN.0b013e3181f9dd4a PMID:20975536

Krafft, T., Garcia Castrillo-Riesgo, L., Edwards, S., Fischer, M., Overton, J., Robertson-Steel, I., & Konig, A. (2003). European Emergency Data Project (EED Project): EMS data-based health surveillance system. *European Journal of Public Health*, *13*(3Suppl), 85–90. doi:10.1093/eurpub/13.suppl_1.85 PMID:14533755

Kupari, P., Skrifvars, M., & Kuisma, M. (2017). External validation of the ROSC after cardiac arrest (RACA) score in a physician staffed emergency medical service system. *Scandinavian Journal of Trauma, Resuscitation and Emergency Medicine*, *25*(1), 34. doi:10.118613049-017-0380-2 PMID:28356134

Kyle, R., & Murray, W. B. (2010). *Clinical Simulation*. Elsevier Science.

Lateef, F. (2006). The emergency medical services in Singapore. *Resuscitation*, *68*(3), 323–328. doi:10.1016/j.resuscitation.2005.12.007 PMID:16503277

Levine, A. I., DeMaria, S., Schwartz, A. D., & Sim, A. J. (2013). *The Comprehensive Textbook of Healthcare Simulation*. Springer. doi:10.1007/978-1-4614-5993-4

Luiz, T., Dittrich, S., Pollach, G., & Madler, C. (2017). Kenntnisstand der Bevölkerung über Leitsymptome kardiovaskulärer Notfälle und Zuständigkeit und Erreichbarkeit von Notrufeinrichtungen. *Der Anaesthesist*, *66*(11), 840–849. doi:10.100700101-017-0367-4 PMID:29046934

Masterson, S., Wright, P., O'Donnell, C., Vellinga, A., Murphy, A. W., Hennelly, D., ... Deasy, C. (2015). Urban and rural differences in out-of-hospital cardiac arrest in Ireland. *Resuscitation*, *91*, 42–47. doi:10.1016/j.resuscitation.2015.03.012 PMID:25818707

Metelmann, B., & Metelmann, C. (2016). M-Health in Prehospital Emergency Medicine: Experiences from the EU funded Project LiveCity. In M. Anastasius (Ed.), *M-Health Innovations for Patient-Centered Care* (pp. 197–212). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-9861-1.ch010

Nehme, Z., Andrew, E., Bernard, S., & Smith, K. (2014). The impact of partial resuscitation attempts on the reported outcomes of out-of-hospital cardiac arrest in Victoria, Australia: Implications for Utstein-style outcome reports. *Resuscitation*, *85*(9), 1185–1191. doi:10.1016/j.resuscitation.2014.05.032 PMID:24914831

Nielsen, K., Mock, C., Joshipura, M., Rubiano, A. M., Zakariah, A., & Rivara, F. (2012). Assessment of the Status of Prehospital Care in 13 Low- and Middle-Income Countries. *Prehospital Emergency Care*, *16*(3), 381–389. doi:10.3109/10903127.2012.664245 PMID:22490009

Nilsen, J. E. (2012). *Improving quality of care in the Emergency Medical Communication Centres (EMCC).* Paper presented at the Konferanse for medisinsk nødmeldetjeneste, Sola, Norway.

Palma, D., Goncalves, J., Cordeiro, L., Simoes, P., Monteiro, E., Magdalinos, P., & Chochliouros, I. (2013). Tutamen: An Integrated Personal Mobile and Adaptable Video Platform for Health and Protection. In H. Papadopoulos, A. Andreou, L. Iliadis, & I. Maglogiannis (Eds.), *Artificial Intelligence Applications and Innovations* (Vol. 412, pp. 442–451). Springer Berlin Heidelberg. doi:10.1007/978-3-642-41142-7_45

Razzak, J. A., & Kellermann, A. L. (2002). Emergency medical care in developing countries: Is it worthwhile? *Bulletin of the World Health Organization*, *80*(11), 900–905. PMID:12481213

Rho, M. J., Choi, I. Y., & Lee, J. (2014). Predictive factors of telemedicine service acceptance and behavioral intention of physicians. *International Journal of Medical Informatics*, *83*(8), 559–571. doi:10.1016/j.ijmedinf.2014.05.005 PMID:24961820

Roessler, M., & Zuzan, O. (2006). EMS systems in Germany. *Resuscitation*, *68*(1), 45–49. doi:10.1016/j.resuscitation.2005.08.004 PMID:16401522

Rogers, H., Madathil, K. C., Agnisarman, S., Narasimha, S., Ashok, A., Nair, A., ... McElligott, J. T. (2017). A Systematic Review of the Implementation Challenges of Telemedicine Systems in Ambulances. *Telemedicine Journal and e-Health*, *23*(9), 707–717. doi:10.1089/tmj.2016.0248 PMID:28294704

Roudsari, B., Nathens, A., Cameron, P., Civil, I., Gruen, R., Koepsell, T., ... Rivara, F. (2007). International comparison of prehospital trauma care systems. *Injury*, *38*(9), 993–1000. doi:10.1016/j.injury.2007.03.028 PMID:17640641

Sasser, S., Varghese, M., Kellermann, A., & Lormand, J. D. (2005). *Prehospital trauma care systems*. Geneva: World Health Organization.

Schmiedel, R., & Behrendt, H. (2011). *Leistungen des Rettungsdienstes 2008/09*. Bonn: Dr. Schmiedel GmbH.

Schwamm, L. H., Holloway, R. G., Amarenco, P., Audebert, H. J., Bakas, T., Chumbler, N. R., ... Wechsler, L. R. (2009). A review of the evidence for the use of telemedicine within stroke systems of care: A scientific statement from the American Heart Association/American Stroke Association. *Stroke*, *40*(7), 2616–2634. doi:10.1161/STROKEAHA.109.192360 PMID:19423852

Sood, S., Mbarika, V., Jugoo, S., Dookhy, R., Doarn, C. R., Prakash, N., & Merrell, R. C. (2007). What is telemedicine? A collection of 104 peer-reviewed perspectives and theoretical underpinnings. *Telemedicine Journal and e-Health*, *13*(5), 573–590. doi:10.1089/tmj.2006.0073 PMID:17999619

Soroka, S. N. (2007). Canadian perceptions of the health care system. Toronto: Academic Press.

Suryanto, P., Plummer, V., & Boyle, M. (2017). EMS Systems in Lower-Middle Income Countries: A Literature Review. *Prehospital and Disaster Medicine*, *32*(1), 64–70. doi:10.1017/S1049023X1600114X PMID:27938449

Timerman, S., Gonzalez, M. M. C., Zaroni, A. C., & Ramires, J. A. F. (2006). Emergency medical services: Brazil. *Resuscitation*, *70*(3), 356–359. doi:10.1016/j.resuscitation.2006.05.010 PMID:16901612

Vaitkaitis, D. (2008). EMS systems in Lithuania. *Resuscitation*, *76*(3), 329–332. doi:10.1016/j.resuscitation.2007.07.028 PMID:17822828

Wade, V. A., Eliott, J. A., & Hiller, J. E. (2014). Clinician Acceptance is the Key Factor for Sustainable Telehealth Services. *Qualitative Health Research*, *24*(5), 682–694. doi:10.1177/1049732314528809 PMID:24685708

Wandling, M. W., Nathens, A. B., Shapiro, M. B., & Haut, E. R. (2016). Police transport versus ground EMS: A trauma system-level evaluation of prehospital care policies and their effect on clinical outcomes. *The Journal of Trauma and Acute Care Surgery*, *81*(5), 931–935. doi:10.1097/TA.0000000000001228 PMID:27537514

Weerakkody, V., El-Haddadeh, R., Chochliouros, I., & Morris, D. (2012). Utilizing a High Definition Live Video Platform to Facilitate Public Service Delivery. In L. Iliadis, I. Maglogiannis, H. Papadopoulos, K. Karatzas, & S. Sioutas (Eds.), *Artificial Intelligence Applications and Innovations* (Vol. 382, pp. 290–299). Springer Berlin Heidelberg. doi:10.1007/978-3-642-33412-2_30

WHO. (1996). Report: Investing in health research and development; WHO reference number: TDR/Gen/96.1. Geneva: World Health Organization: Ad Hoc Committee on Health Research Relating to Future Intervention Options.

WHO. (2010). *Injuries and violence: the facts*. Geneva: WHO.

WHO. (2011). *Telemedicine – Opportunities and developments in Member States: report on the second global survey on eHealth 2009. In Global Observatory for eHealth series* (Vol. 2). World Health Oragnization.

Zailani, S., Gilani, M. S., Nikbin, D., & Iranmanesh, M. (2014). Determinants of Telemedicine Acceptance in Selected Public Hospitals in Malaysia: Clinical Perspective. *Journal of Medical Systems*, *38*(9), 1–12. doi:10.100710916-014-0111-4 PMID:25038891

This research was previously published in Strategic Management and Innovative Applications of E-Government edited by Andreea Molnar; pages 26-50, copyright year 2019 by Information Science Reference (an imprint of IGI Global).

Chapter 6
Effective Prevention and Reduction in the Rate of Accidents Using Internet of Things and Data Analytics

B. J. Sowmya
Ramaiah Institute of Technology, India

Chetan Shetty
Ramaiah Institute of Technology, India

S. Seema
Ramaiah Institute of Technology, India

K. G. Srinivasa
CBP Government Engineering College, India

ABSTRACT

Hundreds of lives in India are lost each day due to the delayed medical response. In the present scenario, the victims completely rely on the passersby for almost every kind of medical help such as informing the hospital or ambulance. This project aims to automate the process of detecting and reporting accidents using accident detection kits in vehicles. The kit has a system on chip and various sensors which sense various parameters that change drastically during the occurrence of accidents such as the vibration levels, orientation of vehicles with respect to the ground. The accident is said to occur when these values cross the permissible threshold limit. As soon as this happens, the latitude and longitude of the accident spot is tracked using the GPS module present in the kit. The nearest hospital and police station is computed by the GPS module, which uses the latitude and longitude values as the input. The accident notifications are sent to the concerned hospital and police station

DOI: 10.4018/978-1-7998-2535-7.ch006

over the web interface accordingly. The assignment of particular ambulance and the required traffic policemen to the accident cases is done using the web interface. The android application guides the ambulance driver as well as the policemen to the accident spot and also helps in the detailed registration of the accidents. The closest doctor facility and police headquarters is processed by the GPS module, which utilizes the scope and longitude esteems as the information. The accident warnings are sent to the concerned healing facility and police headquarters over the web interface as needs be. The task of specific rescue vehicle and policemen to the accident cases is finished utilizing the web interface. An intelligent analysis of the last five years' rich dataset uncovers the patterns followed by the accidents and gives valuable insights on how to deploy the existing resources such as ambulances and traffic-police efficiently. Various types of analysis are done to identify the cause-effect relationships and deal with this in a better way. Such technical solutions to the frequently occurring problems would result in saving many lives as well as making the cities safer and smarter.

1. INTRODUCTION

Hundreds of accidents occur in the country everyday causing an immense damage to lives and property. These accidents go unnoticed and unattended by the police and medical help such as ambulance all over the world. This is due to the absence of a mechanism, which can detect the accidents, notify all the nearest concerned authorities such as the police station, hospitals, insurance agents etc. Things haven't changed much in the context of accidents in the last few decades.

The product which is proposed as the solution is Accident Detection Kit, which has a Raspberry Pi as the System on Chip and some of the sensors such as Vibration or Shock sensors, Tilt sensors, Fire and Smoke sensors etc. each dedicated to the sensing of certain parameters which help in the detection of accidents further. The values sensed by them are continuously monitored and on encountering that they have crossed the threshold, the accident is said to occur. The threshold is set based on the testing which was performed on a model car which has undergone certain conditions which could be considered to be as accidents such as extreme vibrations, tilting of vehicles to an angle that sliding or falling becomes very likely, release of smoke/fire near the engine of the vehicle etc. On detecting the occurrence of accident, the location of the accident spot is tracked in terms of latitude and longitude using GPS Module.

The EC2 instance of Amazon Web Services as in is deployed to collect the data from the Raspberry Pi as discussed by (Ignacio, Stefano, Marco, & Maurizio, 2013). The cloud computes the nearest police station as well as the nearest hospital using Google Maps API and the output of GPS module and hence, allots these accident cases to their nearest concerned authorities. The accident details are sent to the hospitals and police station over on their web interfaces so that they can choose the ambulance and police staff to be sent to the accident spot respectively. Automated SMSs are sent to the associated ambulance driver and police staff, intimating them with the details of the accident. The android application eases the process of reaching to the accident spot by guiding the ambulance drivers and the policemen to the associated accident spot in real time. The police staffs also have the option to register the accidents after they examine the situation. This helps in a better monitoring of the accidents which happen in the country and also in the maintenance of a centralized data repository which would be of extreme use further.

The accidents are analyzed to know the cause-effect behavior as discussed by Miyaji (2014) and the generated reports are sent weekly as well as monthly to the respective authorities for further actions using automated e-mail system. This helps in a better understanding of how the deployment of resources such as the police staffs, ambulances etc. can be done. It helps in smarter planning of cities by identifying the suitable sites to build the hospitals, preferably in the areas which are the most prone to accidents so that the time taken by the ambulances to reach the hospital would be lesser. Similarly, the schools, colleges and old-age homes could be constructed or relocated to the areas which are very less prone to accidents to ensure safety of lives. Also, the cab services can improve their patrolling or stationing in the areas with more drunken-driving accidents expecting the people to book their cabs after they drink. Such business strategies could also be made using the inferences drawn from the analysis.

Different Objectives for the Modules

1. Ambulance Service Provider controls both ambulances and hospitals registered under him. Each area consists of an Ambulance Service Provider. Whenever an accident occurs, the corresponding Ambulance Service Provider gets a notification about occurrence of accident in that area. He then assigns ambulance and also books beds in nearby hospital.
2. The drivers of ambulances would get notifications about accidents from corresponding Ambulance Service Provider. He also gets details about the assigned hospital so that they can reach the accident spot faster and admit victim in assigned hospital.
3. This spot of accident is tracked and sent to ambulance driver so that he can reach accident spot. Also the location is shown on graphical user interface (Google maps API) so that he can change travelling directions depending on the traffic to reach accident spot faster.

4. The GPS module which is in-built to get position, altitude, speed etc.
5. The concerned car insurance and life insurance organizations can also be intimated with the notifications regarding the accidents. The blood banks can also be notified in case of any medical urgencies leading to the requirement of blood.

2. LITERATURE SURVEY

Internet of Things offers a great and advanced connection between the many devices, system as well as the services. This goes beyond the machine-to-machine (M2M) communication and includes many protocols, domains as well as applications. (Shah, Nair, Parikh, & Shah, 2015) used piezoelectric sensors which sense the vibrations statically as well as dynamically. They have used a combination of GPS and GSM module to fetch the location. Wakure, Patkar, Dagale, Priyanka, and Solanki (2014) used AVR microcontroller along with accelerometer to detect the accidents. They also used airbag and alcohol sensor to detect the accidents mostly occurred in the four wheelers. Patil, Rawat, Singh, Dixit (2016) discussed about detection of accidents using FPGA, ARM processor and Raspberry Pi. They have designed an intelligent system to control the movement of ambulances on the roads with no loss of time. Poongundran and Jeevabharathi (2015) have designed a vehicle monitoring and tracking system using Raspberry Pi, Thermistor, Shock sensor and Gas Sensor. Hussain, Sharma, Bhatnagar, & Goyal (2011) have discussed about several units such as Vehicle Unit, Ambulance Unit, Traffic Unit, Hopsital Unit and Central Server and implemented them using Arduino as the System on chip. Sonika, Sekhar and Jaishree (2014) have used the same units such as hospital unit, ambulance unit etc and simulated them using nodes in Network Simulation tool NS2. They have found the shortest path for the ambulance to cover in case of occurrence of accidents using Radio Frequency transmitters. Bai, Wu and Tsai (2012) designed a fall monitor system using accelerometers which could analyze the actions of humans such as jumping, waling, sitting etc. The similar kind of approach can also be designed for the monitoring of vehicles too. Prabha, Sunitha and Anitha (2014) discussed that ARM is used by them for the detection of accidents. They used a sensor and used it to detect the accidents. The GSM is used to send the SMS having latitude and longitude values to the number which is pre-saved in the EEPROM. A paper on IoT Based Accident Prevention & Tracking System for Night Drivers as discussed by Lakshmi & Balakrishnan, (2012). They discussed the accident detection mechanism and used KNN algorithm to find the nearest hospital. They have designed an automatic alarm device for the traffic accidents. They have also talked about the chances of false accidents for which a solution is very important to be incorporated.

Kumar and Toshniwal (2015) used clustering initially to partition the working data into multiple groups and then, they have used Probit model to identify the relationships between various characteristics related to accidents. Poisson models and negative binomial models are used by many people, researchers and analysts to mine the relationship between the traffic accidents and the causes of accidents. Rovsek et al. (2017) analyzed the crash data from 2005 to 2009 of Slovenia using classification and regression tree algorithm. Kashani et al. (2011) also used classification and regression tree algorithm to analyze crash records obtained from information and technology department of the Iran traffic police from 2006 to 2008. Depaire et al. (2008) had used latent class clustering on two road user traffic accident data from 1997 to 1999 of Belgium. He divided the data into seven clusters and then performed the analysis. Chang and Chen (2005) analyzed the national freeway data from Taiwan. They have used CART and negative binomial regression model for this analysis. Abdel & Radwan (2000) used an unrelated Negative Binomial regression model to predict the total number of property damages and the injury crashes. Karlaftis and Tarko (1998) used cluster analysis to categorize the accident data into many categories and then analyzed the results obtained from the cluster analysis using the Negative Binomial. They have also revealed the impact of the driver age on the road accidents.

Sangeetha et al. (2014) emphasize the requirements on the ambulance side i.e., reaching the accident site in time. This is accomplished by controlling the traffic lights whenever an ambulance is detected nearby traffic junctions so as to provide a clear path to the ambulance by giving green signal to the lane in which the ambulance is currently travelling. The authors have constructed 2 units namely: ambulance unit, to communicate the position of the ambulance and traffic junction unit, to control the traffic lights as and when the ambulance comes near its vicinity. In the ambulance unit, a GPRS 3G modem is installed so as to provide position of the ambulance as well as to receive the coordinates of the accident site. The position is represented in terms of latitude and longitude, which is displayed on the LCD. In the traffic junction unit, the signal received from the ambulance will cause the circuitry to change the traffic signals as and when necessary. Hence the basic ideology in this work is the automatic control of traffic lights. In this work, other important transportation vehicles which have to reach on time to the delivery site will suffer due to the disruption in the traffic lights and also it will take time to decode the actual position based on latitude and longitude to pin point the actual location and to provide the said location to the ambulance driver.

Shruti Gotadki et al. (2104) have implemented intelligent ambulance system by providing mechanisms to measure vital patient information such as heart rate and body temperature. The ambulance is also provided with the capability of changing traffic signals to provide a smoother ride of ambulance. A visual system is designed and implemented in the hospitals concerned so that the necessary preparations can be made as suitable for the victim and as quickly as possible. The design of the work is as follows. There are 3 main parts namely Ambulance unit, Hospital unit and Traffic signal unit. In the ambulance unit sensors to measure patient parameters such as heart beat/pulse rate and body temperature is embedded on to the micro controller. It also has an analog to digital converter and a Zigbee module. Zigbee module maintains high energy efficiency as a result it works well on low power batteries. The analog to digital converter converts the analog signal detected from the embedded sensors and converts it to appropriate digital signals so that necessary operations can be carried on. The microcontroller reads the parameters and displays on the LCD. It is then sent to the Zigbee module to send the information to the hospital. The traffic signal unit consists of RFID reader, microcontroller, relay driver and light signal. RFID reader detects the signals emitted by the ambulance and each ambulance will have unique RFID. Based on the received signals, the signals are passed on to the microcontroller which is then passed on t the relay to change the traffic signal as and when necessary. The hospital unit consists of Zigbee which is connected to a visual system to display the patient parameters so that the hospital staff can make the necessary preparations even before the arrival of the patient.

Numerous analysts did their examinations on accident discovery framework. Aishwarya explained an IoT based vehicle accident avoidance and framework for night drivers in this paper gives Eye Blink Monitoring System (EBM) that alarms the subject amid condition of drowsiness. Transportation has extraordinary significance in our everyday life and IoT based vehicle accident location framework utilizing GPS and WIFI has picked up consideration. At the point when accident happens, this framework sends short message to WhatsApp of a versatile number by means of Wi-Fi over web. Message will give longitude and scope esteems. From these qualities area of mishap can be resolved (Aishwarya et.al, 2105). Sadhana B clarified Smart head protector keen security for motorcyclist utilizing raspberry pi and open CV. The thought is acquired in the wake of realizing that there is expanded number of deadly street accident throughout the years. This undertaking is intended to present security frameworks for the motorcyclist to wear the cap legitimately. Keen Helmet - Intelligent Safety Helmet for Motorcyclist is a venture attempted to expand the rate of street security among motorcyclists. The thought is gotten after realizing that there is expanded number of harmful street accidents throughout the years. Through the investigation recognized, it is broke down that the caps utilized isn't in wellbeing highlights for example, not wearing a cap string and not utilize the proper size (Shabrin et al., 2016). The primary goal of the referred paper is to computerize every one of the gadgets i.e. home machines through web utilizing Raspberry Pi, and in addition we can have the security for the framework by utilizing sensors like PIR, LPG, temperature sensors. The calculation is produced in Python dialect, which is default programming dialect of Raspberry Pi. To limit the measure of carbon outflows that we contribute towards the total carbon discharges of this world, Use of Sustainable power Sources in Household application has dependably been the best strategy. By creating distinctive codes the correspondence between the remote clients, the web server, the raspberry pi card and the home parts are conceivable (Ghorpade et al., 2016). A productive car security framework is actualized for hostile to robbery and accident location, utilizing an installed framework comprising of a Global Positioning System (GPS) and a Wi-Fi Module. The framework in case of robbery will send predefined message to the proprietor of vehicle. The client (in the event that he feels his vehicle is getting stolen) can begin following the position of focused vehicle on Google Earth on a committed vehicle tracker application. Utilizing GPS locator, the target's present area is resolved and sent, alongside different parameters got by vehicle's information port, through Web through Wifi module that is associated with PC or cell phone. Since the fundamental medium of correspondence is web (framework to client and the other way around), the term IoT or 'Web of Things' is actualized here. The proprietor will have the decision of slicing the supply of fuel to the motor on the off chance that he needs to make prompt move catch the criminal. This highlight will be available on the vehicle tracker application. The other part of the venture is the accident location. The procedure is same as in robbery identification, i.e., when accident takes put; the accelerometer's readings will trigger the framework to begin sending directions of the accident site to the law requirement experts and healing centers, because of which crisis move can be made by them instantly (Karande et al., 2016). The minimal effort and adaptable home control and observing framework utilizing a Raspberry PI module and a Static Relay, with web availability for getting to and controlling gadgets and machines remotely utilizing Smartphone android application. The proposed framework does not require a committed server PC as for comparative frameworks and offers a novel correspondence convention to screen and control the home condition with something beyond the exchanging usefulness. To exhibit the practicality and viability of this framework, gadgets, for example, Static transfers and a Wi-Fi switch can be coordinated with the home control framework (Anitha et al., 2016).

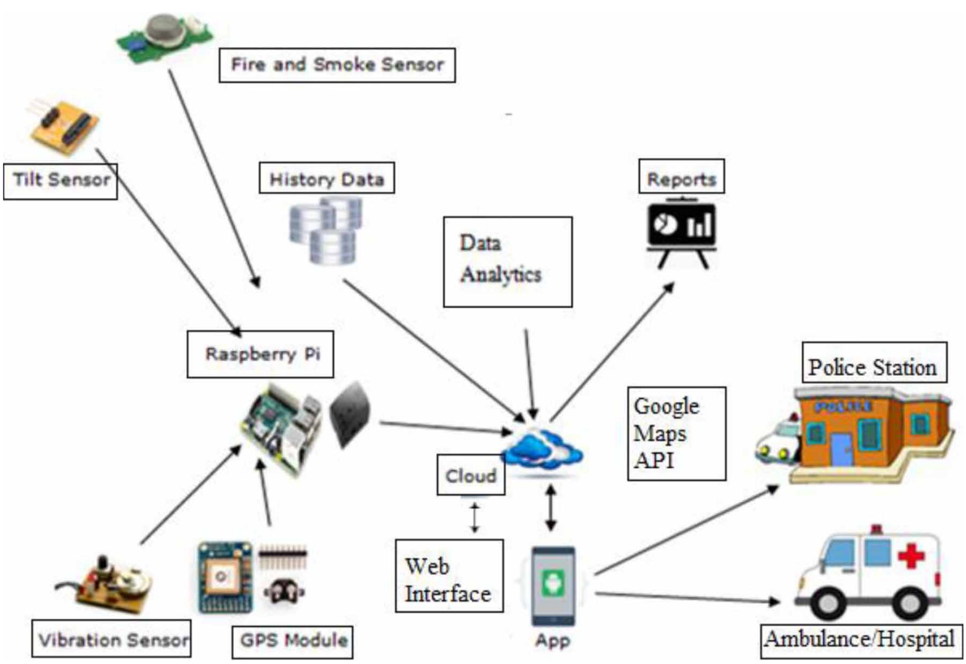
3. ARCHITECTURE

The architecture can be roughly divided in to Internet of Things and Data Analytics part. The Internet of Things part aims to provide solutions after the occurrence of accidents whereas the Data Analytics part proves to be helpful in the pre-accident context. The Internet of Things part consists of the accident detection kit, web interface and android application. The Accident Detection Kit has Raspberry Pi 2

(Model B) as the System on chip. To power it up, a single 2.0 USB connector was used. The SD card was set up with NOOBS and Raspbian OS, which worked in the similar way as the Linux Operating system does. The board has 10/100 Ethernet RJ45 jack for internet connectivity which was used to communicate with the cloud in real time. The Vibration Sensor LM393 served the purpose of detecting the vibrations produced in the vehicle as a result of movements and collisions. They use piezoelectric effect to measure the changes to electrical charge and provide the output in terms of voltages. The sensitivity of the sensor was adjusted by the potentiometer available in the sensor itself. The Tri-Axis tilt sensor, MPU 6050, with programmable full-scale range and digital output was used for measuring the orientation of the vehicles with respect to the ground. Depending on the electric current which is produced from the piezoelectric walls, the direction of inclination of the vehicle and magnitude along the X, Y and Z axes was also determined. The GPS Module, s1216 – R1 is used as the GPS Module, which uses NMEA-0183 protocol for the communication. It has an antenna which communicates with the satellite and finally, the output is obtained as the latitude and the longitude values as discussed by Shah, Nair, Parikh, & Shah (2015). The fire sensor is used to detect the presence of fire, which might have caused due to the combustion of fuel in the vehicle.

The Google Maps API is used on the cloud to compute the nearest hospital and the police station. The cloud performs this using the latitude and longitude values

Figure 1. Architecture design of the system



and performs a nearby search for the desired entity. The accident notifications are sent to the concerned hospital and police station over the web interface accordingly. The assignment of particular ambulance and the required traffic policemen to the accident cases is also done using the web interface. The android application guides the ambulance driver as well as the policemen to the accident spot and also helps in the detailed registration of the accidents. The web interface and android application runs with the cloud instance and is hosted on the same. The five years' data set is stored on the cloud referred to as history data. The Data Analytics is implemented on this data using the R analytical tool after identifying the variables which are closely related and dependent. The output of analytics part is a set of various demographic plots which give a richer and better insight into this concern. These accident analysis reports are mailed to the police station at regular intervals of time so that they can take some steps to overcome or control these problems.

4. IMPLEMENTATION

The implementation can be roughly divided into two parts, namely the Internet of Things part and Data Analytics part. The Internet of Things part consists of the accident detection, tracking of the location using GPS module, finding the nearest hospital and police station, sending them notifications using the web interface, guiding the policemen and the ambulance drivers to the accident spot using the Android application. The data analytics part gives us insights into the trends which are followed by the accidents. The initial part here is the detection of accident for which the authors used a model car to the set up of the sensors as shown in the figure 2. The Raspberry Pi 2 is used as the System on chip. The sensors are used

Figure 2. Model car with system on Chip and the sensors

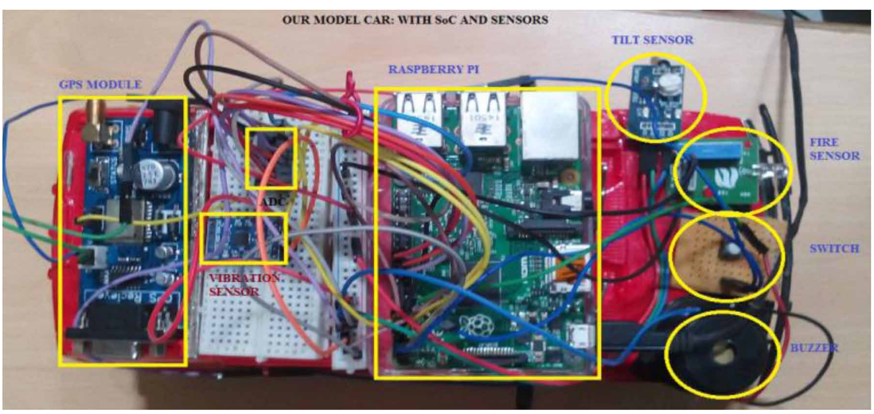
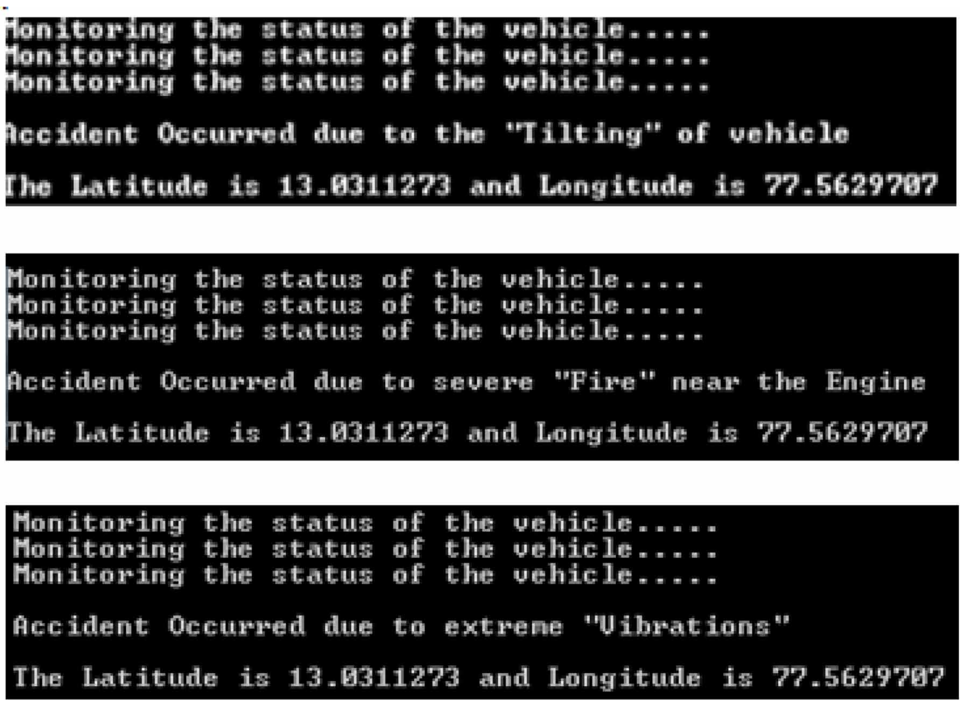


Figure 3. Accidents caused due to different reasons



help in the detection of accidents by sensing the parameters such as vibration, tilting, presence of fire etc. EC2 instance of Amazon Web Services is used as the cloud and it does the computations as well as serves as the storage for the data. It hosts the websites and the database too.

Accident Detection Part Using the Accident Detection Kit Having SoC and Sensors

Step 1: The Raspberry Pi, model 2 B Board is configured.
Step 2: The GPS module is configured to work in association with the System on chip.
Step 3: Connect the accident detection kit to the MySQL database and AWS cloud.
Step 4: The vibration sensor is set up on the model car, which is interfaced to the Raspberry Pi board (SoC). The vehicle is moved and the vibrations caused usually are noted. The vibrations caused when the vehicle collides are also noted.
Step 5: The tilt sensor is set up in the car, which is interfaced to the Raspberry Pi board. The tilting of the vehicle is done along all the three axes, namely X, Y and Z axes. The variations caused in the values of the angles are noted.
Step 6: The fire sensor is set up, ideally near the engine.

Step 7: The test cases for the accident cases are written, considering the conditions such as extreme vibrations, tilting and sensing of fire. This makes sure that all kinds of accidents are detected.

Step 8: The vehicle is titled and is made to collide. As soon as the parameters are noted to be unusual, the buzzer present in the kit starts buzzing. This buzzing happens for 15 seconds and it indicates that there might be an accident in the vehicle.

In cases when the person in the vehicle is fine and doesn't need any kind of help, he can press the switch present near the buzzer in lesser than 15 seconds. Such cases aren't updated in the cloud and are just cancelled as soon as the switch is pressed. This help in taking care of the false accidents and reducing the burden on the cloud too.

In case if he's not fine, the switch will not be pressed at all and this will be considered as an accident and will be hence updated to the cloud after 15 seconds have passed. The various possibilities are shown in Figure 3.

Step 9: Fetch the latitude and longitude using the GPS module as soon as the accident occurs and store them on the cloud.

Finding Out the Hospital and the Police Station Which Are the Nearest to the Accident Spot

The nearest hospital and the nearest police station is found using the Google Maps Script which takes the latitude and longitude values as the input. The pseudo code for searching the nearest hospital using the latitude and longitude as input is as below:

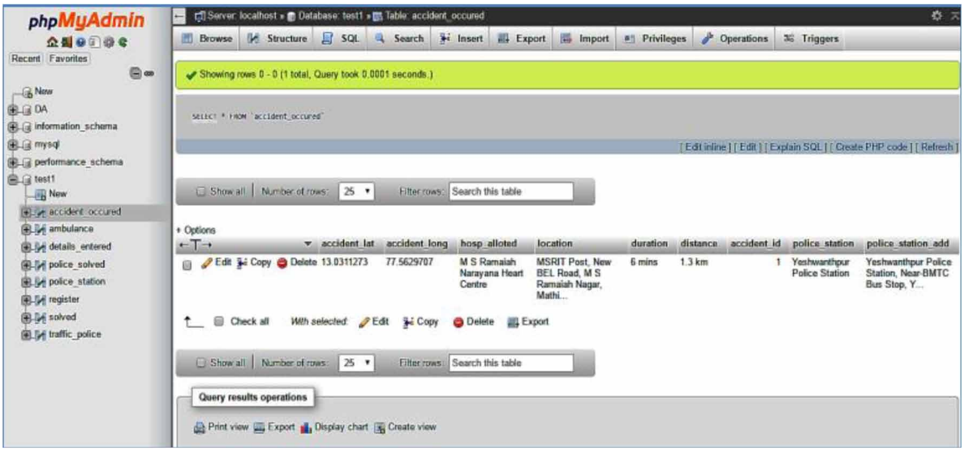
Step 1: The radius for searching the hospital and police station is set to 500 meters initially.

Radius=500 meters

Step 2: Perform a nearby search of type hospital and police station, with source as the address of accident location and within the range as mentioned in the radius. The output of this is the latitude and longitude of the nearest hospital and police station.

Nearest Hospital= nearby search (type='hospital', source=Address, distance=Radius)

Figure 4. Fetching the nearest hospital and police station using Google Maps API and storing them on to the cloud database



Nearest Police Station = nearby search (type='police', source=Address, distance=Radius)

Step 3: If the hospital is found in that range, then go to Step 4, else go to step 6.
Step 4: Get the address of the hospital and police station using Reverse Geo-coding of the location co-ordinates.

Hospital Address = Reverse Geo-code (Nearest Hospital)

Police Station Address = Reverse Geo-code (Police Station)

Step 5: Obtain the shortest path between the accident spot and the hospital as well as the time required to travel from the accident spot to the nearest hospital.

Duration from accident spot to hospital=getDuration (Hospital Address., vicinity, Address)

Distance from accident spot to hospital =getDistance(Hospital Address., vicinity, Address)

Duration from accident spot to police station =getDuration(Police Station Address., vicinity, Address)

Distance from accident spot to police station =getDistance(Police Station Address., vicinity, Address)

Go to step 7

Step 6: Increment the value of Radius by 100 meters. Go to step 3
Step 7: Update the distance and duration in database and commit the changes.

Here, the latitude and longitude for the accident location was 13.0311273 and 77.5629707 respectively. The nearest hospital based on this location is M S Ramaiah Narayana Heart Centre and the nearest police station is Yeshwanthpur police station. This is shown in the figure 4 below. Even the location is geo-coded and stored as the address with the distance and the time duration required to travel from the hospital or police station to the accident spot.

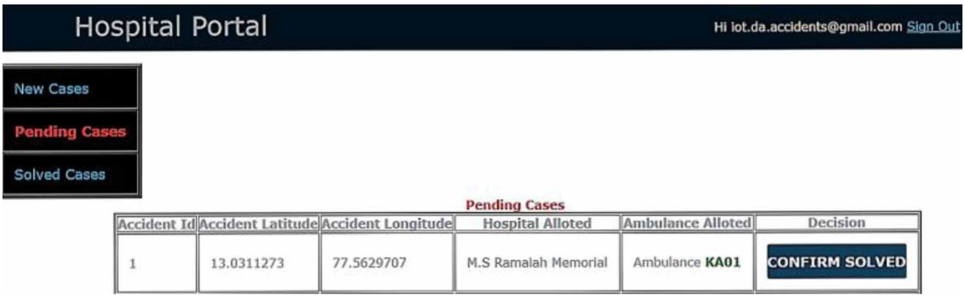
Notifying the Nearest Hospital and the Police Station Using the Web Interface

The hospitals as well as police stations are supposed to register on the website in prior. Only single registration is required for one hospital or a police station. The hospitals have to provide the details of ambulances which they have. These details include the ambulance vehicle numbers, names of drivers and the driver's contact information. Similarly, the police stations have to provide information such as the number of police staff working at that particular branch and their contact details. Once logged in, they get a list of all such accidents which have been allotted to them, meaning that these accidents have occurred in places near to them and hence, are concerned for those cases. These new cases would appear under the New Cases tab as shown in the figure 5.

The concerned person at the hospital checks this and needs to pick an ambulance from the list of available ambulances at his hospital which appears in the form of a

Figure 5. Snapshot of SMS received

Figure 6. The case appears under Pending Cases



drop-down menu and hence, assigns particular ambulance to the accident case. As soon as this happens, the associated ambulance driver receives a notification in the form of SMS to log in to the android application as shown in the figure 8. Similarly, the concerned person at the police station has the option to pick the available police staff and assign him/her to the accident case. The associated staff gets an SMS requesting him to login to the android application using his/her credentials.

Once, the SMS has been sent to the allotted ambulance driver and the police staff, the status of accident changes from new to pending for the hospital's and the police station's account respectively as shown in the figure 6. New accidents which occur now would also again appear under the new cases only.

On the arrival of the ambulance to the hospital after picking the victim, the status of the accident changes from pending to solved finally. Similarly, when the police staffs reach the accident spot and register the accidents using android application, the status of the case changes from pending to solved. All the cases which were solved in the past get saved under the solved cases and hence, is a kind of repository for the hospitals and police station too.

Guiding the Associated Ambulance Driver and the Police Staffs Using the Android Application

The android application is coded in Android Studio. The front end is coded in XML and the back end is Java with MySQL, which is hosted on the cloud. The connection between Java and cloud is established using JDBC. The android application allows the user to login. The user of the android application would be the ambulance drivers or the policemen who have to report to the accident spot after being allotted by the hospital and police station respectively. On entering the valid login credentials, the accident identifier to which they are allotted is found. The login credentials are very simple, such as the vehicle number for the ambulance drivers and the employee id for the policemen. This ensures that there is minimal delay introduced in picture

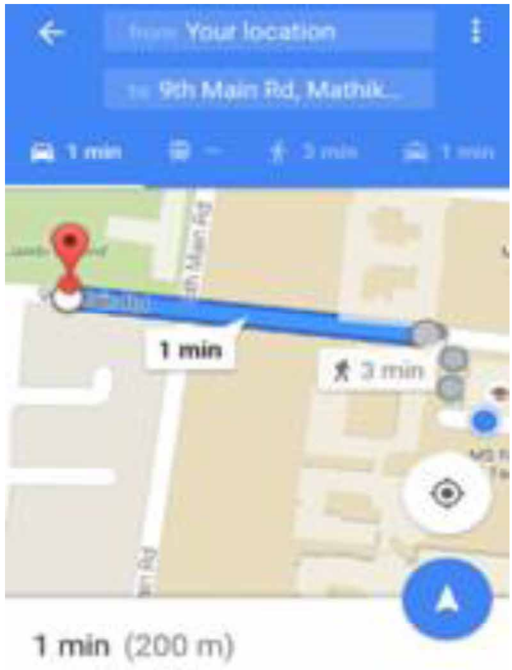
Figure 7. The accident location appears in the android application

as there's no delivery of OTPs and all which saved time. Using the accident id, the latitude and longitude values of the accident location is found from the database, which is further represented by the red marker as shown in figure 7.

The android application uses Google Maps API to find out the shortest route from the current location to the destination. The API key to get this functionality is achieved by publishing the app to the Google Developers Console. The destination for the ambulance driver and the policemen is the accident location. As shown at the bottom right in the figure 7, the options to get the real time travelling direction are also available. The direction appears on the phone as shown in the figure 8.

The policemen can also register the accident by providing further details after they reach the accident spot. That option is also available in the android application. They can describe the parameters related to accidents, which help in the analysis late, such as type of accident, severity, phase of day when accident occurred, if it is a hit and run case, the vehicle number, number of vehicles involved, number of pedestrians injured, number of motorcycles, heavy and public vehicles involved etc.

Figure 8. Travelling directions using Google Maps API



Solutions for Safer and Smarter Cities Using Data Analytics on the Accident Dataset

The Data Analytics part was performed on a dataset having 140,000 accident data points. The installation of the packages required for the analysis, visualizations and the mailing of the results was done. The environment was connected to the cloud, database was selected and a SQL query to fetch the data from the MySQL database was written.

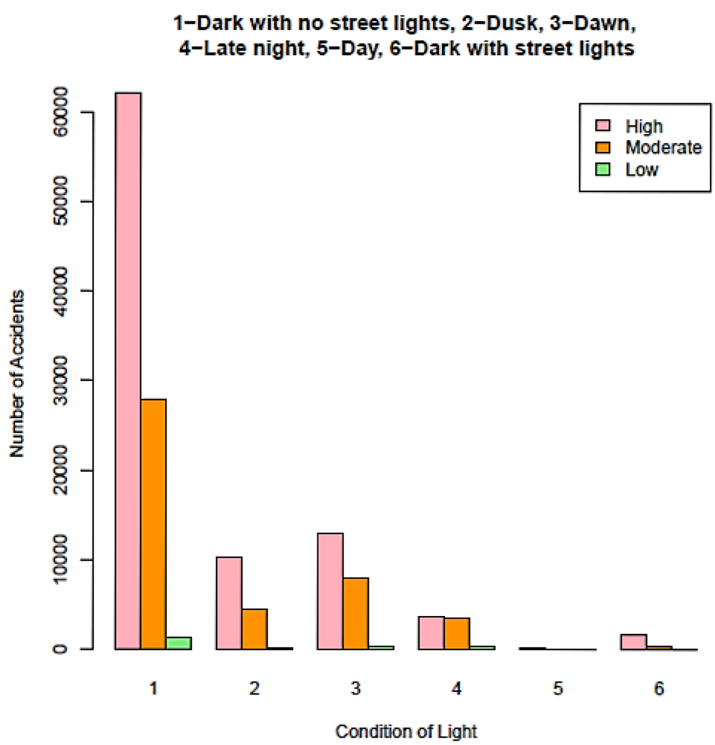
Various graphs were plotted to visualize the relationship between the various columns. These graphs were added to a PDF file and then mailed to the concerned person at the police station using mailR package and related functions. The idea is to find out the severity of accidents as discussed by (Esmaeili, Khalili, & Pakgohar, 2012).

In the first graph as shown in figure 9, the relationship between the severity of accidents and the phase of day is identified. The X-axis shows the various light conditions such as complete dark with no street lights, dusk, dawn, late night, day and dark with street lights. The accidents were extremely higher in number and were more severe, when there was pitch-darkness and street lights were absent. The number of highly severe accidents caused during the dawn time is more than the number of severe accidents occurred during the dusk and afternoon. The number of moderate accidents occurred during the dawn and dusk are very much considerable too as they are large in number. The least, moderately and highly severe accidents mostly don't occur during the day time.

The pseudo code for the same is as below:

Step 1: Import the libraries.
Step 2: Extract or read the entire dataset in a variable.
Step 3: Identify the column of the dataset to be plotted on the X and Y axes. Here it is the number of highly, moderately and less severe accidents on the Y-axis and the phase of day when they occur on the X-axis.
Step 4: Count the frequency of accidents and plot the results in the form of a bar graph.
Step 5: Add the main tag to the image, which usually appears at the top of the bar graph as well as the labels for the X and Y axes.
Step 6: Set the legend and specify the various colors to be shown for each of them.

Figure 9. Analysis of the severity of accidents and the phase of day when they occurred

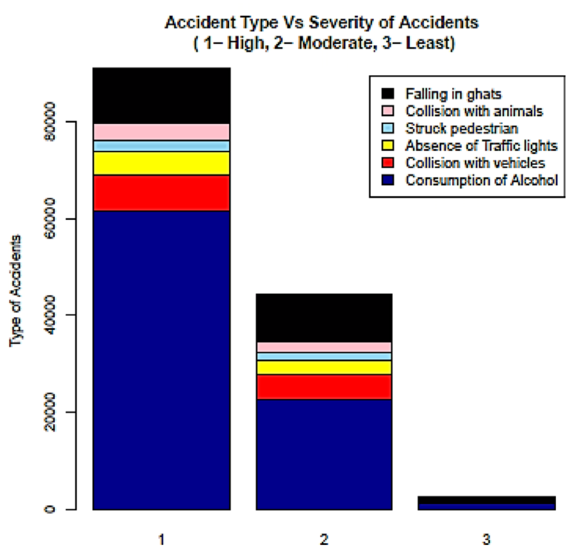


As shown in figure 10, the maximum number of highly and moderately severe accidents occurred due to the consumption of alcohol. The number of accidents occurred die to collision with vehicles and absence of traffic lights is also quite considerable. The accidents which have happened due to the falling of vehicles in the ghats are also very severe. The number of least severe accidents occurred due to the absence of traffic lights, colliding with pedestrians and animals is almost negligible. Using this analysis, some solutions can be derived such as the cab companies can improve their services expecting the people to book their cabs after consuming alcohol. The concerned department can rework on the construction of boundaries near the ghats to reduce the number of accidents.

The pseudo code for the same is as below:

Step 1: Import the libraries.
Step 2: Extract or read the entire dataset in a variable.
Step 3: Identify the column of the dataset to be plotted on the X and Y axes. Here it is the number of highly, moderately and less severe accidents on the Y-axis and the cause of accidents on the X-axis.
Step 4: Count the frequency of accidents and plot the results in the form of a bar graph.
Step 5: Add the main tag to the image, which usually appears at the top of the bar graph as well as the labels for the X and Y axes.
Step 6: Set the legend and specify the various colors to be shown for each of them

Figure 10. Analysis of the type of accident and severity



The X-axis in the figure 11 corresponds to the severity of the accidents being highly, moderately and least severe. The majority of severe accidents occur in the speed zones where allowable driving speed is 60 km/hr. The reason could be too many vehicles moving in those zones causing mayhem and commotion in the dense roads. The number of accidents happened in the zones where allowable speed is nearly 50 and 100 km/hr is also pretty much considerable. The majority of moderately severe accidents occur in the zones where the driving limit is 70 km/hr, followed by the places with a speed limit of 40 km/hr. One important inference from this is that maximum accidents don't occur in the high speed zones but they are in the average speed zones only. The number of less severe accidents is comparatively quite less in number and have mostly occurred in the areas with a speed limit of 50km/hr. Overall, the accidents are very unevenly distributed here.

The pseudo code for the same is as below:

The pseudo code for the same is as below:

Figure 11. Analysis of the severity of accidents based on the speed zones in which they have occurred

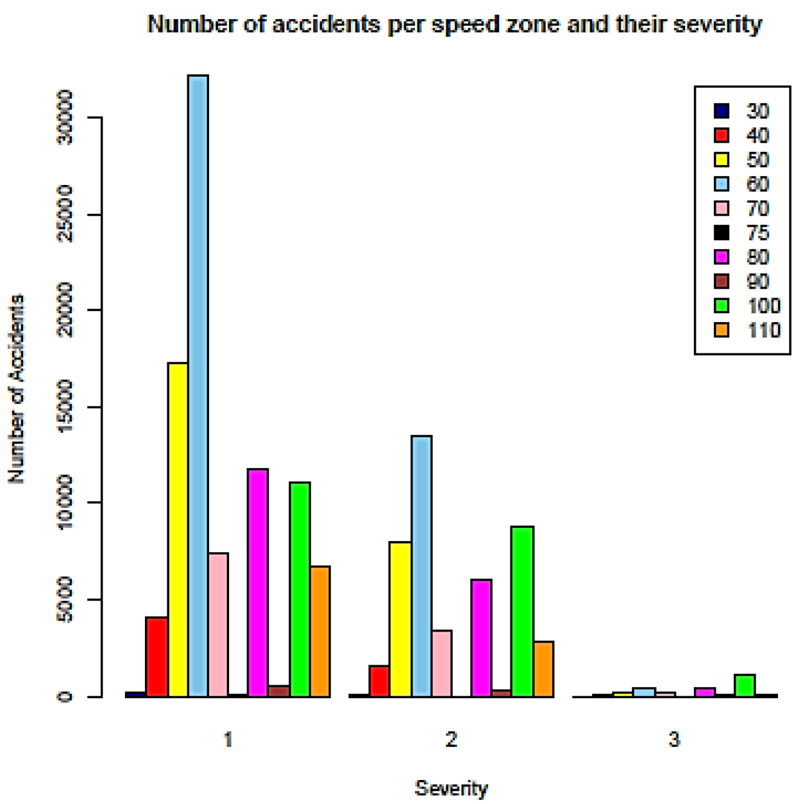
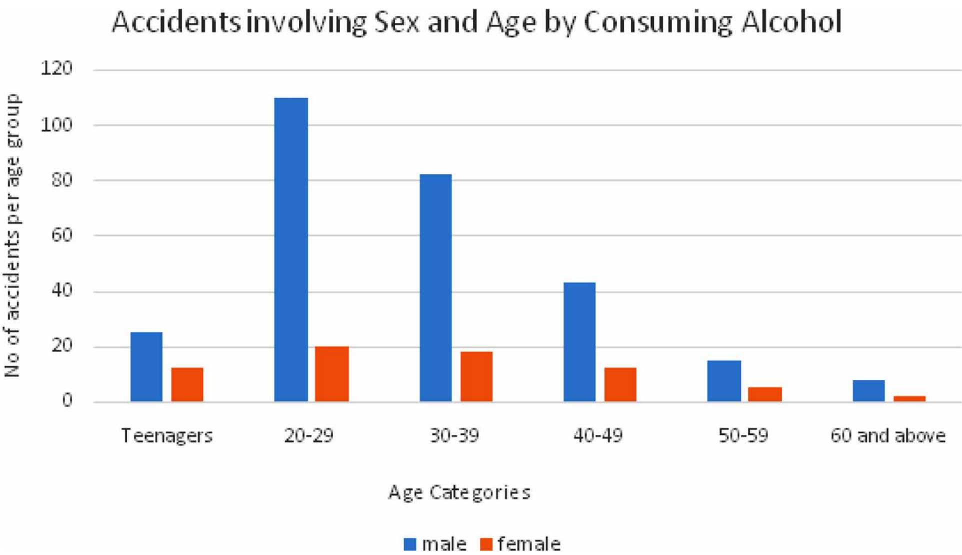


Figure 12. Analysis of the number of Accidents involving Sex and Age by consuming Alcohol



Step 1: Import the libraries.
Step 2: Extract or read the entire dataset in a variable.
Step 3: Identify the column of the dataset to be plotted on the X and Y axes. Here it is the number of highly, moderately and less severe accidents on the Y-axis and the speed zone in which they occur is showed on the X-axis.
Step 4: Count the frequency of accidents and plot the results in the form of a bar graph.
Step 5: Add the main tag to the image, which usually appears at the top of the bar graph as well as the labels for the X and Y axes.
Step 6: Set the legend and specify the various colors to be shown for each of them

The X-axis in the figure 12 corresponds to the age and sex who consumes alcohol. The majority of accidents which is indicated in the y-axis is for the age group 20-29 and more of Male Gender. That is more than 90%. Above 50% of accidents are in the age group 30-39 and again it is more number of male. Above 60 less number of accidents.

The pseudo code for the same is as below:

Step 1: Import the libraries.
Step 2: Extract or read the entire dataset in a variable.

Step 3: Identify the column of the dataset to be plotted on the X and Y axes. Here it is the Age group of different categories teenagers, 20-29, 30-39, 40-49, 50-59 and above 60 and Number of accidents on the Y-axis.
Step 4: Count the frequency of accidents and plot the results in the form of a bar graph.
Step 5: Add the main tag to the image, which usually appears at the top of the bar graph as well as the labels for the X and Y axes.
Step 6: Set the legend and specify the various colors to be shown for each of them

The X-axis in the figure 13 corresponds to the Teenages death. The majority of accidents of teenagers and death are in the duration of Mid night and minimal during the day time.

The pseudo code for the same is as below:

Step 1: Import the libraries.
Step 2: Extract or read the entire dataset in a variable.
Step 3: Identify the column of the dataset to be plotted on the X and Y axes.
Step 4: Count the frequency of accidents and plot the results in the form of a bar graph.
Step 5: Add the main tag to the image, which usually appears at the top of the bar graph as well as the labels for the X and Y axes.
Step 6: Set the legend and specify the various colors to be shown for each of them

Figure 13. Analysis of Teenages death by time of day

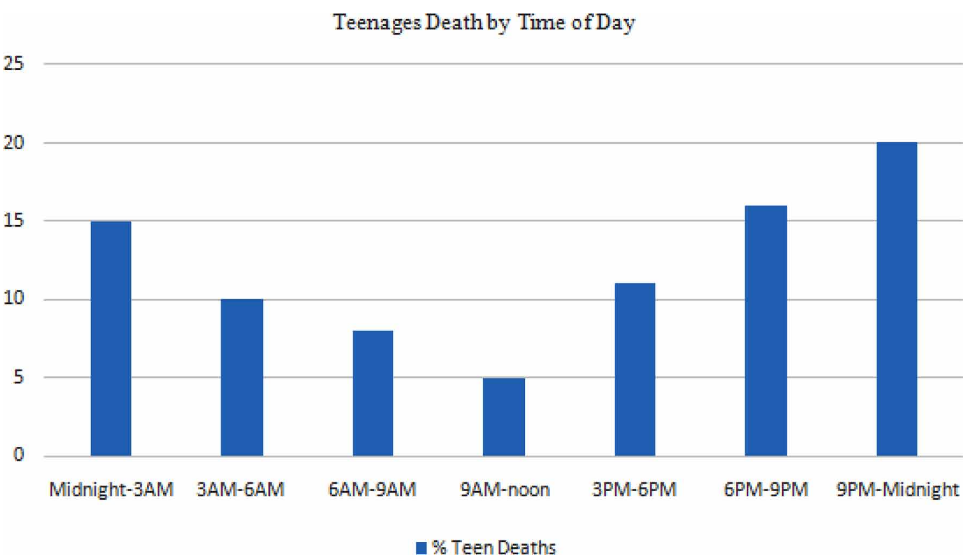
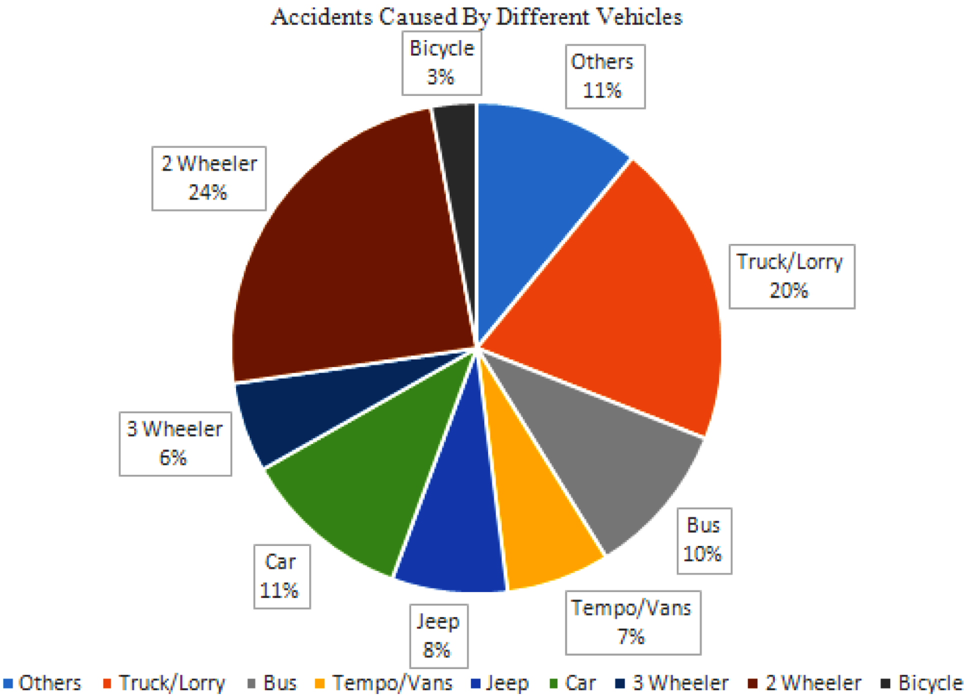


Figure 14. Analysis of the Accidents caused by different vehicles



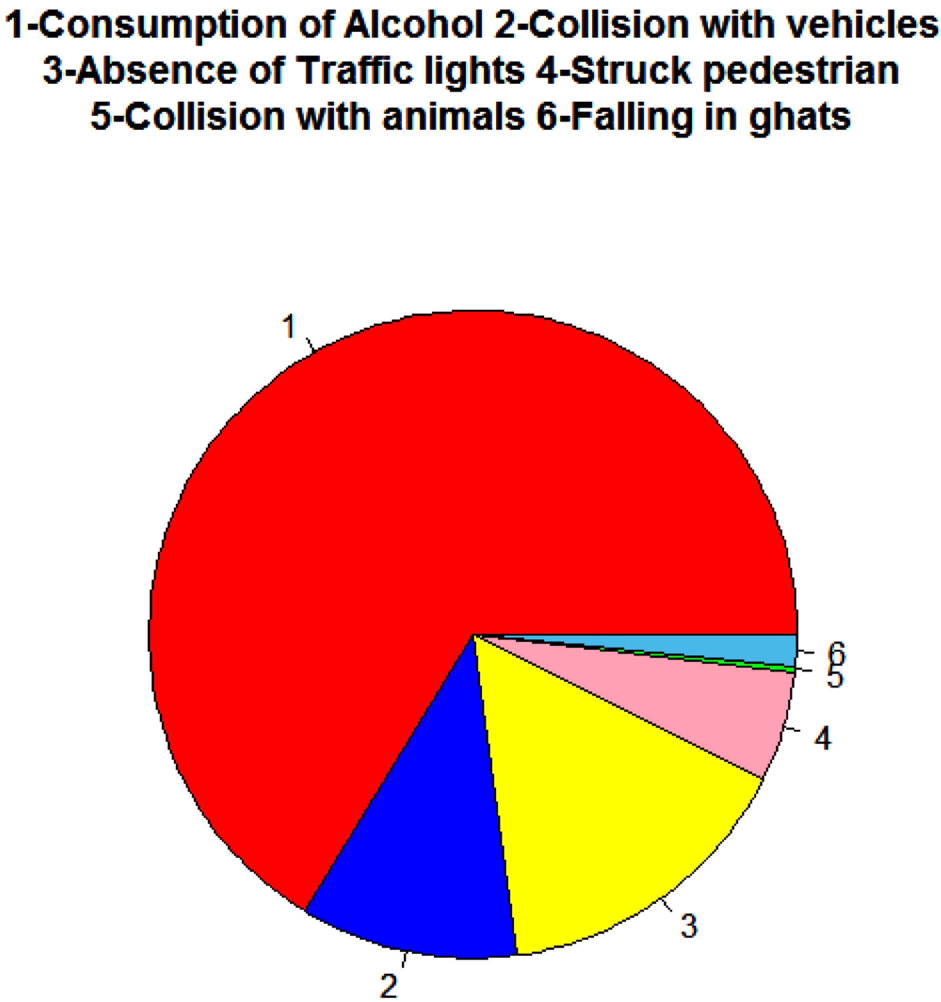
The Accident caused by different vehicles and analysis is given in the figure 14. Most of the accidents are due to the 2 wheelers.

The overall analysis of the cause of accidents was also done which is shown in the figure 15. Most of the accidents, closer to 60% of the total, occurred due to the consumption of alcohol. A large number of accidents have occurred due to the absence of traffic lights while driving. The number of accidents which have occurred due to the collision with the vehicles and the animals is also considerable. The least number of accidents have occurred due to the falling of vehicles in the ghats. A large number of accidents have also occurred leading to the striking of the pedestrians on the roads.

The pseudo code for the same is as below:

Step 1: Import the libraries.
Step 2: Extract or read the entire dataset in a variable.
Step 3: Identify the column of the dataset to be represented in the form of pie chart.
Step 4: Count the frequency of accidents and plot the results in the form of a bar graph.

Figure 15. Analysis of the overall causes of the accidents



Step 5: Add the main tag to the image, which usually appears at the top of the bar graph.

Step 6: Set the legend and specify the various colors to be shown for each of them.

5. COMPARISON AND PERFORMANCE

The existing products similar to this are very rare. Most of them are very static and are installed in very less vehicles due to constraints such as poor performance, non-functioning of sensors etc. The kit designed by the authors is very well-functioning and compact. The existing related work involves detection of accidents by placing sensors in the vehicle and sending SMS. The sending of SMS doesn't take care of the entire process. The authors' solution to this problem makes the entire process easy and hassle free. The information regarding accidents being sent to the nearest hospital and police station using Google Maps API is a novel idea and carries immense social impacts. The sensors used for the project work at a great degree of temperature, moisture and pressure which ensures that the kit doesn't malfunction in certain adverse conditions such as submerging of vehicle in water etc. Most of the related works use GSM Modules for communication, which is a kind of one-way communication and hinders the communication from the other side. The authors have used Ethernet Module to overcome this and using so, they are able to have a proper flow of the both sided communication. The response time of updating the cloud is also very minimal. The usual response time with 3G speed is 1 second and with 2G speed is 3 seconds. The login to the website and android application takes minimum delay. The redirection of android app to the page where the user gets the travelling directions and the related information requires 5 seconds to open with 3G internet speed and 8 seconds with 2G speed. These timing measurements are on an average and completely depend on the speed of internet. The registration of accidents using the android application is also a new idea. The sole purpose of doing this is to obtain and store more information about the accidents so that preventive steps and measures can be taken well in advance. The collection of this accident data serves as the target data for the analysis. The idea of generating reports after analysis and sending it to the concerned person at the police stations is also new and it hardly takes 30 seconds for the script to run.

CONCLUSION

Accidents are one of the most devastating tragedies with the ever-rising trends and these trends have to be necessarily uncovered in order to mine the factors which add severity to them. This product is highly important, quite innovative and very challenging to be used in the country. The product at this time is able to detect the accidents caused due the tilting of vehicles as a consequence of collision, extreme and abnormal vibrations produced in the vehicles, fire caused due to the combustion of fuel in the engine etc. The product also works fine when multiple accident conditions occur. The false alarm is also present, implemented using a buzzer and switch, with the purpose of not notifying anyone when the switch is pressed indicating that the victim is safe. The concerned people at hospital and police station are notified. The allotted ambulance driver as well as police staff is guided to the accident spot. Hence, the Internet of Things as well as Data Analytics helps to save more lives. It also attempts to reduce the number of drunken driving cases. The timely arrival of the ambulances and the policemen to the accident spots can be ensured as the communication becomes quickly. The accident records updated by the policemen serve as a solid proof for the occurrence of the accidents. This solution is an attempt to use technology to solve problems in an eco-friendly and cost-effective manner. The product is very user-friendly, durable and fault tolerant.

FUTURE WORK

The Accident Detection Kit consists of many sensors and is able to sense and record the values properly, but it would be better if the decision is taken using more sensors such as pressure sensors, accelerometers etc. This would strengthen the decision making on the system on chip. The product may need to undergo some customization based on the make and model of the vehicle in which it has to be installed. Some modification will also be required in case of two-wheelers. The app can be used to notify some of the few more concerned authorities such as the blood bank, insurance agents etc. This would make sure that the requirement of blood reaches the concerned department in lesser time. Also, the accident records serve as a proof for the claiming of insurances, which makes the process easy and hassle-free. The commuters can get the real time notifications about the severity of the zone they are traveling in. Alternate routes which are less severe can be suggested to them in such cases to ensure the safety of their lives. Even the website can also be created for the other authorities such as insurance companies and blood banks in the same way as we have for police and hospital at this time. The police stations can have an option to download the weekly and monthly reports generated after the analysis. The data analysis part aims to improve the approach of solving the method of collection and analysis of accident related information. The sensitive areas such as schools, old age homes, orphanages and hospitals can be relocated to the areas which are least prone to accidents. Similarly, the hospitals can be constructed or relocated to the areas which are very much prone to accidents. This would save the travelling time of victims in the ambulances. The real time monitoring of the victim's health condition can also be done by measuring the various parameters such as the blood pressure, heart beat etc. This data can be sent to the hospital prior to the arrival of the victim to plan better well in advance. This analysis can be used to implement protective measure to ensure road-safety of elderly citizens, wildlife and also. This analysis can also be used to identify the areas where consumption of alcohol is found to be the leading cause of accident occurrences. Such areas would be the target for the cab companies as the drunken people would prefer to book their cabs to commute from one place to another. These results can be used by the policy-makers to design the policies which ensure road safety and life safety too.

REFERENCES

Abdel-Aty, M. A., & Radwan, A. E. (2000). Modeling traffic accident occurrence and involvement. *Accident; Analysis and Prevention*, *32*(5), 633–642. doi:10.1016/S0001-4575(99)00094-9 PMID:10908135

Aishwarya, S.R., & Rai, A., Charitha, Prasanth, M.A, & Savitha, S.C. (2015). An IoT based vehicle accident prevention and tracking system for night drivers. *International Journal of Innovative Research in Computer and Communication Engineering*, *3*(4), 3493–3499.

Anitha, T., & Uppalaigh, T. (2016). Android based home automation using Raspberry pi. *International Journal of Innovative Technologies.*, *4*(1), 2351–8665.

Bai, Y., Wu, S., & Tsai, C. (2012). Design and implementation of a fall monitor system by using a 3-axis accelerometer in a smart phone. *Proceedings of the 16th International Symposium on Consumer Electronics (ISCE).*

Bermudez, I., Traverso, S., Mellia, M., & Munao, M. (2013). Exploring the cloud from passive measurements: The Amazon AWS case. Proceedings of IEEE INFOCOM, 230-234.

Chang, L. Y., & Chen, W. C. (2005). Data mining of tree-based model to analyze freeway accident frequency. *Journal of Safety Research*, *36*(4), 365–375. doi:10.1016/j.jsr.2005.06.013 PMID:16253276

Depaire, B., Wets, G., & Vanhoof, K. (2008). Traffic accident segmentation by means of latent class clustering. *Accident Analysis and Prevention, 40*(4).

Ghorpade, D. D., & Patki, A. M. (2016). IoT Based Smart Home Automation Using Renewable Energy Sources. *International Journal of Advanced Research in Electrical Electronics and Instrumental Engineering*, *5*(7), 6065–6072.

Gotadki, S., Mohan, R., Attarwala, M., & Gajare, M. P. (2014). Intelligent Ambulance. *International Journal of Engineering and Technical Research*, *2*(4).

Hussain, F., Sharma, A., Bhatnagar, S., & Goyal, S. (2011). GPS and GSM based Accident Monitoring System. *International Journal of Scientific Research and Management Studies*, *2*(12), 473–480.

Karande, I., Deshpande, G., Kumbhar, S., & Deshmukh, A. V. (2016). Intelligent Anti-Theft Tracking and Accident Detection System for Automobiles Based on Internet of Things. *International Journal of Innovative Research in Computer and Communication Engineering*, *4*(3), 4142–4149.

Karlaftis, M. G., & Tarko, A. P. (1998). Heterogeneity considerations in accident modeling. *Accident; Analysis and Prevention*, *30*(4), 425–433. doi:10.1016/S0001-4575(97)00122-X PMID:9666239

Kashani, T., Mohaymany, A. S., & Rajbari, A. A. (2011). data mining approach to identify key factors of traffic injury severity. *PROMET- Traffic & Transportation, 23*(1). Retrieved from http://www.fpz.unizg.hr/traffic/index.php/PROMTT/article/view/144/51

Kumar, S., & Toshniwal, D. (2015). A data mining framework to analyze road accident data. *Journal of Big Data*, *2*(26).

Lakshmi, C. V., & Balakrishnan, J. R. (2012). Automatic Accident Detection via Embedded GSM message interface with Sensor Technology. *International Journal of Scientific and Research Publication*, *2*(4).

Miyaji, M. (2014). Study on the reduction effect of traffic accident by using analysis of Internet survey, Internet of Things (WF-IoT). *IEEE World Forum on Internet of Things (WF-IoT)*, 325-330.

Patil, M., Rawat, A., Singh, P., & Dixit, S. (2016). Accident Detection and Ambulance Control using Intelligent Traffic Control System. *International Journal of Engineering Trends and Technology*, *34*(8).

Poongundran, A. A., & Jeevabharathi, M. (2015). Vehicular Monitoring and Tracking Using Raspberry Pi. *International Journal of Innovative Research in Science, Engineering and Technology*, *4*(2), 2319–8573.

Prabha, C., Sunitha, R., & Anitha, R. (2014). Automatic Vehicle Accidents Detection and Messaging System Using GSM and GPS Modem. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*. Retrieved from http://www.rroij.com/open-access/automatic-vehicle-accident-detection-andmessaging-system-using-gsm-and-gpsmodem.php?aid=44586

Rovsek, V., Batista, M., & Bogunovic, B. (2017). Identifying the key risk factors of traffic accident injury severity on Slovenian roads using a non-parametric classification tree. *Transport*, *32*(3), 272–281. doi:10.3846/16484142.2014.915581

Sangeetha, K., Archana, P., Ramya, M., & Ramya, P. (2014). Automatic Ambulance Rescue with Intelligent Traffic Light System. *IOSR Journal of Engineering*, *4*(2), 53–57. doi:10.9790/3021-04255357

Shabrin, S. B., Nikharge, B. J., Poojary, M. M., & Pooja, T. (2016). Smart helmet–intelligent safety for motorcyclist using raspberry pi and open CV. *International Research Journal of Engineering and Technology*, *3*(3), 2395–0056.

Shah, D., Nair, R., Parikh, V., & Shah, V. (2015). Accident Alarm System using GSM, GPS and Accelerometer. *International Journal of Innovative Research in Computer and Communication Engineering*, *3*(4).

Sonika, S., Sekhar, K. S., & Jaishree, S. (2014). Intelligent accident identification system using GPS and GSM modem. *International Journal of Advanced Research in Computer and Communication Engineering*, *3*(2).

Wakure, A. R., Patkar, A. R., Dagale, M. V., & Solanki, P. P. (2014). Vehicle Accident Detection and Reporting System Using GPS and GSM. *International Journal of Engineering Research and Development*, *10*(4), 25–28.

This research was previously published in Exploring Critical Approaches of Evolutionary Computation edited by Muhammad Sarfraz; pages 99-121, copyright year 2019 by Engineering Science Reference (an imprint of IGI Global).

Chapter 7
Assessing the Performance of a SAR Boat Location-Allocation Plan via Simulation

Mumtaz Karatas
National Defense University, Turkey

Nasuh Razi
Turkish Naval Forces, Turkey

Hakan Tozan
Istanbul Medipol University, Turkey

ABSTRACT

Maritime search and rescue (SAR) operation is a critical process that aims to minimize the loss of life, injury, and material damage by rendering aid to persons in distress or imminent danger at sea. Optimal allocation of SAR vessels is a strategic level process that is to be carried out with a plan to react rapidly. This chapter seeks to evaluate the performance of a SAR boat location plan using simulation. The proposed methodology in this chapter works in two stages: First, an optimal allocation scheme of SAR resources is determined via a multi-objective mathematical model. Next, simulation is used to test the performance of the analytical solution under stochastic demand. With the heaviest traffic and maritime risk, the methodology is applied to a case study in the Aegean Sea.

DOI: 10.4018/978-1-7998-2535-7.ch007

INTRODUCTION

Each year the Turkish Coast Guard (TurCG) receives hundreds of calls and distress signals from the vessels in danger. As the time difference between life and death can sometimes be measured in minutes, quick response to these signals plays a vital role in reducing fatalities and physical damage (Razi and Karatas, 2016). However, an average SAR operation requires substantial amounts of time, effort and money as well. Hence, emergency response operations should be planned with care and foresight. SAR operations planning can be counted as an emergency system planning. As discussed by Green and Colesar (2004), despite many challenges, operations research and management science applications play an important role in decreasing the negative outcomes of emergencies. This argument is particularly applicable to SAR operations conducted by the TurCG.

TurCG conducts SAR operations in the Turkish Maritime SAR Zone, which is divided into four sub-responsibility areas as follows: the Black Sea, the Sea of Marmara and Adjacent Straits, the Aegean Sea and the Mediterranean Sea. Of all those sub-areas, the Aegean Sea has the heaviest marine traffic due to maritime transportation from and to the Black Sea, shipping, cruise tours, yachting, windsurfing and enormous illegal-border crossing activities.

As a consequence of the heavy maritime traffic, the Aegean Sea has an increased level of risk in maritime safety, which is as much high as the maritime incident rate. Together with (UNHCR Global Appeal, 2015) and (Giuliani, 2015)'s works, Razi and Karatas (2016)'s study show that the number of incidents tend to increase in the Aegean Sea responsibility area each year due to a number of reasons such as:

- Presence of narrow waters and dangerous routes among 3000 islands of various sizes
- Increased vessel traffic passing through the region as an outcome of the turmoil in Syria and Iraq
- Being the main route for immigrants to illegally cross EU borders
- Increased number of vessels carrying hazardous cargo
- Lack of designated shipping lanes

In 2014 alone, TurCG conducted 842 SAR operations, and 716 of them (85% of all operations) were in the Aegean Sea. The data provided by TurCG reveals that during those operations, 12,901 victims were saved, 190 boats were recovered undamaged and 154 lives were lost, while 62% of all operations were related to illegal-border crossing activities.

Considering the abovementioned risks related to the increasing traffic density, Razi and Karatas (2016) detailed the problem of establishing well-planned SAR organizations for the TurCG and they developed a decision support tool named as the "Incident Based-Boat Allocation Model (IB-BAM)". IB-BAM is a three step methodology designed to allocate search and rescue resources. The methodology first ranks and assigns a weight to each incident type observed in the region. Next, utilizing deterministic historical incident data, a Zonal Distribution Model (ZDM) generates aggregated weighted demand locations. Finally, it employs a multi-objective mixed integer program (mo-MIP) model to determine locations and responsibility zones of each SAR boat. Using IB-BAM, the authors attain a more efficient utilization of boats considering multiple objectives.

Although IB-BAM is a powerful and flexible tool in the sense that using real-world data and subjective decision maker assessments on the severity of incident types, it generates effective boat allocation plans, it also has some drawbacks. Currently, IB-BAM does not consider variability in the demand, that is, it generates allocation plans for deterministic incident data. In real-world the nature of the demand is stochastic, hence the performance of IB-BAM should also be evaluated for stochastic incident data. Secondly, IB-BAM aggregates the incidents to concentrated demand points, called *superincidents*, by applying a weighted *k*-clustering algorithm. Such aggregation techniques bring out some potential errors which may affect the accuracy of the results.

For those reasons, in this study we develop a discrete event simulation (DES) to (1) measure the performance of boat allocation plans given by IB-BAM under stochastic demand and (2) measure the error introduced by aggregating demands to superincident locations. The simulation model basically implements the output (allocation plan) of IB-BAM and tests its performance with respect to a number of performance metrics under stochastic incident type, demand, location and time. We also investigate the impacts of different scenarios and business rules when assigning boats to incidents.

The paper is organized as follows. Next section reviews related literature on DES and SAR applications. The following chapter describes the implemented optimization and simulation methodology. Next, we explain our simulation model and present our numerical results for the TurCG boat allocation plan. Finally, we discuss our results and conclude.

RELATED WORK

Simulation is an essential way to evaluate the performance of real-world systems and also assist to design systems for meeting future concerns (Banks, 1999, p.7-13). Shawki et al. (2015, p.533-540) categorize simulation models mainly as mathematical and physical while defining computer simulation as a sub-type of mathematical modeling application. Computer simulation is a decisive method for evaluating complex systems which requires great budget or enormous effort to construct physically in real. Besides, it is more practical than analytic approaches to deal with problems which consider stochastic aspects. Through the history, computer simulation has been applied in a number of private and public firms (Jahangirian et al., 2010, p.1-13). For example, a distinguished review by Aboueljinane et al. (2013, p.734-750) provides a good perspective about computer simulation models applications which are constructed for improving emergency medical services.

DES is a widely used simulation method to analyze and study systems that have state changes at discrete time intervals (Goldsman and Goldsman, 2015, p.103-109). Discrete event-systems have two major features: (1) randomness, (2) changes at discrete points in time. These systems are applicable to the traditional OR fields which are about queuing and inventory theory such as manufacturing, security, network and airport operations (Fu, 1994, p.199-247). In his survey, Smith (2003, p.157-171) displays studies of DES application about manufacturing, published between 1969 and 2002. Williams and Celik (1998, p.915-920) utilize discrete-event simulation method to evaluate the conveyor systems in automotive final assembly line. In their model, they consider a number of issues such as meeting production goal, flow time, determining bottlenecks and improving system performance. For another example of manufacturing application, Byrne and Heavey (2006, p.420-437) formulate a DES model for analyzing the performance of supply chain with multiple customer, distributors and product families. In military sector, Parsons and Krause (1999, p.1174-1178) use discrete-event simulation method to evaluate logistic issues of U.S. Marine Corps while Burke et al. (2000) develop a discrete-event simulation model, namely Transportation System Capability (TRANSCAP) model, for dealing with the problem of deployment of forces from bases. Similarly, Yıldırım et al. (2009, p.597-611) study military deployment planning problem and formulate simulation model with event graph methodology for analyzing efficiency of deployment plans. They experiment their approach with a given scenario which consider deployment of four battalions from north-western Turkey to southeast border. In another example, Varol and Gunal (2015, p.2037-2049) conduct a hybrid DES and Agent-Based Simulation (ABS) model to imitate and evaluate counter-piracy operations on the Gulf of Aden. In their model, they study the problem with behaviors of three main actors such as pirates, transporters and naval forces, in a piracy activity. Consequently, they state that helicopter is the most important vehicle in counter-piracy operations. Similarly, Onggo and Karatas (2015, p.254-265) and Onggo and Karatas (2016) develop a simulation model to analyze maritime search operations such as SAR and patrol. In their study, they try to generate an alternative approach to improve search operations with a simulation model that considers behaviors of searcher and target.

In addition to these areas, researchers confront with other application fields that healthcare and emergency medical services (EMS) constitute a large amount. Günal and Pidd (2010, p.42-51) state that there is a notable increase in the number of DES applications in healthcare over ten years and gather recent DES applications about healthcare systems favorably. They concern each study in literature in terms of application area and categorize studies into six groups such as accident and emergencies (A&Es), inpatient facilities, outpatient clinics, other hospital units, whole hospital simulation and other relevant issues. Ingolfsson et al. (2013, p.736-746) develop a DES to analyze the effects of changing ambulances shift organizations from multiple-start system (MS) to single-start system (SS) in which all ambulances start and end their shifts at the same location. They use historical data of 2000 summer and apply model for north-west and central Edmonton, Western Canada. Zhen et al. (2014, p.12-23) apply DES optimization method to analyze the operational efficiency of ambulance deployment and relocation plan in stochastic scene. Furthermore, responding to distress call as quickly as possible is the main goal for an EMS. However, several issues such as heavy traffic, unexpected failures and breakdowns, and lack of idle resources cause delay and affect the success of operations. Wu et al. (2009, p.1359-1366) study the problem of finding optimal deployment strategies and critical level of demand that requires the ambulance fleet size expanded. They propose a DES model to evaluate EMS of Tainan City while keeping a pre-defined service level as intercepting 90% of calls within 9 minutes. Aboueljinane et al. (2012, p.84) try to improve response time of the French Emergency Medical service (SAMU) in Val-de-Marne department. They develop a DES model to reduce three factors as waiting time, travel time and processing time which determine response time to a distress call. In their study, they experiment their approach with seven scenarios which consider expanding resource fleet, relocation of existing teams and reducing process time. In a different study, Aboueljinane et al. (2014, p.46-59) use DES in five different strategies to advance same system, SAMU, with the objective of intercepting patients' calls within 20 minutes. Wei et al. (2014, p.207-216) utilize DES to improve ambulance response times in Singapore EMS. They follow three main strategies which consist of relocation ambulances, adding private ambulances and modified dispatch policy and provide a significant improvement for the system. In another study, Nogueira et al. (2014, p.1-12) concentrate on minimizing response times of EMS with optimization and simulation approach. They formulate a multi-objective optimization model to determine deployment plan of ambulances. Then, they define the deployment plan obtained from optimization model as initial plan for DES model. They apply their methodology to EMS in Belo Horizonte, Brazil with six different scenarios which consider dynamic changes in number of ambulances, bases and hospitals.

Maritime SAR operations can be counted as another application field for DES to improve response time to incidents. However, there are few DES studies about maritime SAR systems in the literature. Afshartous et al. (2009, p.1086-1096) propose an optimization and simulation combination methodology to determine locations of the US Coast Guard air stations while minimizing total travel cost (distance). In optimization model, they build the model as *p*-Uncapacitated Facility Location Problem (p-UFLP), combination of p-MP and UFLP. Then, they apply simulation method to evaluate the solutions of optimization model. In simulation model, they formulate a statistical model which generates stochastic distress calls from an inhomogeneous Poisson process, using historical data of the year 2000, in order to utilize in simulation model. As another simulation application in maritime SAR, Goerlandt et al. (2013, p.1-6) identify the maritime search and rescue operation as a multi-server, multi-customer queuing system that incidents/incident locations are customers and boats at ports are servers. They develop a DES model to provide a decision-support tool for The Finnish Lifeboat Institution in determining total number and type of boats at each station for SAR organization. For model inputs, they utilize historical incident data from the year 2007 to 2010 in Gulf of Finland and categorize incidents into 21 different types. In addition, they import wave conditions at incident locations into model for imitating real-world state which is an important aspect in determining which type of boat should be assigned. Under these circumstances, they try to locate 29 boats to 11 different stations along Gulf of Finland.

In literature, we confront with few studies addressing locating maritime SAR resources. Even though each study tries to solve the problem from a different perspective, there are a number of common approaches applied in formulation. For example, authors focus mainly on cost minimization and coverage. In contrast with private services, user accessibility and response time should be the main concern in public and emergency services (Balcik and Beamon, 2008, p.101-121). Most studies use aggregated demand and try to meet that demand with the total capacity of boats. However, this assumption ignores actual locations of the demand and affects the solution quality due to the aggregation error. In real-world scenarios, sometimes technical limitations on resources and strategic business rules can be relaxed depending on the severity of the emergency. Hence, the actual outcome of an analytic solution may significantly vary in real world.

In the recent studies, Razi et al. (2016) and Karatas et al. (2017) consider locating SAR helicopters for the TurCG and they propose a combined optimization and simulation approach. Similar to our approach in this chapter, Razi et al. (2016) also employs simulation to measure the performance of SAR helicopter location plans. Karatas et al. (2017), on the other hand, propose a novel three step approach to locate helicopters. At the first stage, they employ a mathematical model which uses deterministic data to generate a good location plan. Next, they implement a heuristic called the alternative plan generation, which generates a number of candidate location schemes. Finally, the authors use simulation to test the performance of each alternative under stochastic data. In the following section, we describe our simulation methodology which addresses these issues.

METHODOLOGY

When planning the locations of SAR resources, decision makers aim to respond to all incidents at sea as rapidly as possible in order to increase the rate of survivals and decrease that of material damages. Moreover, a number of key factors such as real-world incident data, incident severity levels, resource constraints and limitations, geographical limitations, available ports and their capacities, and business rules of the organization should be taken into account when construction allocation models.

Razi and Karatas (2016)'s proposed methodology, IB-BAM, takes into account all above factors and generates effective boat allocation plans in three steps (see Figure 1). They first determine weights for each incident type using a widely used Multi Criteria Decision Making (MCDM) technique named Analytical Hierarchy Process (AHP). Next, the authors develop a ZDM to cluster incidents and generate superincident locations. Finally, they employ a mo-MIP model to generate boat allocation plans.

In this paper we first summarize the three steps of IB-BAM and extend it by implementing a DES model as shown in Figure 1. The DES uses the allocation plan determined by IB-BAM as an input and measures its performance under stochastic data. Next, it evaluates the impact of alternative business rules (rules of assigning a boat to an incident) as well as data aggregation.

We now give an overview of the IB-BAM methodology proposed by Razi and Karatas (2016) and then describe the key aspects of our simulation approach in detail.

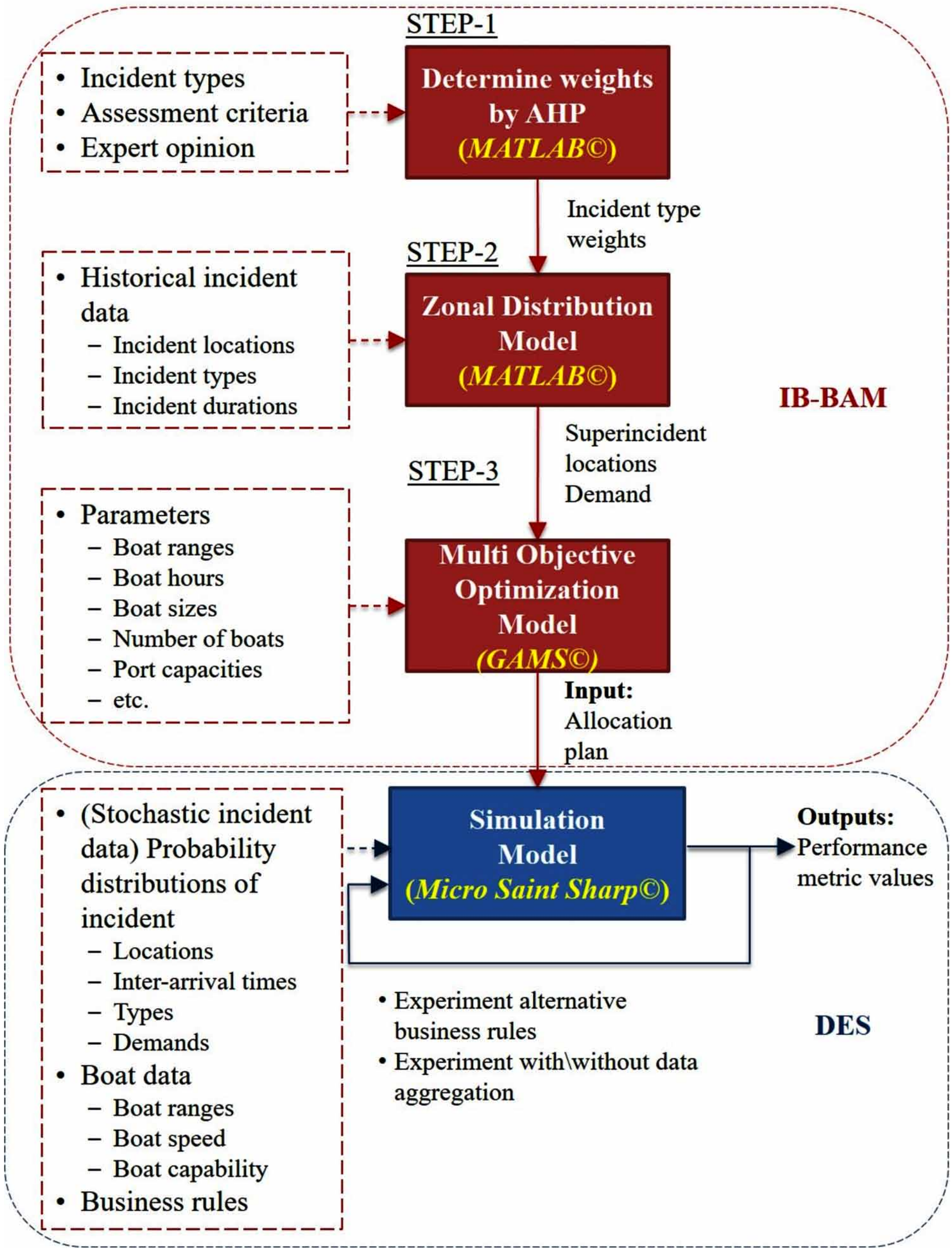
Incident Based-Boat Allocation Model (IB-BAM)

IB-BAM takes into account all above factors and generates effective boat allocation plans in three steps as explained below.

Weight Determination

Using AHP, IB-BAM first determines incident type weights. AHP allows a decision maker to determine relative importance of alternatives by conducting a series of pairwise comparisons with regard to a number of decision criteria.

Figure 1. IB-BAM and DES model methodology



A comprehensive review of Vaidya and Kumar (2006, p.1-29) analyzes the applications of the AHP in literature with a number of themes such as selection, assessment, cost-benefit analysis, allocations, planning and development, priority and ranking, and decision-making. In addition, they also categorize all studies in terms of the application area, such as manufacturing, engineering, personal, social, political, education, industry, government, and others. Korpela and Tuominen (1996, p.169-180) develop an approach to select warehouse sites by the AHP while both tangible and intangible criteria are considered. Similarly, Lirn et al. (2004, p.70-91) utilize the AHP technique to the problem of transshipment port selection. Amer and Daim (2011, p.420-435) overcome the problem of selecting renewable energy option for Pakistan with the AHP. They evaluate four alternative renewable energy options such as wind energy, solar photovoltaic, solar thermal and biomass energy with five criteria and 22 sub-criteria. Karacan (2015) develops a hybrid decision support tool that considers the AHP with other MCDM techniques such as TOPSIS/ Fuzzy TOPSIS, VIKOR/Fuzzy VIKOR, and Goal Programming. The author tests the tool in selection of obesity surgery selection among three alternatives. Işıklar and Büyükozan (2007, p.265-274) study the problem of mobile phone selection by utilizing AHP methodology. Sivilevičius and Maskeliūnaite (2010, p.368-381) try to increase the quality of railway transportation and for that purpose, they get passengers evaluated a number of criteria which are categorized mainly into four groups and conduct the AHP technique. Recent studies of Ho (2008, p.211-228), Dağdeviren et al. (2009, p.8143-8151), Amiri (2010, p.6218-6224), Ishizaka et al. (2011, p.1801-1812), Stein (2013, p.157-171), Herva and Roca (2013, p.77-84), Ren and Sovacool (2014, p.589-597), Luthra et al. (2015, p.762-776) provide further AHP applications for interested researchers.

Razi and Karatas (2016) determine the criteria to assess the importance of an incident type is determined as fatality, material damage, response arduousness and environmental impact. The incident types observed in the Aegean Sea are drifting, capsizing, grounding, fire, collision, flooding, missing, and medical assistance. Denoting the set of incident types by $i \in I$, AHP technique provides the decision makers with a weight of each incident type i, w_i.

Zonal Distribution Model (ZDM)

Given a set of deterministic incident locations and incident type weights (from step-1), in this step

IB-BAM determines superincident locations with a ZDM. The ZDM uses Kerdprasop et al. (2005)'s "*weighted k-means clustering algorithm*" (*wk*-MCA) to generate superincident locations. The *wk*-MCA seeks to minimize the weighted sum of squared distances between each point and its *weighted*-centroid. Actual locations and superincident locations are shown in Figures 3(a) and 3(b), respectively.

Let $z \in Z$ denote the set of superincident zones. The number of zones is determined by *the rule of thumb method* (Kodinariya and Makwana,2013), and computed by the formula $\|Z\| \approx \sqrt{K/2}$, where *K* denotes the number of incidents.

In a facility location problem, locations constitute the majority of inputs in a model. However, as the amount of location data increases, it makes the optimization model so complex to solve in a decent time. In addition, using large-sized data brings out a number of issues by which the decision-maker must confront such as data collection cost, modeling cost, computing cost, confidentiality concerns and statistical data uncertainty (Francis et al., 2009, p.171-208). Thus, data aggregation that Fredrikson et al. (1999) state also as "*a single point that represents or summarizes the group of data points*" is a practicable method to deal with these hardships.

In literature, researchers encounter with a number of clustering techniques. With a more than 50 years history, *k*-means clustering algorithm (*k*-MCA) is a prevalent method for data clustering due to its simplicity, efficiency, and implementation with ease (Jain, 2010, p.651-666). The algorithm provides *k* centers, called "*centroids*", on given *n* data while minimizing the squared error between the center of the cluster and each point in it. In the application process, *k*-MCA follows three main steps (Jain and Dubes, 1988):

1. Initial partition with *k*-cluster,
2. Assigning new patterns to nearest cluster for generating a new partition,
3. Determining new centroids. Re-apply steps 2 and 3 until obtaining stable clusters.

The main parameter of *k*-MCA, *k*-number of clusters to be generated, can be determined in various ways. While Tibshirani et al. (2001, p.411-423) develop a heuristic method, the gap statistic, Kodinariya and Makwana (2013, p.90-95) mention six approaches: rule of thumb, elbow method, information criterion approach, information theoretic approach, choosing *k* using the Silhouette and cross-validation in their review. The algorithm runs separately for any *k* value no matter which method is used for determining "*k*" (Jain, 2010, p.651-666).

Data aggregation has been applied for a number of purposes such as grouping, defining patterns and determining similarity of data. There are a number of papers that contain data aggregation for different purposes in facility location models. Nemes et al. (2004, p.15-20) study the problem of evaluating the performance of AIDS care clinics where deliver antiretroviral treatment in Brasil. They conduct a questionnaire at 27 sites to determine service quality and utilize *k*-means clustering to gather health services in four groups as "Best", "Medium", "Poor" and "Very Poor" in terms of questionnaire scores. Liao and Guo (2008, p.323-339) generate a clustering-based method to deal with capacitated facility location problem. At first, they determine the allocation plan with minimum cost. Then, they utilize *k*-means clustering-based iterative optimization method to allocate facilities while minimizing demand-weighted distance between demand and associated facility. They also evaluate their methodology with Genetic Algorithm (GA) and state that clustering-based method provides better solutions and lower cost of time. In their study, Li et al. (2012, p.1103-1117) develop a clustering-based scatter search method to determine locations of transshipment points (TPs) which allow multi-commodity flow. They use *k*-means clustering approach to obtain initial solution for their method. In another application, Esnaf and Küçükdeniz (2009, p.259-265) propose a fuzzy clustering-based hybrid method for the multi-facility location problem. The problem is about to deploy multiple facilities for serving demand points. In their method, authors utilize clustering approach to group demand points with the aim of degrading problem from multiple to single facility location problem. They partition demand points into clusters and try to locate a single facility in each cluster. Similarly, Sahraeian and Kazemi (2011, p.1098-1102) study the problem of locating multiple facilities among a number of sites whereas all demand points are covered at least one facility. In their three stage method, firstly they determine the minimum number of facilities needed, in other words, *k*, with fuzzy set covering approach. Then, they implement *k*-means clustering approach to group demand points into *k*. Finally, they seek the optimal locations of *k* facilities in each group (cluster).

Optimization Model

As the third step, IB-BAM generates effective allocation plans using a *mo*-MIP model. The model considers incident types, candidate ports, superincident zones, boat types, boat features and capacities, and some organizational rules. The sets, indices, parameters, decision variables, objective function, and constraints used in the formulation are explained below.

Sets and Indices

$i \in I$: Set of incident types.
$p \in P$: Set of candidate ports.
$z \in Z$: Set of (superincident) zones.
$b \in B$: Set of boat types.
$B_i \subset B$: Set of boat types that are appropriate for incident type $i \in I$.
$B_p \subset B$: Set of boat types that are allowed at port $p \in P$.

$B_{pz} \subset B$: Set of boat types that can respond to incidents in zone $z \in Z$ from port $p \in P$.
$g \in G$: Set of goals.

Parameters

cf_{bp} = Yearly fixed cost of utilizing one type b boat at port p (\$/year).
$c\upsilon_b$ = Variable cost of operating one type b boat for one hour (\$/hr).
U_b = Total available number of type b boats.
$u_b^{\min}$ = Minimum allowable number of type b boats at a port if allocated.
$u_b^{\max}$ = Maximum number of type b boats that can be allocated to a port.
S_b = Annual Operation Capacity (AOC) of a single type b boat (hrs).
r_b = Maximum allowable percentage of AOC that can be exceeded for type b boat.
γ_b = Multiplier to provide minimum allowable yearly total task time for boats of type b assigned from a port to a zone for a single incident type (hrs).
w_i = Weight of incident type i.
D_{zi} = Aggregated yearly demand in zone z for incident type i (hrs).
n_{zi} = Number of type i incidents aggregated to zone z.
rt_{bpz} = Response time of a type b boat from port p to zone z (hrs).
crt_i = Critical response time threshold for incident type i (hrs).
L_p = Physical capacity of port p (mts).
ℓ_b = Length of type b boat (mts).
FB = Annual fleet operating budget (M\$).
w_g = Weight of goal g (assigned by the decision maker)
θ_g = Normalization factor for goal g (assigned by the decision maker)
M = Large number

Decision Variables

x_{bp} = Number of type b boats allocated to port p (integer).
y_{bp} = Variable indicating whether or not type b boats are utilized in port p (binary).
s_{bpzi} = Total number of yearly hours (supply) of type b boats assigned from port p to zone z for incidents type i (hrs).
λ_{bpzi} = Variable indicating whether or not type b boats are utilized in port p to zone z for incidents type i (binary).
$dev_{bpzi}^{crt+}, dev_{bpzi}^{crt-}$ = Positive and negative deviations associated with critical response time threshold for each individual incident type i in zone z responded from port p by type b boat (hrs).

dev^{fb+}, dev^{fb-} = Positive and negative deviations associated with the annual fleet operating budget ($).

$dev_{bp}^{s+}, dev_{bp}^{s-}$ = Positive and negative deviations associated with the AOC for type b boats in port p (hrs).

Objective Function

Utilizing incident type weights from step-1 and superincident locations from step-2, it provides an optimal allocation plans while minimizing three terms in the objective function (1):

- The total weighted deviations resulting from exceeding critical response times to incidents.
- The deviation resulting from exceeding the allocated fleet budget.
- The total deviation of supply from capacity (annual operation capacity of SAR boats).

As an output the model provides the number of each boat type allocated to each port.

$$\min z = \omega_1 \theta_1 \sum_{b \in B} \sum_{p \in P} \sum_{z \in Z} \sum_{i \in I} w_i n_{zi} dev_{bpzi}^{crt+} + \omega_2 \theta_2 dev^{fb+} + \omega_3 \theta_3 \sum_{b \in B} \sum_{p \in P} \left(dev_{bp}^{s+} + dev_{bp}^{s-} \right) \tag{1}$$

Although there are a number of solution techniques for multi-objective problems, we choose weighted sum method to solve our model. A brief discussion for solving multi objective location models also exist in Karatas (2017, 2018) and Karatas and Yakici (2018). However, each section of the objective function has a different scale and this difference could affect the correctness of results. Thus, the normalization of the objective function component is necessary.

Regarding the type of our optimization model, it is proper to utilize the notion of Pareto optimality which provides no other solutions that improves at least one part of the objective function without degradation in another (Zitzler and Thiele, 1999, p.257-271). At this point we use the normalization technique described in (Grodzevich and Romanko, 2006, p.89-101). In this technique, two special points are calculated for each section of the objective function individually, namely Nadir and Utopia points. Utopia point, z^U, represents the lower bound of mentioned section and could be obtained by minimizing each section i as follows:

$$z^{*} = \arg\min_{x} \left\{ f_{i}\left(x\right) : x \in \Omega \right\} \tag{2}$$

Nadir Point, z^N, represents the upper bound of each objective section *i* and could be defined as:

$$z_{i}^{N} = \max_{1 \le j \le k} \left(f_{i}\left(x^{[j]} \right) \right), \forall i = 1, \ldots, k \tag{3}$$

After calculations of these points, normalization coefficient value for each section, θ_i, could be determined as in equation (4):

$$\theta_{i} = \frac{1}{z_{i}^{N} - z_{i}^{U}} \tag{4}$$

Each of these coefficient values, θ_i, normalize scales and make the magnitude of each section equalized. Furthermore, it is clear that utilization of normalization technique bounds the objective function value as:

$$0 \le \frac{f_{i}(x) - z_{i}^{U}}{z_{i}^{N} - z_{i}^{U}} \le 1 \tag{5}$$

The θ_g values are determined by computing the Nadir and Utopia values as described in Grodzevich and Romanko (2006). These coefficients are used to scale objective function terms which have different magnitudes.

Constraints

$$\sum_{p \in P} x_{bp} \le U_{b}, \forall b \in B \tag{6}$$

$$y_{bp} u_{b}^{\min} \le x_{bp} \le y_{bp} u_{b}^{\max}, \forall b \in B, p \in P \tag{7}$$

$$\sum_{p \in P} \sum_{b \in B} s_{bpzi} = D_{zi}, \forall z \in Z, i \in I \tag{8}$$

$$\lambda_{bpzi}\gamma_{b} \leq s_{bpzi} \leq \lambda_{bpzi}M, \forall b \in B, p \in P, z \in Z, i \in I \tag{9}$$

$$\sum_{z\in Z}\sum_{i\in I} s_{bpzi} \leq x_{bp}M, \forall b \in B, p \in P \tag{10}$$

$$\sum_{b\in B} x_{bp}\ell_{b} \leq L_{p}, \forall p \in P \tag{11}$$

$$\sum_{b|b\in B\setminus B_{p}} x_{bp} = 0, \forall p \in P \tag{12}$$

$$\sum_{b|b\in B\setminus B_{i}}\sum_{p\in P}\sum_{z\in Z} s_{bpzi} = 0, \forall i \in I \tag{13}$$

$$\sum_{b|b\in B\setminus B_{pz}}\sum_{i\in I} s_{bpzi} = 0, \forall p \in P, z \in Z \tag{14}$$

$$rt_{bpz}\lambda_{bpzi} + dev_{bpzi}^{crt-} - dev_{bpzi}^{crt+} = crt_{i}, \forall b \in B, p \in P, z \in Z, i \in I \tag{15}$$

$$\sum_{z\in Z}\sum_{i\in I}\left(s_{bpzi} + 2n_{zi}rt_{bpz}\lambda_{bpzi}\right) + dev_{bp}^{s-} - dev_{bp}^{s+} = S_{b}x_{bp}, \forall b \in B, p \in P \tag{16}$$

$$\left(\sum_{b\in B}\sum_{p\in P} cf_{bp}x_{bp} + \sum_{b\in B}\sum_{p\in P}\sum_{z\in Z}\sum_{i\in I} cv_{b}s_{bpzi}\right) + dev^{fb-} - dev^{fb+} = FB \tag{17}$$

$$dev_{bp}^{s+} \leq S_{b}x_{bp}r_{b}, \forall b \in B, \forall p \in P \tag{18}$$

$$x_{bp} \in \{0,1,2,...\}, \forall b \in B, p \in P \tag{19}$$

$$y_{bp} \in \{0,1\}, \forall b \in B, p \in P \tag{20}$$

$$\lambda_{bpzi} \in \{0,1\}, \forall b \in B, p \in P, z \in Z, i \in I \tag{21}$$

$$s_{bpzi}, dev_{bpzi}^{crt+}, dev_{bpzi}^{crt-} \geq 0, \forall b \in B, p \in P, z \in Z, i \in I \tag{22}$$

$$dev^{fb+}, dev^{fb-} \geq 0 \tag{23}$$

$$dev_{bp}^{s+}, dev_{bp}^{s-} \geq 0, \forall b \in B, p \in P \tag{24}$$

Constraint set (6) ensures that the number of boats allocated does not exceed the total number of boats available. Constraint set (7) implements the business rule for the minimum and maximum number of boats requirements, and ensures that for each boat, there should be at least $u_b^{\min}$ and at most $u_b^{\max}$ of it respectively. Considering scheduled events such as maintenance or overhauling, or the unexpected situations such as breakdowns or crew shortages, this constraint provides backup supply to ports. Constraint set (8) satisfies the supply-demand balance for each zone and incident type. Constraint set (9) determines the minimum allowable s_{bpzi} hours. Constraint set (10) ensures that supply from a boat type *b* in port *p* can be positive only if x_{bp} is positive. Constraint set (11) restricts the number of assigned boats for a port. According to business rules, certain boat types are not allowed at certain ports. These rules are implemented by constraint set (12). Constraint set (13), on the other hand, dictates appropriate boat type-incident type assignments. Constraint set (14) makes sure boats operate within their maximum ranges. Constraint sets (15), (16) and (17) represent the goals for response time, boat capacity and budget. Constraint set (18) ensures that, for each boat type in a port, the positive deviation associated with the AOC does not exceed the maximum allowable time.

Simulation Model

In this study, we identify Maritime SAR process as server-to-customer queuing system which incidents/ demands are customers and boats/resources are servers and perform simulation methodology to evaluate the system. Simulation optimization technique requires advanced computers and takes respectable time to conduct. Thus, we apply DES model to test the performance of optimization model.

To evaluate the optimization model properly and to measure aggregation error, we demonstrated two distinctive simulation models: model with grids (SimModel-1), and model with data aggregation (SimModel-2). These models will be discussed in the following sections. In both models, we followed four different business rules about supply capacity policy. Firstly, we ran the model with the business rule that does not allow decision-makers to use boats having already consumed all of the yearly supply capacity (AOC). It was followed by three alternative business rules that allow 10%, 20% and unlimited exceedance on the AOC. Experiments were conducted in Micro Saint Sharp© version 3.7 on a computer with Intel Core i5-3330S CPU@2.70 Ghz processor and 6.00 GB memory. Our simulation model is constructed with three stages as (1) Inputs, (2) Process Flow, and (3) Outputs. We now briefly explain these stages.

Input

In our simulation model, we utilize three inputs: (1) Incidents (demand), (2) Ports, (3) SAR boats (resources). In stage of determining incidents, we use historical incident data for year 2014 provided by TurCG. However, utilizing all incidents individually makes the model more complex as in optimization model. Thus, we divide the responsibility area into rectangular grids. Each grid represents a sub-area with its individual incident patterns. It is clear that generating smaller grids approximates the system to the real case. However, geographical features of the area could not let it to do easily. More importantly, generating a smaller grid structure enables to represent risky sub-regions. Then, we analyze real-world data to generate the below-mentioned probability distributions for each grid:

- Inter-arrival time distributions for each incident type,
- Incident location distributions,
- Incident duration (demand).

For other inputs, we take the data of activated ports and assigned boats from IB-BAM optimization model's outputs. We implement the allocation plan provided by the optimization model as an input to the simulation model.

Process Flow

A maritime SAR operation usually starts with a distress call from the vessel in danger. Decision-makers in an operation center assess the situation and pass all related information about incident to the nearest port which hosts at least one idle capable boat. When all information is recorded, port dispatches a capable boat with respect to incident type, e.g. decision-makers must assign a faster boat to medical assistance incident for transferring patient to nearest medical services as quickly as possible. Then, boat conducts the operation unless it is in need of refueling otherwise it turns back to port for refueling. After that, it goes on duty if requires, otherwise, stands in port for next missions.

In our DES model structure (see Figure 2), a SAR process begins with a distress call to the operation center. Then, the model calculates distances from incident position to each port and sorts them. Port-zone distances are calculated by an online tool called the Marine vessel traffic ©. Next, the operation center checks ports in ascending order (with respect to distance) for an idle capable boat. If the operation center determines port and boat type to assign, designated boat dispatches for conducting the SAR mission. However, in some cases, there could be more than one capable and idle boat for a mission. Thus, we implement two different selection criteria for determining which boat to assign among capable ones: (1) remaining capacity and (2) speed.

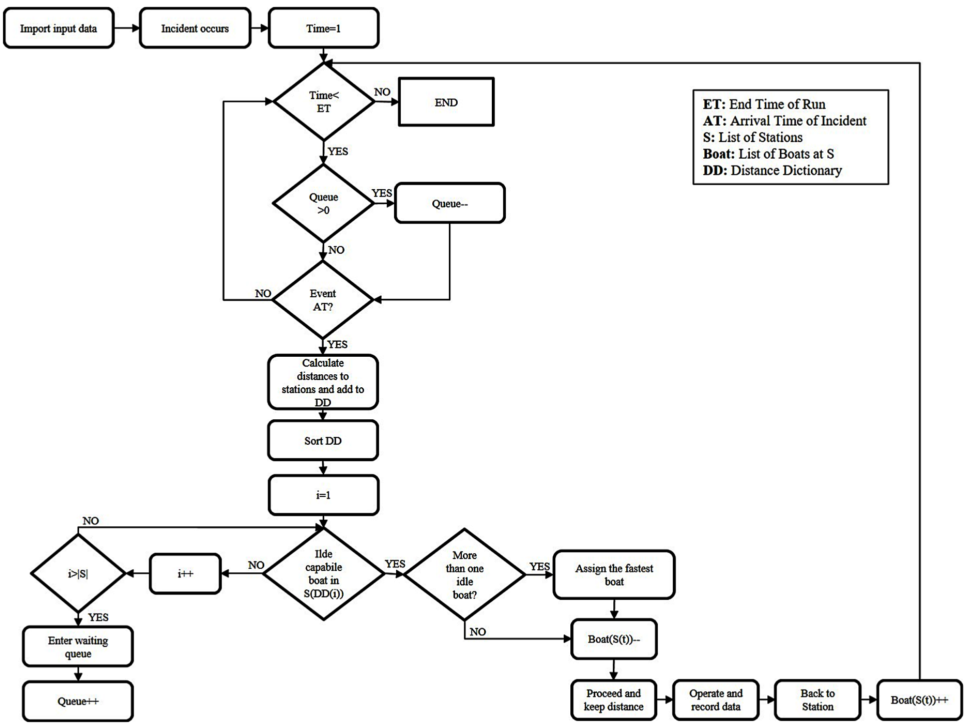
Remaining Capacity

The main goal of this criterion is to maintain balanced workload among boats. Hence, operation center selects the capable one with higher remaining capacity, even if there is a faster idle boat. Furthermore, we try to represent the third section of the objective function in optimization model with this criterion. After selection, the boat conducts the duty. However, in case of no idle boat for a duty, incident waits for an idle boat in the queue (FIFO).

Speed

With this criterion, the model follows a greedy approach by assigning the available fastest boat for each incident. When an incident occurs and there is more than one idle boat, the model (operation center) selects the fastest idle boat among capable ones. It is clear that this approach could help to reduce response times. However, giving priority to faster ones could also cause consuming faster boats toward the end of the simulation model. After selection, the boat conducts the duty. However, in case of no idle boat for a duty, incident waits for an idle boat in the queue (FIFO). Model executes a process flow for 24x365=8760 hours which imitate a year.

Figure 2. Flow chart of simulation model



Output

We use our simulation model to evaluate the performance of the optimization model in terms of 12 measure of effectiveness (MoE) values summarized in Table 1.

NUMERICAL APPLICATION

Input

In our simulation model, we consider locating 9 types of SAR boats to 25 candidate ports. For confidentiality purposes we name boats as $B1$, $B2$,…, $B9$ and ports as $P1$, $P2$,…, $P25$. The historical data for year 2014 includes 716 incidents of 8 different types in the Aegean Sea. Key parameters with respect to incidents (incident type weights, number of incidents observed and average demand per incident) and boat types are presented in Tables 2 and 3, respectively.

Table 1. Model outputs (AOC: annual operation capacity of a boat)

	Performance Metric	Definition
MoE_1	Total delay (hrs)	≜ Sum of positive deviations associated with the critical reaction time threshold
MoE_2	Total weighted delay (hrs)	≜ Sum of weighted positive deviations associated with the critical reaction time threshold
MoE_3	Shortage on the budget (M$)	≜ Positive deviation associated with the annual budget
MoE_4	Ratio of budget used	$\triangleq \frac{\text{used fleet budget}}{\text{planned fleet budget}}$
MoE_5	Total excess AOC (hrs)	≜ Sum of negative deviations associated with the AOCs
MoE_6	Total shortage on the AOC (hrs)	≜ Sum of positive deviations associated with the AOCs
MoE_7	Total deviation on the AOC (hrs)	≜ Sum of (positive and negative) deviations associated with the AOCs
MoE_8	Ratio of utilized fleet size	$\triangleq \frac{\text{total number of boats utilized}}{\text{total number of boats available}}$
MoE_9	Ratio of incidents intercepted	$\triangleq \frac{\text{total number of incidents intercepted}}{\text{total number of incidents occured}}$
MoE_{10}	Ratio of demands satisfied	$\triangleq \frac{\text{total number of demands satisfied}}{\text{total number of demands generated}}$
MoE_{11}	Total reaction time (hrs)	≜ Sum of reaction times to incidents intercepted
MoE_{12}	Reaction time per incident (hrs)	$\triangleq \frac{\text{total reaction time}}{\text{total number of incidents intercepted}}$

Table 2. Key parameters related to incident types

Incident Type	Weight	Number of Incidents Observed	Demand per Incident (hrs)
Drifting	0.044	474	8.506
Capsizing	0.249	30	74.533
Grounding	0.060	11	7.182
Fire	0.188	4	11.500
Collision	0.139	2	3.000
Flooding	0.085	34	10.618
Missing	0.119	43	24.930
Medical Asst.	0.116	118	2.381

Table 3. Key parameters related to boat types (For confidentiality purposes, some parameters are not presented in this table)

Boat Type	Range (nm)	Speed (kts)	Variable Cost ($M/hr)
*B*1	300	22	0.00417
*B*2	110	27	0.00080
*B*3	100	27	0.00071
*B*4	95	27	0.00081
*B*5	90	18	0.00060
*B*6	75	45	0.00052
*B*7	65	47	0.00070
*B*8	55	62	0.00051
*B*9	20	54	0.00041

As the allocation plan input, we used the plan obtained from IB-BAM strategy #12 in Razi and Karatas (2016)'s paper. In that strategy, the optimization model activates 13 ports and utilizes 8 different boat types. TurCG defines the threshold of the critical response time to an incident as 0.5 hours for all types of incidents.

To generate incident input data, we divided the area of interest, The Aegean Sea sub-responsible region, into 0.25x0.25 degree-sized grids with respect to incident

Figure 3. (a) Incident locations occurred in 2014. Solid line represents the TurCG responsibility zone border. (b) Superincident (*) and port (●) locations (c) Grid structure of sub-responsible region

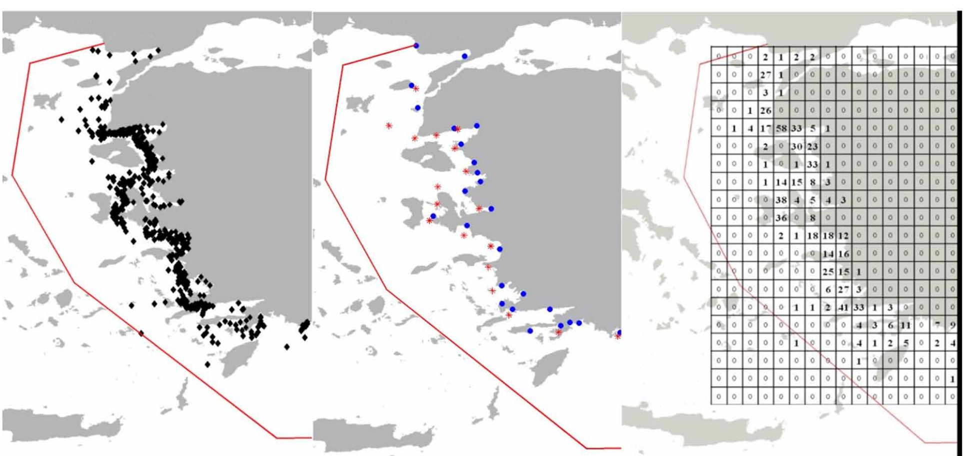
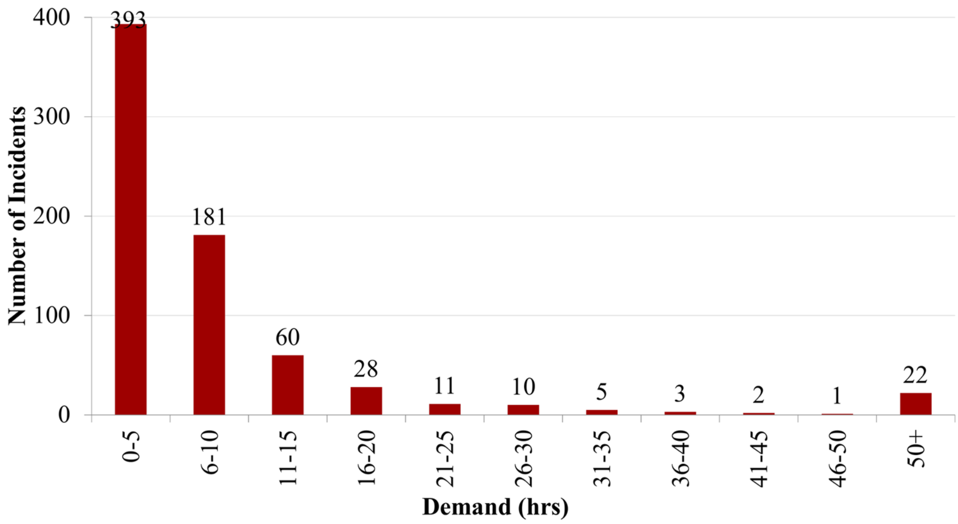


Figure 4. Demand distribution



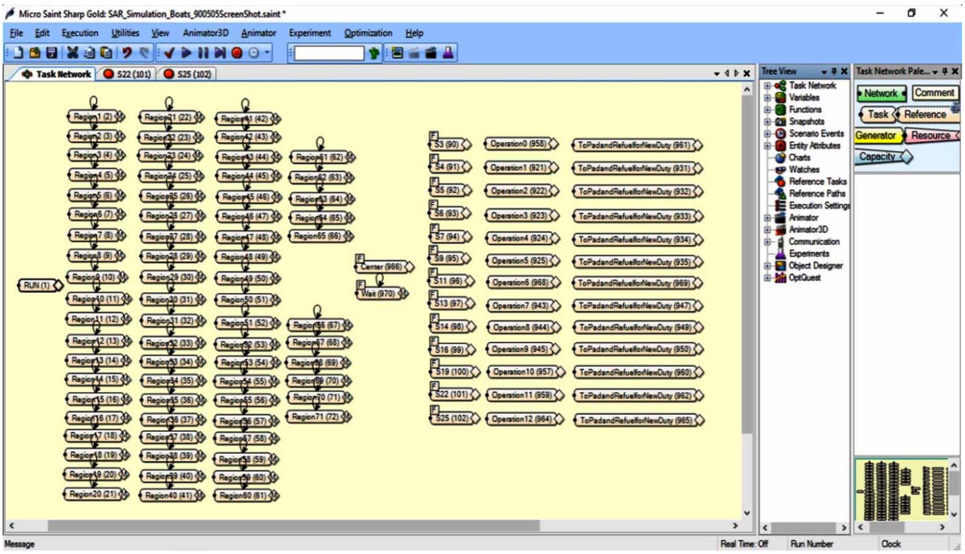
density. Figure 3 displays (a) the locations of the 716 incidents (each represented by a diamond) having occurred in the Aegean Sea sub-responsible region throughout, (b) the 18 superincidents derived by the IB-BAM ZDM and all candidate ports, and (c) generated grid structure of the area of interest.

In grid view structure, we confronted with 71 regions where at least one incident was observed. It is assumed that incident creation is a Poisson process. After an incident type breakdown, the inter-incident time distribution for each incident type in a grid is computed as an exponential distribution with a mean of (1 year)/(number of incidents of that type). We further assume that incidents are distributed in sub-areas random uniformly. To determine the demand (required operation time) distribution, we analyzed the demand size of all incidents (see Figure 4 for a histogram of demand hours). Our analysis showed that distribution of operation times fit in the geometric distribution with parameter $p = 0.00147$/min. Consequently, we utilized the allocation plan obtained from strategy #12 to supply stochastic demands that were generated in a grid for evaluating the performance of optimization model.

Simulation Model

The structure of SimModel-1 is shown in Figure 5. Each grid is represented by 71 task modules on the left side of the figure. Incident entity that is generated in a grid takes a step forward and enters into the "Center" task module. In the "Center", the model tries to determine port and boat assignments and sends incident entity to the determined port task. However, in case of no idle boat, incident entity lines up in

Figure 5. Simulation model structure of SimModel-1 in Micro Saint Sharp©



the queue (FIFO) in "Waiting" task module to wait for an idle capable boat. Port modules represent the proceeding process to incident locations. Then, incident entity follows the path to "Operation#" task where SAR operation is conducted. Finally, task groups on the right side of the figure release boats which complete the duty and collects all related data.

In SimModel-2, we utilized 18 zones obtained from data aggregation (ZDM) to represent regions in which incidents occur. Except this difference, we formulated SimModel-2 with the same assumptions and business rules implemented in SimModel-1. The structure of SimModel-2 is shown in Figure 6:

Results of Simulation Model

Simulation models were performed 2000 times for each business rule and selection criteria. Table 4 displays results of both optimization model and simulation model with grids (SimModel-1). Best values for the simulation model results are highlighted in bold.

Firstly, results show that both optimization model and SimModel-1 provide no risk in budget. As we apply the allocation plan of analytic approach in simulation models, ratio of utilized fleet (MoE_8) values and surely fixed costs are equal for each experiment. SimModel-1 uses 94.83% of the budget at most whereas assigned boats exceed total of 1118 hours in the AOC. Secondly, in the case where AOC exceedance is not allowed (optimization model assumption), there is difference

Figure 6. Structure of the SimModel-2 in Micro Saint Sharp©

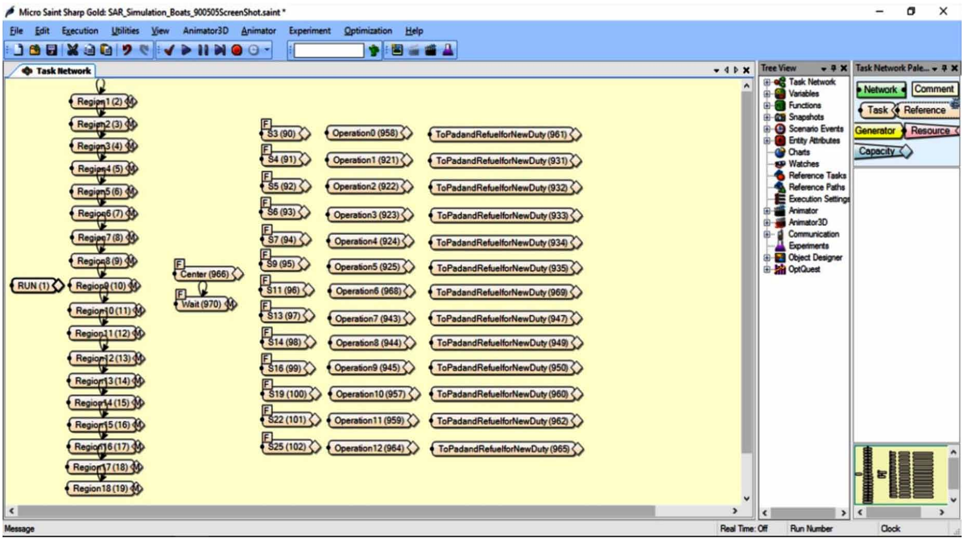


Table 4. Results of optimization model and SimModel-1

MoE#	IB-BAM Result	Simulation Model Results							
		Case-I: Shortage on the AOC 0%		Case-II: Shortage on the AOC 10%		Case-III: Shortage on the AOC 20%		Case-IV: AOC Unlimited	
		Remaining Capacity	Speed	Remaining Capacity	Speed	Remaining Capacity	Speed	Remaining Capacity	Speed
MoE$_1$	2.14	193.69	224.15	170.06	189.20	141.44	140.13	79.39	**42.69**
MoE$_2$	0.38	14.60	16.05	12.75	13.93	10.72	10.50	6.16	**3.47**
MoE$_3$	0	0	0	0	0	0	0	0	0
MoE$_4$	94.00%	93.07%	93.30%	94.09%	94.17%	94.83%	94.46%	94.78%	**91.99%**
MoE$_5$	224	693	**612**	914	983	1231	1598	2331	4680
MoE$_6$	39	**154**	183	624	692	1118	1311	2082	4016
MoE$_7$	263	847	**795**	1538	1675	2349	2909	4413	8696
MoE$_8$	92.00%	92.00%	92.00%	92.00%	92.00%	92.00%	92.00%	92.00%	92.00%
MoE$_9$	100%	92.38%	93.35%	95.84%	96.54%	98.89%	98.89%	**99.86%**	**99.86%**
MoE$_{10}$	100%	92.36%	93.43%	95.96%	96.72%	98.98%	98.95%	**99.94%**	**99.94%**
MoE$_{11}$	302.532	438.89	470.442	422.259	440.418	397.722	391.159	321.743	**256.247**
MoE$_{12}$	0.422	0.658	0.698	0.610	0.632	0.557	0.548	0.446	**0.355**

between analytic and SimModel-1 in terms of total delay (MoE_1) gets its highest value. The optimization model provides 2.143 hours of total delay whereas SimModel-1 results in 193.69 and 224.146 hours of total delay. Besides, reaction time per incident (MoE_{12}) increases by 55.7% even if 7.62% of incidents are not responded (MoE_9). Particularly, 0.658 hours of reaction time per incident (MoE_{12}) indicates that SAR boats are getting late to each incident about 9 minutes in SimModel-1.

With the other three alternative business rules, SimModel-1 provides better solutions in terms of MoE_1, MoE_9, MoE_{10}, MoE_{11} and MoE_{12}. However, ratio of the budget used (MoE_4) worsens especially when "Remaining Capacity" criterion is implemented. As stated in Table 3, larger-capacitated units have a higher variable cost than smaller-faster ones. Thus, SimModel-1 is to bear a higher cost when the "Remaining Capacity" criterion is applied. In the case where 10% exceedance on the AOC is allowed, total delay (MoE_1) decreases by 15.6% and boats respond to each incident almost 4 minutes earlier (MoE_{12}). Besides, exceedance on supply capacity provides 3.5% more incidents to be intercepted. In the case that permits 20% exceedance on the AOC, boats respond to almost %98.9 of stochastically generated incidents while 2349 and 2909 hours of deviation on the AOC occurs. The model provides 25.9% improvement on total delay (MoE_1) when the "Speed" criterion is implemented. Besides, reaction time per incident (MoE_{12}) decreases to 33 minutes.

In the last case that allows full relaxation on capacity policy, SimModel-1 with "Speed" criterion dominates the model with "Remaining Capacity" in all MoE values except MoE_5, MoE_6 and MoE_7. The model provides this dominance along with a %3 lower budget. Outputs of this experiment indicate that we can have at least 42.69 hours of total delay (MoE_1), even though we utilize uncapacitated boats in the model. However, the model provides 0.3554 hours of reaction time per incident (MoE_{12}), which means responding to each incident in almost 21 minutes.

To sum up, the first three business rules (cases) in SimModel-1 yields higher values for the reaction time per incident (MoE_{12}) when compared with the optimization model. As we relax the capacity policy, total delay (MoE_1), ratio of incidents intercepted (MoE_9) and response time per incident (MoE_{12}) values decrease drastically and align with the analytic solution. For the last business rule (unlimited capacity), SimModel-1 provides the best values for all MoEs with the maximum deviation on the AOC. In order to summarize the scene, we displayed response time of each incident in Figures 7 and 8.

In Table 5, we presented the results of SimModel-2 which is demonstrated with data aggregation (ZDM) technique. Best values for the simulation model results are highlighted in bold.

Before we discuss results of all cases individually, there are a number of general points that should be mentioned about simulation model outputs. Firstly, "Speed" criterion in Case-IV is the dominant experiment over all tests in terms of all MoEs

Figure 7. Response time of each incident with "Remaining Capacity" (SimModel-1)

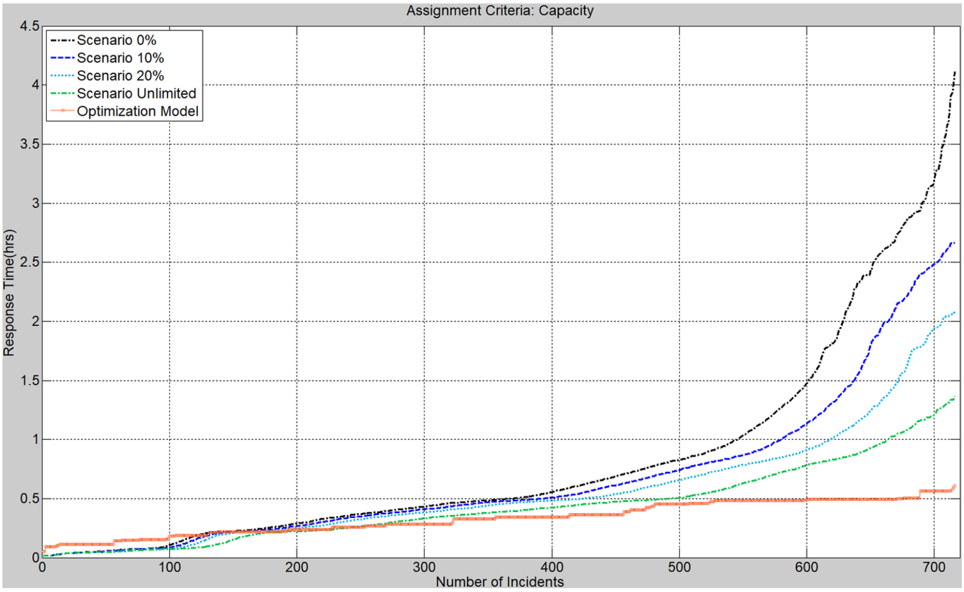


Figure 8. Response time of each incident with "Speed" (SimModel-1)

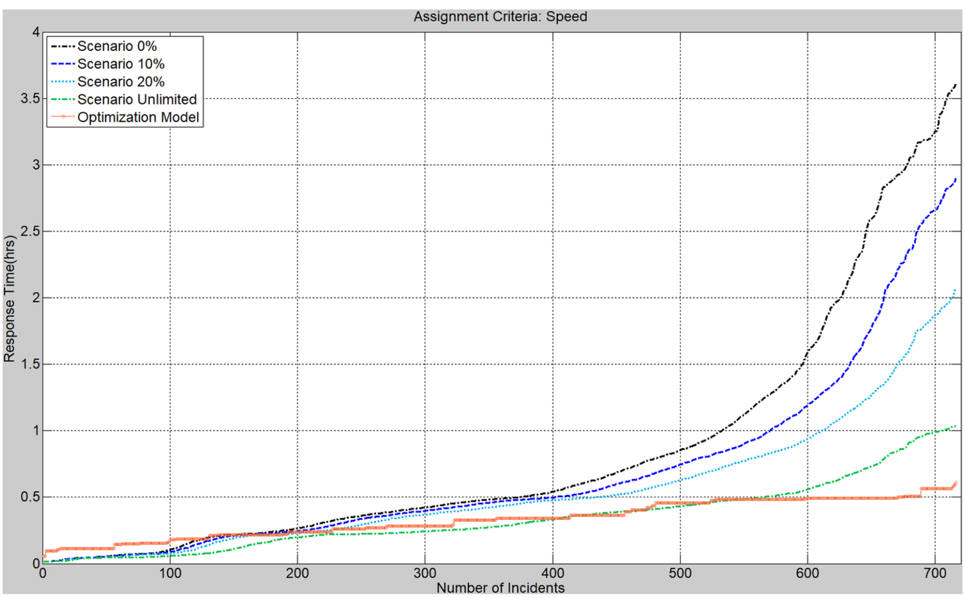


Table 5. Results of optimization model and SimModel-2

MoE#	IB-BAM Result	Simulation Model Results							
		Case-I: Shortage on the AOC 0%		Case-II: Shortage on the AOC 10%		Case-III: Shortage on the AOC 20%		Case-IV: AOC Unlimited	
		Remaining Capacity	Speed	Remaining Capacity	Speed	Remaining Capacity	Speed	Remaining Capacity	Speed
MoE_1	2.14	97.45	128.28	58.99	89.46	53.48	58.88	26.01	**9.12**
MoE_2	0.38	6.33	8.39	4.16	6.15	3.78	4.18	1.99	**0.89**
MoE_3	0	0	0	0	0	0	0	0	0
MoE_4	94.00%	93.07%	93.12%	94.41%	93.80%	94.30%	93.89%	94.23%	**91.50%**
MoE_5	224	**891**	967	1203	1506	1245	1910	1412	4157
MoE_6	39	**158**	204	680	695	718	1056	900	3201
MoE_7	263	**1049**	1171	1883	2201	1963	2966	2312	7358
MoE_8	92.00%	92.00%	92.00%	92.00%	92.00%	92.00%	92.00%	92.00%	92.00%
MoE_9	100%	94.18%	94.46%	98.61%	97.51%	98.89%	98.48%	**100.00%**	**100.00%**
MoE_{10}	100%	93.96%	94.38%	98.41%	97.33%	98.82%	98.44%	**99.86%**	**99.86%**
MoE_{11}	302.532	325.73	353.666	295.84	317.424	289.287	284.53	260.39	**208.853**
MoE_{12}	0.422	0.479	0.519	0.415	0.451	0.405	0.400	0.361	**0.289**

(except MoE_7). However, for other cases, the model with "Speed" criterion provides worse values in total delay (MoE_1) and total deviation on the AOC (MoE_7). Secondly, the model provides reaction time per incident (MoE_{12}) value under the critical time threshold (0.5 hour) in all cases (except the first case with "Speed" criterion). Finally, as in SimModel-1, implemented budget is enough to conduct each business rule and the model spends 0.41% more funds than the optimization model does at most.

In the first case, SimModel-2 is far worse than the optimization model in terms of total delay (MoE_1), even though there is not much difference in the other MoEs. While the total delay in optimization model is 2.143 hours, boats respond to incidents with 97.45 and 128.278 hours of total delay (MoE_1) in SimModel-2. SimModel-2 also provides five times higher exceedance on the AOC (MoE_6) than the optimization model does. Even if 158 and 204 hours of exceedance occur on the AOC, approximately 5.5% of generated incidents cannot be responded by any capable boat. For intercepted incidents, mean time to be responded is about 28.75 minutes (Remaining Capacity) and 31.11 minutes (Speed). In addition, SimModel-2 utilizes 1% lower budget than the analytic approach does.

SimModel-2 improves the delay time about 40% (Remaining Capacity) and 30% (Speed) when 10% exceedance is allowed on the AOC. With this relaxation, total exceedance (MoE_6) jumps from 158 and 204 hours to 680 and 695 hours. Moreover,

Figure 9. Response time of each incident with "Remaining Capacity" (SimModel-2)

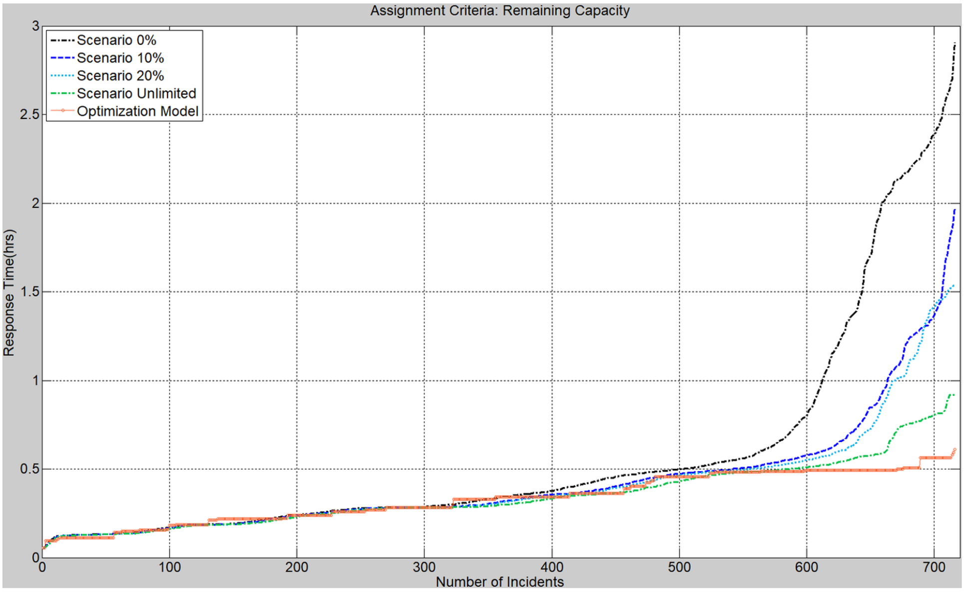
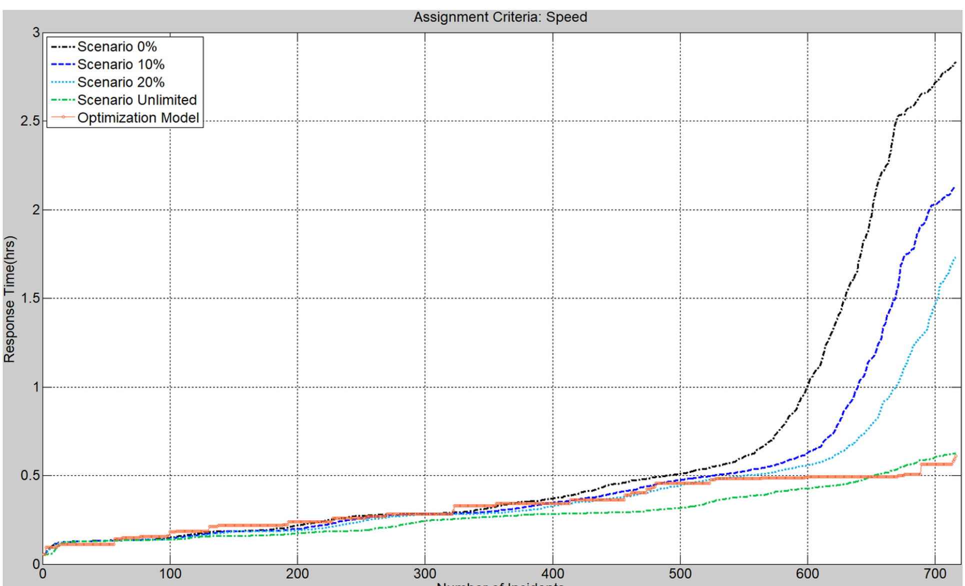


Figure 10. Response time of each incident with "Speed" (SimModel-2)



ratio of incidents intercepted (MoE_9) increases by 4% and reaction time per incident (MoE_{12}) decreases by 13% to 24.9 and 27 minutes. Along with these improvements, ratio of the budget used (MoE_4) worsens about 1%. When relaxation on the AOC is expanded to 20% (Case-III), we confront with a different improvement ratio for each selection criterion. Total delay (MoE_1) decreases by 35% with the "Speed" criterion while it is by 10% with that of "Remaining Capacity". This difference also appears in the reaction time per incident (MoE_{12}). While boats respond to incidents 0.6 minutes earlier with the "Remaining Capacity" criterion, reaction time per incident (MoE_{12}) decreases to 24 minutes in the other criterion.

In the last case, the most important point is to mention the ratio of incidents intercepted (MoE_9). While SimModel-2 cannot provide full coverage in other cases, it responds to all generated incidents in Case-IV. Total delay (MoE_1) also gets the lowest value of 9.119 hours with the "Speed" criterion whereas reaction time per incident decreases to 17.3 minutes. Furthermore, SimModel-2 utilizes 2.5% lower budget than the optimization model itself, with that, boats exploit the highest exceedance on the AOC with 3201 hours.We plotted the response time of each incident in Figures 9 and 10 in order to visualize the dominance of any cases in terms of that factor.

DISCUSSION

When we compare results of simulation models with IB-BAM results, we notice that there is a significant difference in terms of total delay (MoE_1). However, with the capacity relaxation (Case-II, Case-III and Case-IV), MoE_1, MoE_{11} and MoE_{12} improve and the value of total delay (MoE_1) starts getting closer to output of optimization model. Making use of the "Remaining Capacity" selection criterion, the operation center assigns the boat with more available capacity in case of an incident and maintains balanced workload at a port. As high-capacity units are slower, the operation center begins operations with slower units and utilizes them till their capacity gets equal with the faster ones. This approach provides better solutions than other selection criterion when limited capacity policy is conducted (Case-I and Case-II). However, results of this criterion worsen when boat capacities are unbounded.

SimModel-1 gives the best solution with "Speed" selection criterion in Case-IV that allows using boats unrestrictedly. Total delay (MoE_1) has the value of 42.69 hours at least whereas the optimization model provides 2.143 hours. The model also improves reaction time per incident (MoE_{12}) for four minutes. In this criterion, as boat capacities are unbounded, operation center assigns the fastest available boat for each incident that occurs in range. Thus, incidents near to the shore are responded in a short time, which decreases the total reaction time (MoE_{11}) and reaction time per incident (MoE_{12}) for sure. As expected, bigger units have long range but low speed. Therefore, operation center assigns slower boats when the incident occurs far from the port (long distance), which undoubtedly causes delay.

Despite the improvement in reaction time per incident (MoE_{12}), a number of incidents are responded late even though the model allows using faster boats unrestrictedly. It is clear that the main reason of this problem is the data aggregation in optimization model. The optimization model utilizes each incident on the superincident of its zone whereas the SimModel-1 applies grid structure that generates the incident in nearly its real location and provides longer distances than data aggregation. In some cases, the boat spends more time in proceeding to incident than the operation time on scene. Therefore, proceeding to far distances consumes a considerable amount of supply from annual capacity and makes the boat out of order earlier than expected in terms of capacity limitation. In the beginning, the model responds to incidents within 30 minutes since all boat types are operable. However, reaction time to incident increases especially when faster boats start to get out of order. It can also be seen in Figures 9 and 10 that response time to incidents rises up to 2-4 hours with capacity limitation.

To reveal the effects of data aggregation clearly, we generate SimModel-2 which utilizes 18 zones directly obtained from the ZDM. Although there is a significant difference between optimization model and SimModel-2 in terms of total delay (MoE_1) in Case-I (optimization model assumption), SimModel-2 yields 97.45 and 128.278 hours of total delay that are approximately %50 lower than those of SimModel-1. The benefit of data aggregation in SimModel-2 rises to 60%-65% with higher percentages of relaxed capacity (Case-II and Case-III). However, SimModel-2 provides the best results when boats are utilized unrestrictedly with the "Speed" criterion (Case-IV). In this case, boats respond to all generated incidents with a total delay of 9.119 hours and reaction time per incident decreases to 17.3 minutes. According to this result, using grid structure to generate demand undoubtedly results in five times worse result than the model with data aggregation. However, it can be assumed that 9.119 hours of total delay in 716 incidents is negligible and SimModel-2 gets close to the optimization model in terms of total delay (MoE_1). Along with data aggregation, scheduling is another reason for the delays in the system. The optimization model locates SAR resources according to supply-demand relation and does not consider scheduling which is also an important factor that deteriorates performance of the optimization model. In real world, more than one incident may occur simultaneously and there could not be enough idle resources to respond them all. In that case, the incident waits for an idle boat and delay happens. As we develop two DES models, scheduling factor is taken into consideration and causes delays in a number of incidents.

The other factor that causes delay in the system is the stochastic demand data. We believe that solving simulation models by using the "exact" locations of the incidents as in optimization model would be a repetition of the past in terms of model input data. Instead, we utilize stochastic demand that relies on historical data. We believe that this approach would enable models to represent the uncertainty. It also helps the model to be tested for different demand sizes. On the other hand, this demand variability affects operation matters and causes difference in solutions.

Simulation models (SimModel-1 and SimModel-2) help to test the performance of the optimization model in realistic settings where scheduling and stochastic demand data are allowed. Comparison of both models reveals that data aggregation elicits an error in the model regarding the delay to incidents. In other respects, simulation models perform close to the optimization model with regard to total delay and reaction time per incident in the following cases:

- SimModel-1 with the "Speed" criterion in Case-IV,
- SimModel-2 with both criteria in Case-IV.

In real life, we would expect that the operation center would assign the fastest boat without considering the remaining capacity at a given time. Thus, we believe that the analytic model is a good representation of the real world SAR operation process, and decision makers can apply it to manage their SAR organizations.

CONCLUSION

We have developed a model (IB-BAM) for allocating SAR resources in an area of interest. The model consists of three steps: weighting incident types with AHP technique, data aggregation (ZDM) to generate demand data and mo-MIP optimization model that provides optimal allocation plan. It aims at minimizing the following three objectives: total weighted delay over critical time threshold, exceedance on budget and deviation on the annual operation capacity of boats. To observe its performance, we utilized our model to locate SAR resources into ports along the Aegean Sea. The model was performed for 15 different weighting strategies. Results show that the optimization model helps decision makers respond to 716 incidents with only a three-minute delay in total. The sensitivity analysis shows that respond to incidents within a pre-defined time threshold is only achievable with the help of analytic approach which locates SAR resources optimally.

Along with this result, we developed simulation models (SimModel-1 and SimModel-2) to test results of the optimization model in real world settings. Scheduling and stochastic demand are considered and three different capacity policies are performed. Outputs of both models indicate that simulation models provide similar results with the optimization model under fully relaxed capacity policy. Scheduling and stochastic demand are considered and three different capacity policies are performed. Outputs of both models indicate that simulation models provide similar results with the optimization model under fully relaxed capacity policy.

In this thesis, we applied deterministic inputs into the optimization model. As a future study, stochastic and fuzzy theory can be used to determine the demands in the problem. It enables forecasting future incident rates and also makes the model more flexible to deal with different possible scenarios. As another future study, a combined model utilizing both aircraft and surface units together may be developed to organize joint SAR operations.

Disclaimer

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of any affiliated organization or government.

REFERENCES

Aboueljinane, L., Jemai, Z., & Sahin, E. (2012, December). Reducing ambulance response time using simulation: The case of Val-de-Marne department Emergency Medical Service. *Simulation Conference (WSC) Proceedings of the*, *2012*(Winter), 1–12.

Aboueljinane, L., Sahin, E., & Jemai, Z. (2013). A review on simulation models applied to emergency medical service operations. *Computers & Industrial Engineering*, *66*(4), 734–750.

Aboueljinane, L., Sahin, E., Jemai, Z., & Marty, J. (2014). A simulation study to improve the performance of an emergency medical service: Application to the French Val-de-Marne department. *Simulation Modelling Practice and Theory*, *47*, 46–59.

Afshartous, D., Guan, Y., & Mehrotra, A. (2009). US Coast Guard air station location with respect to distress calls: A spatial statistics and optimization based methodology. *European Journal of Operational Research*, *196*(3), 1086–1096.

Amer, M., & Daim, T. U. (2011). Selection of renewable energy technologies for a developing county: A case of Pakistan. *Energy for Sustainable Development*, *15*(4), 420–435.

Amiri, M. P. (2010). Project selection for oil-fields development by using the AHP and fuzzy TOPSIS methods. *Expert Systems with Applications*, *37*(9), 6218–6224.

Balcik, B., & Beamon, B. M. (2008). Facility location in humanitarian relief. *International Journal of Logistics*, *11*(2), 101–121.

Banks, J. (1999). Introduction to simulation. In *Simulation Conference Proceedings*, 1999 Winter (Vol. 1, pp. 7-13). IEEE.

Burke, J. F., Love, R. J., Macal, C. M., Howard, D. L., & Jackson, J. (2000). *Modeling force deployment from army installations using the transportation system capability (TRANSCAP) model*. Argonne National Laboratory.

Byrne, P. J., & Heavey, C. (2006). The impact of information sharing and forecasting in capacitated industrial supply chains: A case study. *International Journal of Production Economics*, *103*(1), 420–437.

Dağdeviren, M., Yavuz, S., & Kılınç, N. (2009). Weapon selection using the AHP and TOPSIS methods under fuzzy environment. *Expert Systems with Applications*, *36*(4), 8143–8151.

Esnaf, Ş., & Küçükdeniz, T. (2009). A fuzzy clustering-based hybrid method for a multi-facility location problem. *Journal of Intelligent Manufacturing*, *20*(2), 259–265.

Francis, R. L., Lowe, T. J., Rayco, M. B., & Tamir, A. (2009). Aggregation error for location models: Survey and analysis. *Annals of Operations Research*, *167*(1), 171–208.

Fredrikson, A., North, C., Plaisant, C., & Shneiderman, B. (1999, November). Temporal, geographical and categorical aggregations viewed through coordinated displays: a case study with highway incident data. In *Proceedings of the 1999 workshop on new paradigms in information visualization and manipulation in conjunction with the eighth ACM internation conference on Information and knowledge management* (pp. 26-34). ACM.

Fu, M. C. (1994). Optimization via simulation: A review. *Annals of Operations Research*, *53*(1), 199–247.

Giuliani, J. (2015, April 14). *The Challenge of Illegal Immigration in the Mediterranean*. Retrieved from http://www.robert-schuman.eu/en/doc/questions-d-europe/qe-352-en.pdf

Goerlandt, F., Torabihaghighi, F., & Kujala, P. (2013). A model for evaluating performance and reliability of the voluntary maritime rescue system in the Gulf of Finland. In *11th International Probabilistic Safety Assessment and Management Annual European Safety and Reliability Conference* (pp. 1-6). Academic Press.

Goldsman, D., & Goldsman, P. (2015). *Modeling and Simulation in the Systems Engineering Life Cycle*. London: Springer.

Green, L. V., & Kolesar, P. J. (2004). Anniversary article: Improving emergency responsiveness with management science. *Management Science*, *50*(8), 1001–1014.

Grodzevich, O., & Romanko, O. (2006). Normalization and other topics in multi-objective optimization. In *Proceedings of the Fields–MITACS Industrial Problems Workshop* (pp.89-101.), Toronto, Canada: Academic Press.

Günal, M. M., & Pidd, M. (2010). Discrete event simulation for performance modelling in health care: A review of the literature. *Journal of Simulation*, *4*(1), 42–51.

Herva, M., & Roca, E. (2013). Ranking municipal solid waste treatment alternatives based on ecological footprint and multi-criteria analysis. *Ecological Indicators*, *25*, 77–84.

Ho, W. (2008). Integrated analytic hierarchy process and its applications–A literature review. *European Journal of Operational Research*, *186*(1), 211–228.

Ingolfsson, A., Erkut, E., & Budge, S. (2003). Simulation of single start station for Edmonton EMS. *The Journal of the Operational Research Society*, *54*(7), 736–746.

Ishizaka, A., Balkenborg, D., & Kaplan, T. (2011). Does AHP help us make a choice? An experimental evaluation. *The Journal of the Operational Research Society*, *62*(10), 1801–1812.

Işıklar, G., & Büyüközkan, G. (2007). Using a multi-criteria decision making approach to evaluate mobile phone alternatives. *Computer Standards & Interfaces*, *29*(2), 265–274.

Jahangirian, M., Eldabi, T., Naseer, A., Stergioulas, L. K., & Young, T. (2010). Simulation in manufacturing and business: A review. *European Journal of Operational Research*, *203*(1), 1–13.

Jain, A. K. (2010). Data clustering: 50 years beyond K-means. *Pattern Recognition Letters*, *31*(8), 651–666.

Jain, A. K., & Dubes, R. C. (1988). *Algorithms for clustering data*. Prentice-Hall, Inc.

Karacan, İ. (2015). *A New Hybrid Decision Support Tool and an Application to Health Technology Selection* (Doctoral dissertation). Naval Science and Engineering Institute, Department of Operations Research, Turkish Naval Academy.

Karatas, M. (2017). A multi-objective facility location problem in the presence of variable gradual coverage performance and cooperative cover. *European Journal of Operational Research*, *262*(3), 1040–1051.

Karatas, M. (2018). Optimal Deployment of Heterogeneous Sensor Networks for a Hybrid Point and Barrier Coverage Application. *Computer Networks*, *132*(26), 129–144. doi:10.1016/j.comnet.2018.01.001

Karatas, M., Razı, N., & Gunal, M. (2017). An ILP and Simulation Model to Optimize Search and Rescue Helicopter Operations. *The Journal of the Operational Research Society*, 1–17. doi:10.105741274-016-0154-7

Karatas, M., & Yakıcı, E. (2018). An iterative solution approach to a multi-objective facility location problem. *Applied Soft Computing*, *62*, 272–287.

Kerdprasop, K., Kerdprasop, N., & Sattayatham, P. (2005). Weighted k-means for density-biased clustering. *Data Warehousing and Knowledge Discovery*, 488-497.

Kodinariya, T. M., & Makwana, P. R. (2013). Review on determining number of Cluster in K-Means Clustering. *International Journal (Toronto, Ont.)*, *1*(6).

Korpela, J., & Tuominen, M. (1996). A Decision Aid in Warehouse Site Selection. *International Journal of Production Economics*, *45*(1), 169–180.

Li, J., Prins, C., & Chu, F. (2012). A Scatter Search for A Multi-Type Transshipment Point Location Problem with Multicommodity Flow. *Journal of Intelligent Manufacturing*, *23*(4), 1103–1117.

Liao, K., & Guo, D. (2008). A Clustering-Based Approach to the Capacitated Facility Location Problem. *Transactions in GIS*, *12*(3), 323–339.

Lirn, T. C., Thanopoulou, H. A., Beynon, M. J., & Beresford, A. K. C. (2004). An application of AHP on transhipment port selection: A global perspective. *Maritime Economics & Logistics*, *6*(1), 70–91.

Luthra, S., Kumar, S., Garg, D., & Haleem, A. (2015). Barriers to renewable/sustainable energy technologies adoption: Indian perspective. *Renewable & Sustainable Energy Reviews*, *41*, 762–776.

Nemes, M. I., Carvalho, H. B., & Souza, M. F. (2004). Antiretroviral therapy adherence in Brazil. *AIDS (London, England)*, *18*, S15–S20. PMID:15322479

Nogueira, L. C., Pinto, L. R., & Silva, P. M. S. (2016). Reducing Emergency Medical Service response time via the reallocation of ambulance bases. *Health Care Management Science*, *19*(1), 31–42. PMID:24744263

Onggo, B. S., & Karatas, M. (2015, December). Agent-based model of maritime search operations: A validation using test-driven simulation modelling. In *Winter Simulation Conference (WSC)*, 2015 (pp. 254-265). IEEE.

Onggo, B. S., & Karatas, M. (2016). Test-driven simulation modelling: A case study using agent-based maritime search-operation simulation. *European Journal of Operational Research*, *254*(2), 517–531.

Parsons, D. J., & Krause, L. C. (1999). Tactical logistics and distribution systems (TLoaDS) simulation. In *Simulation Conference Proceedings*, 1999 Winter (Vol. 2, pp. 1174-1178). IEEE.

Razi, N., & Karatas, M. (2016). A multi-objective model for locating search and rescue boats. *European Journal of Operational Research*, *254*(1), 279–293.

Razi, N., Karatas, M., & Gunal, M. M. (2016). A Combined Optimization and Simulation Based Methodology for Locating Search and Rescue Helicopters. In *Proceedings of the 2016 Spring Simulation Conference*. IEEE Press.

Ren, J., & Sovacool, B. K. (2014). Enhancing China's energy security: Determining influential factors and effective strategic measures. *Energy Conversion and Management*, *88*, 589–597.

Sahraeian, R., & Kazemi, M. S. (2011, December). A fuzzy set covering-clustering algorithm for facility location problem. In *Industrial Engineering and Engineering Management (IEEM), 2011 IEEE International Conference on* (pp. 1098-1102). IEEE.

Shawki, K. M., Kilani, K., & Gomaa, M. A. (2015). Analysis of earth-moving systems using discrete-event simulation. *Alexandria Engineering Journal*, *54*(3), 533–540.

Sivilevičius, H., & Maskeliūnaite, L. (2010). The criteria for identifying the quality of passengers' transportation by railway and their ranking using AHP method. *Transport*, *25*(4), 368–381.

Smith, J. S. (2003). Survey on the use of simulation for manufacturing system design and operation. *Journal of Manufacturing Systems*, *22*(2), 157–171.

Stein, E. W. (2013). A comprehensive multi-criteria model to rank electric energy production technologies. *Renewable & Sustainable Energy Reviews*, *22*, 640–654.

Tibshirani, R., Walther, G., & Hastie, T. (2001). Estimating the number of clusters in a data set via the gap statistic. *Journal of the Royal Statistical Society. Series B, Statistical Methodology*, *63*(2), 411–423.

UNHCR. (n.d.). *Global Appeal 2015 Update*. Retrieved from http://www.unhcr.org/5461e5f80.html

Vaidya, O. S., & Kumar, S. (2006). Analytic hierarchy process: An overview of applications. *European Journal of Operational Research*, *169*(1), 1–29.

Varol, A. E., & Gunal, M. M. (2015). Simulating prevention operations at sea against maritime piracy. *The Journal of the Operational Research Society*, *66*(12), 2037–2049.

Wei Lam, S. S., Zhang, Z. C., Oh, H. C., Ng, Y. Y., Wah, W., & Hock Ong, M. E. (2014). Reducing ambulance response times using discrete event simulation. *Prehospital Emergency Care*, *18*(2), 207–216. PMID:24134647

Williams, E. J., & Çelik, H. (1998, December). Analysis of conveyor systems within automotive final assembly. In *Proceedings of the 30th conference on Winter simulation* (pp. 915-920). IEEE Computer Society Press.

Wu, C. H., & Hwang, K. P. (2009). Using a Discrete-event Simulation to Balance Ambulance Availability and Demand in Static Deployment Systems. *Academic Emergency Medicine*, *16*(12), 1359–1366. PMID:20053259

Yıldırım, U. Z., Tansel, B. Ç., & Sabuncuoğlu, İ. (2009). A multi-modal discrete-event simulation model for military deployment. *Simulation Modelling Practice and Theory*, *17*(4), 597–611.

Zhen, L., Wang, K., Hu, H., & Chang, D. (2014). A simulation optimization framework for ambulance deployment and relocation problems. *Computers & Industrial Engineering*, *72*, 12–23.

Zitzler, E., & Thiele, L. (1999). Multiobjective evolutionary algorithms: A comparative case study and the strength Pareto approach. *IEEE Transactions on Evolutionary Computation*, *3*(4), 257–271.

This research was previously published in Operations Research for Military Organizations edited by Hakan Tozan and Mumtaz Karatas; pages 67-97, copyright year 2019 by Information Science Reference (an imprint of IGI Global).

Section 2

Security and Law Enforcement

Chapter 8
Introducing Predictive Policing Technologies (PPT): An Action Research-Oriented Approach for EBOCD Initiatives

Peter Watt
York St. John University, UK

George Boak
York St. John University, UK

Marija Krlic
York St. John University, UK

Dawn Heather Wilkinson
West Yorkshire Police, UK

Jeff Gold
York Business School, UK

ABSTRACT

This reflective case-history presents the findings of a 12-week pilot study of a collaborative organizational change project which oversaw the implementation of predictive policing technology (PPT) into a territorial police force in the North of England. Based on the first year of a two-year initiative, the reflections consider the impact on the future of the project and their potential future application and cultural embeddedness, beyond the organizational and time-bound specifics of this case.

DOI: 10.4018/978-1-7998-2535-7.ch008

INTRODUCTION

This reflective case-history presents the case of a 12-week pilot-study of a collaborative organizational change project that sought to oversee the successful implementation of a 'predictive policing technology' (PPT) into a territorial police force in the North of England (West Yorkshire Police, referred to henceforth as 'the Force'). We critically reflect on the process of this evidence-based organizational change and development (EBOCD) initiative, the immediate impact of the initiative, and the research findings. In doing so we provide observations regarding the implementation and use of such technologies and the challenges they represent in relation to organizational change and culture. The question underpinning this research was, 'How can predictive policing technology be culturally embedded?' Our hope is that the findings from this pilot-study can be applied more widely as other districts move to engage with similar technologies as part of further Home Office and policing initiatives (Grierson, 2016).

Context and Drivers of the EBOCD Initiative

The 12-week pilot that forms the focus of this case-history was the first phase of an ongoing 'action research' oriented organizational change project between the Force and a team of academics from a range of backgrounds, disciplines and institutions. The project was funded by the UK Home Office and forms part of a wider strategy that sees academic expertise aligned with a range of challenges and crime-prevention initiatives identified in territorial police forces throughout England and Wales. The overarching aim of the collaboration was to facilitate the successful implementation of PPT, based on a number of regional and criminological factors.

The rationale for these initiatives was premised on statistical evidence which correlates the numbers of police officers available for deployment and patrol in relation to the statistics of reported crime. According to UK Home Office figures, in 2009 the number of police officers in England and Wales stood at 143, 769. Following progressive cuts to the public sector, by 2016 this figure fell to 124, 066; a fall of 14% (Harrison, 2015; BBC News, 2016). Even though reported crime-rates tended to fall during this period, by December 2016 this trend had stalled and in some areas (such as fraud) it had reversed.[1] Consequently, police forces in England and Wales have come under increasing amounts of pressure to deliver more with less. A central challenge is that many forms of crime prevention are based around officers' presence preventing crimes being committed (Farrington, MacKenzie, Sherman, & Welsh, 2003). Therefore, with decreasing numbers of "bobbies on the beat" (Hopkins, 2015), the successful direction and presence of resources to the "right place at the right time" has positioned 'predictive policing technology' as a cornerstone for preventative crime measures in the new digital age of policing on both sides of the Atlantic (Bachner, 2013; Holt, 2017).

One response has been to consider the use of predictive analytical software to aid the efficient and effective deployment of 'visible' patrols. In recent years, a significant increase in the volume, velocity, veracity, variety, and value (referenced in Rahman, 2016; Rahman & Aldhaban, 2015) of data ('big data') has meant that organisations in a range of sectors have sought to leverage the data available to enable 'probabilised' decision-making processes (Allenby, Bradlow, George, Liechty, & McCulloch, 2014).

The foremost expectation held by organizations regarding big data's potential is based around 'predictability' (Agarwal & Dhar, 2014; Bughin, Chui, & Manyika, 2010; Hashem et al., 2015). In crude terms, the size of data available is in positive correlation to the leverage against risk. In other words, the accrual and analysis of big data will provide the opportunity to move on from 'present action' and 'past reflection' towards a 'calculable future', derived from evidence-based data incorporated into an algorithm.

Predictive Policing

Predictive policing has become a key feature of what is known as 'Intelligence-led Policing' (ILP, (Ratcliffe, 2016). According to Beck and McCue (2009, p. 22) predictive policing is concerned with '[t]he ability to anticipate the time, the location, and the nature of the crime' in order to '[support] the police manager's ability to proactively allocate resources – preventing or deterring crime through targeted police presence and enabling response by pre-positioning police assets when and where they are likely to be needed.' This approach is based on predictions derived when large data-sets are processed by an algorithm. The logic behind the algorithm is that certain types of crime follow predictable patterns and therefore resources can be deployed to prevent a crime or act as a deterrent through their presence in specific locations. The use of PPT requires a mediated delivery of the output of reported crime as intelligence through a variety of digital technologies (ICT, smart phones and apps etc.).

However, the success of PPT can be inhibited by two types of factors: factors relating to the predictive ability of the technology to identify the appropriate time and place of the officers' deployment, and factors relating to the technology's uptake, which are based on elements such as the views of the officers, their beliefs in evidence-based practice, the supporting systems that inform and direct them on patrol, and the management of compliance with these requirements. Often best intentions are thwarted through the unintended selection of inappropriate techniques (College of Policing, 2015) or a failure of operational officers to be convinced of the value of patrol plans that are based on prediction, leading to a failure to comply with requirements and implement evidence-based crime prevention (Farrington et al., 2003). Likewise, the perceived or real lack of supporting systems and infrastructure is seen as a factor inhibiting effective and efficient operational delivery. The focus of this reflective case history is primarily in relation to the second type of factors; i.e., relating to the acceptance of the technology and the change in working practices that it entailed.

Organizational Analysis: Making Sense of Technology Acceptance

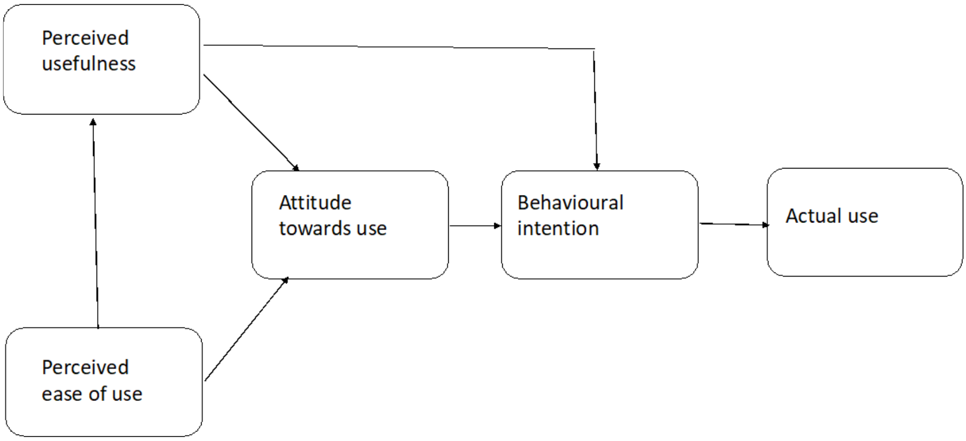
It is a commonplace observation that any attempt to bring about change in organisations may be greeted by a range of responses, from enthusiastic support to indifference or opposition (Beckhard & Harris, 1987). A change may have different potential impacts on those affected by it, and thus will be perceived as a positive development by some stakeholders, and as a negative imposition by others. Attitudes towards a change may be influenced by the manner in which it is introduced, and the extent to which those affected by it accept this method of introduction (Balogun, Hailey & Gustafsson, 2016).

In specific relation to changes concerning the adoption of new technology, the Technology Acceptance Model (TAM) (Davis, 1986, 1989) proposes key factors that are likely to affect the behavioural response to the requirement to change (see Figure 1). Key factors influencing the take-up of information technology by users are the 'perceived usefulness of the technology', and its 'perceived ease of its use'. Later developments of TAM included social influence factors (from colleagues and bosses) that affected perceptions of usefulness and behavioural intention to use the technology (Holden & Karsh, 2010; Turner, Kitchenham, Brerton, Charters & Budgen, 2010).

There is a lack of evidence-based accounts of TAM in police settings, however Lindsey, Jackson and Cooke's model for 'mobile policing' (2011, 2014) was deemed sufficient to provide a framework for a model to apply in our case, adapted to fit the specific requirements and challenges presented by PPT in this context.

We employed TAM in the first instance as an analytical framework, which allowed us to embark on a process of organizational sense-making. This is different from our methodology for reasons we outline below. It was through this analytical framing that we could employ action modes of research (Raelin, 2009) to help gain acceptance of the technology through the production of actionable knowledge (Argyris, 1996) for its progressive implementation throughout the Force.

Figure 1. The TAM
Source: from Holden & Karsh 2010, p. 161)



EVIDENCE-BASED OCD INITIATIVE

An algorithm was developed by a university-based technology team that processed reported crime data for a specific area and generated maps of streets deemed to be at higher risk of further crime, thus indicating priority areas to patrol. The technology was designed to update the maps every 24 hours and to communicate them to the teams of officers responsible for patrolling the area via a tailored application on their hand-held devices (smartphones).

The project was funded by the Home Office, and a project manager within the Force liaised with the range of officers who would be involved, and with academics from three universities who were active in developing and analysing the project. A specific inner city area was chosen to pilot the technology. The focus of the first pilot was chosen by the senior leadership team for the division, and was the crime of domestic burglary.

Action research provided an overall framework for understanding and guiding the project: a collaborative approach was taken to working with police officers at all levels of the Force, to design the pilot, to monitor progress and to address emergent problems as they arose, at the same time generating knowledge as evidence for use in a progressive and cyclical process, starting with diagnosis, questions and planning, leading to action taking (Lewin, 1946) and generating actionable knowledge for wider dissemination (Argyris, 1996).

Meetings were held with senior officers (superintendent and inspectors) responsible for the pilot area, to discuss the working of the project, and to acquire from them a statement of their aims in taking part. From these meetings, three key indicators of success were named:

- A reduction in burglary from dwellings;
- A reduction in calls for service;
- An increase in public confidence.

A meeting was also held with a group of sergeants, to discuss the project and to emphasise the importance of their role. What little research there is on police acceptance of mobile technology (Lindsay et al., 2011, 2014) highlights the influential role of sergeants. Further briefing meetings were held between the project manager, a member of the university research group, and individual sergeants and the police constables (PCs) and the police community support officers (PCSOs) who would use the maps as they patrolled the streets.

The pilot was scheduled to last for 12 weeks. The PCs, PCSOs and the sergeants were asked to use the maps and to report back on their experiences on a regular basis. During the pilot period, 16 meetings were held with sergeants and the officers in their teams at the start of their shift, allowing learning about the working of the technology to be shared with the group and the university researchers. The articulation of what was being learned enabled evidence to emerge of what was working, and what was helping or hindering. The experiences and perceptions of the PCs and PCSOs were sought in a group setting, and then some further information was gathered from each sergeant in a separate interview. Some meetings were also attended by an inspector or the superintendent, to gather information and to contribute to the evaluation.

In the first part of the pilot phase, selected officers in each team were asked to use the technology, and their time was protected ('ring-fenced'). In the second part of the pilot, this ring-fencing was relaxed, and the technology was used by a wider range of officers in the team. Both approaches were evaluated to assess which was more effective.

As the pilot proceeded, different aspects of the use of the technology were discussed and evaluated. Action was taken to make improvements and deal with difficulties, and longer-term actions were identified for future implementation. Information from the team meetings, and from meetings with other officers, was analysed through thematic analysis (Braun & Clarke, 2013), allowing the emergent evidence to be thematised. From this the research team augmented the basic elements of a Technology Acceptance Model (TAM) for use in future phases of the project.

FINDINGS

Certain themes emerged from our discussions with the users of the new system. Of particular interest were factors that appeared to help the system to work, and factors that hindered the system, and thus influenced adoption by the users. Throughout the pilot, officers engaged in processes of sensemaking regarding the new technology, and made adjustments to the ways in which the technology impacted on the work of officers.

Minimal requirements for adoption were the support of senior managers (the Chief Constable, the divisional superintendent and inspectors) and the availability of resources. The early meeting with the divisional superintendent and inspectors, where measures of success for the pilot were discussed and agreed, was an important step. The support of this group of senior managers was also signaled by individuals attending some of the feedback meetings with sergeants and officers.

Resourcing challenges were partly eased by funding from the Home Office for the project, which enabled the project manager to provide the necessary smartphones for PCSOs, and enabled the divisional superintendent to authorize overtime during the pilot period. Resourcing still remained an issue, however, with operational calls on the time of PCs and PCSOs potentially conflicting with the requirements of the system, and some officers seeking time off rather than more overtime. There is a tension between spending time on crime prevention – 'proactive policing' (Clarke, 2006) – and spending time reacting – 'reactive policing' (Scott, 1998) – to reported incidents. This tension between 'proactive' and 'reactive' strategies is central to evidence-based policing matrices (Lum, Koper, & Telep, 2011).

Beyond these minimal requirements of support from senior managers and sufficient resources, major themes arising from discussions with officers concerned the perceived value of the system, which was closely linked to its perceived credibility. Credibility concerned a) the perceived likelihood of the accuracy of the system, b) the perceived plausibility of actual predictions, and c) the effectiveness and reliability of the technology.

In initial briefings for the sergeants and officers, and in subsequent meetings with them, the project manager explained the theory behind patterns of domestic burglaries, using practical examples and demonstrating a good understanding of police approaches to this type of crime. She was also able to explain the volume and type of data that was used by the algorithm, and could give examples of similar systems being used elsewhere. She and the university researchers also emphasized that they wished to get feedback from officers as the pilot progressed, in order to learn how the system could be improved, accepting that adjustments would probably need to be made.

In the early stages of the pilot, queries were raised by some officers about specific predictions, where maps showed locations that did not appear to contain likely premises, or conversely where maps did not indicate a location close to a recent reported crime. In one meeting, officers openly queried the value of the algorithm as compared to the knowledge they had gained through practical experience. The project manager regularly explained that the information from the algorithm should be used alongside the assessment of experienced officers as to which areas to patrol. The question of whether this technology should complement the judgement of experienced officers rather than over-ride it is an important issue in acceptance and operation. As a result of feedback, some adjustments were made to how the algorithm generated maps.

A limitation of the system in the pilot phase was that very little additional information was provided – such as the reason why a particular location had been highlighted for preventive policing. Some officers said that more up-to-date intelligence reports should accompany the patrol plans, to give them a sense of why they were being asked to patrol certain locations, so that the technology could complement their 'craft' and 'beat knowledge'. During the pilot phase, however, it was not possible to link the patrol plans with intelligence in a timely manner.

The effectiveness and reliability of the technology was a third aspect of credibility. Technological 'teething problems' in the early days of the pilot resulted in the maps not changing every 24 hours, as promised, but remaining the same for two weeks. The perceived credibility of the system suffered early damage as a result.

While the perceived value of the system was affected by perceptions of its credibility, another factor of concern was whether it was or would actually be effective in deterring crime.

Deterrence of a crime such as burglary through showing police presence is normally only evidenced in retrospect. During the pilot, officers patrolled the streets indicated by the maps, in addition to their other duties. They were encouraged to be observant and to point out potential risks – such as windows left open – to householders. However, it was not clear to them at the time they were patrolling whether they were being effective in deterring crime. As one sergeant said: 'If you are wandering around and nothing's happening, it's hard for people to see that they are doing a good job'.

Figures on burglaries and incidents were gathered and analyzed at the end of the pilot period. The results were:

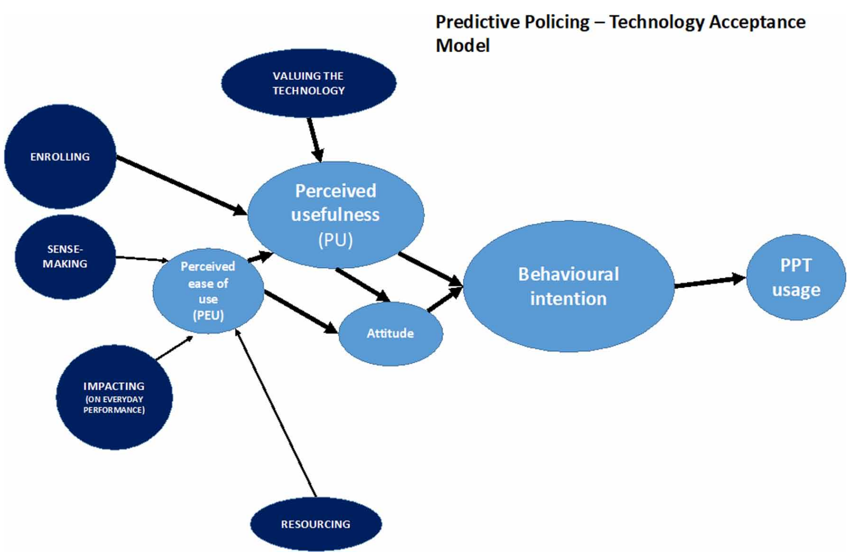
- In the pilot area, burglary dwellings (i.e., domestic burglaries) had fallen relative to the same period the previous year, from 274 to 202 crimes: a reduction of 35.64%
- In the pilot area, burglary dwellings had fallen relative to the previous three months, from 253 to 202 crimes: a reduction of 25.25%
- In the whole district, these crimes had risen relative to the same period the previous year, from 986 to 998: an increase of 1.2%.
- In the whole district, these crimes had risen relative to the preceding three months, from 989 to 998: an increase of 0.9%

Of course, these figures need to be treated cautiously: we are not able to draw firm conclusions on causal links between the project and the figures, but these were at least some positive signs, and they reinforced senior managers' support for the project. Within the teams led by the sergeants, ways of working with the technology had evolved and become accepted. For example, it was found more effective to allocate PPT maps throughout the whole team, rather than ring-fence the time of particular individuals. As one sergeant said at the end of the pilot period: 'It's become part of daily business now.' The review by senior officers at the conclusion of the pilot suggested that the briefing of officers against the maps had become considered 'normal business' with discretion left to sergeants and officers, which is continuing.

DISCUSSION

A variation of the Technology Acceptance Model, the PP-TAM Version 1, was developed in order to analyze the process in this case (see Figure 2). Sensemaking was a constant process, influenced by previous experiences and by attitudes expressed by colleagues, as well as by communications with the project manager and more senior officers. The perception of the extent to which the technology impacted on everyday performance in a positive way, or a negative way, affected perceptions of ease of use, as did resourcing. A key influence on perceived usefulness is the extent to which those involved in the project value the technology, and a critical process is the extent to which various actors, technologies and maps can be enrolled into the activity.

Figure 2. A PP-TAM



Evaluation

It is difficult to determine the extent to which the theory underpinning TAM was successful in our attempt to implement the predictive technology. As stated, the principles underpinning the core of the model have been adapted by others to meet the specific organizational formations and challenges of the Force's culture and structure. Indeed, the quantitative success story that can be told by the comparative figures are only indicators of success. Moving forward, what we have is a working PP-TAM that can continue to be adapted as new data related to the new organizational, methodological, technological and criminological challenges are revealed. This is a crucial basis on which the success of future phases of the project can be based.

Old Insights, New Applications

A central challenge that the pilot uncovered was the view of the technology as something that should *complement* rather than *determine* the conduct of the officers on the beat. At first this might appear to be an obvious and mundane observation. There are certainly more than enough accounts of technologically-oriented organizational change initiatives taking a technological determinist view to development needs. However, moving forward, this challenge is a factor to be reiterated and considered further due to its organizational pertinence regarding the reception to the technology by the Force. This is principally due to the hierarchical structure of the Force and the officer's conduct being channeled by response to 'commands' and the direction of patrol-plans based on intel. As we move forward with the next phases of the project, there are specific challenges as we transferred to different districts, crime-focuses, organizational dynamics (non-ring-fenced provisions) etc. However, underpinning all of these is the essential factor of complementarity in the success of the technology in this pilot phase. This is something that others can learn from, both within the specific Force we are engaged with and more widely as others move forward with similar technologies in other regions as part of wider Home Office and policing initiatives (Grierson, 2016).

CONCLUDING REFLECTIONS

In this chapter we have provided a case history to show how action modes of research, principally action research and action learning research could both support learning of participants and provide evidence to develop a PP-TAM. While the model is based around the conceptualization of abstracted themes, it is made meaningful in the context of continuing work within the Force and beyond through its connection to the evidence. The collaborative nature of this project (between academic researchers and serving police personnel in West Yorkshire) combined with the action modes of research has allowed the benefits of regular access to project participants to develop this actionable knowledge into this early formation discussed in this chapter. The evidence-based nature of this inquiry, and the consolidative nature of the project is deemed of value by both academics and practitioners.

REFERENCES

Agarwal, R., & Dhar, V. (2014). Editorial—big data, data science, and analytics: The opportunity and challenge for IS research. *Information Systems Research*, *25*(3), 443–448. doi:10.1287/isre.2014.0546

Allenby, G. M., Bradlow, E. T., George, E. I., Liechty, J., & McCulloch, R. E. (2014). Perspectives on Bayesian Methods and Big Data. *Customer Needs and Solutions*, *1*(3), 169–175. doi:10.100740547-014-0017-9

Argyris, C. (1996). Actionable knowledge: Design causality in the service of consequential theory. *The Journal of Applied Behavioral Science*, *32*(4), 390–406. doi:10.1177/0021886396324004

Bachner, J. (2013). *Predictive policing: preventing crime with data and analytics*. Johns Hopkins University, IBM Center for the Business of Government.

Beck, C., & McCue, C. (2009). Predictive policing: What can we learn from Wal-Mart and Amazon about fighting crime in a recession? *The Police Chief*, *76*(11), 18–25.

Braun, V., & Clarke, V. (2013). *Successful qualitative research: a practical guide for beginners*. London: Sage.

Bughin, J., Chui, M., & Manyika, J. (2010). Clouds, big data, and smart assets: Ten tech-enabled business trends to watch. *The McKinsey Quarterly*, *56*(1), 75–86.

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. Massachusetts Institute of Technology. Retrieved from https://www.researchgate.net/profile/Fred_Davis2/publication/35465050_A_technology_acceptance_model_for_empirically_testing_new_enduser_information_systems__theory_and_results_/links/0c960519fbaddf3ba7000000.pdf

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Management Information Systems Quarterly*, *13*(3), 319–340. doi:10.2307/249008

Farrington, D. P., MacKenzie, D. L., Sherman, L. W., & Welsh, B. C. (2003). *Evidence-based crime prevention*. London: Routledge. doi:10.4324/9780203166697

Grierson, J. (2016, February 24). Police and academics developing system to map crime hotspots. *The Guardian*.

Harrison, J. (2015, May 20). Are bobbies on the beat "endangered"? *BBC News*. Retrieved from http://www.bbc.co.uk/news/uk-32807677

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. *Information Systems*, *47*, 98–115. doi:10.1016/j.is.2014.07.006

Holt, J. (2017, June 23). "Right place at right time" nets burglary suspects. *The Signal.* Retrieved from https://signalscv.com/2017/06/right-place-right-time-nets-burglary-suspects/

Hopkins, N. (2015, October 27). Bobbies on the beat coming to an end, senior officers say. *BBC News*. Retrieved from http://www.bbc.co.uk/news/uk-34651119

Lewin, K. (1946). Action research and minority problems. *The Journal of Social Issues*, *2*(4), 34–46. doi:10.1111/j.1540-4560.1946.tb02295.x

Lindsay, R., Jackson, T. W., & Cooke, L. (2011). Adapted technology acceptance model for mobile policing. *Journal of Systems and Information Technology*, *13*(4), 389–407. doi:10.1108/13287261111183988

Lindsay, R., Jackson, T. W., & Cooke, L. (2014). Empirical evaluation of a technology acceptance model for mobile policing. *Police Practice and Research*, *15*(5), 419–436. doi:10.1080/15614263.2013.829602

News, B. B. C. (2016, July 21). *Police officer numbers drop by nearly 20,000 since 2009*. Retrieved from http://www.bbc.co.uk/news/uk-36857326

Raelin, J. A. (2009). *Seeking conceptual clarity in the action modalities (SSRN Scholarly Paper No. ID 1558086)*. Rochester, NY: Social Science Research Network.

Rahman, N. (2016). *Factors affecting big data technology adoption*. Student Research Symposium. Retrieved from http://pdxscholar.library.pdx.edu/studentsymposium/2016/Presentations/10/

Rahman, N., & Aldhaban, F. (2015). Assessing the effectiveness of big data initiatives. In *Management of Engineering and Technology (PICMET), 2015 Portland International Conference on* (pp. 478–484). IEEE. Retrieved from http://ieeexplore.ieee.org/abstract/document/7273189/

Ratcliffe, J. H. (2016). *Intelligence-led policing*. London: Routledge. doi:10.4324/9781315717579

Scott, J. (1998). 'Performance culture': The return of reactive policing. *Policing and Society*, *8*(3), 269–288. doi:10.1080/10439463.1998.9964792

Turner, M., Kitchenham, B., Brereton, P., Charters, S., & Budgen, D. (2010). Does the technology acceptance model predict actual use? A systematic literature review. *Information and Software Technology*, *52*(5), 463–479. doi:10.1016/j.infsof.2009.11.005

ENDNOTE

1 For more information on crime statistics and trends in the England and Wales, see https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdec2016, accessed June 2017.

This research was previously published in Evidence-Based Initiatives for Organizational Change and Development edited by Robert G. Hamlin, Andrea D. Ellinger, and Jenni Jones; pages 472-482, copyright year 2019 by Business Science Reference (an imprint of IGI Global).

Chapter 9
PRISM:
Visualizing Personalized Real-Time Incident on Security Map

Takuhiro Kagawa
Kobe University, Japan

Sachio Saiki
Kobe University, Japan

Masahide Nakamura
Kobe University, Japan & RIKEN AIP, Japan

ABSTRACT

This article describes how local governments in Japan recently provide security information services for residents, which deliver regional incident information using Email or Web. However, since the conventional services usually provide "one-for-all" information. users tend to miss important incidents within the flood of information. This article proposes a new security information service, called PRISM (Personalized Real-time Information with Security Map). For given incident information and user's living area, PRISM first computes severity of the incident, based on distance, time, and type of the incident. It then visualizes the incidents with the severity on a heat map. Thus, PRISM provides real-time personalized information adapted to individual situation of users. To illustrate the feasibility, we implement PRISM as a Web application using Hyogo Bouhan Net, and Kobe city facility open data.

DOI: 10.4018/978-1-7998-2535-7.ch009

INTRODUCTION

Street crimes are a major factor that threatens safety and security of people living in the region. There are many incidents reported every day, including murder, robbery, assault, snatching, groping, exposure, suspicious act of speaking, and observation of dangerous animals. In order to achieve the safety and security of the community, individual residents are recommended to protect themselves by understanding the street crimes and incidents, spontaneously.

Based on such circumstances, researches that attempt to clarify factors associated with crimes have been conducted so far (Hipp & Kane, 2017; McCall, Land & Parker, 2011; McCall, Parker & MacDonald, 2008; Stults & Hasbrouck, 2015). In addition, local governments have implemented various policies (Tulumello, 2017). In Japan, many local governments recently start providing security information services for residents. The security information services distribute information of crimes and incidents to residents using the Internet. Residents can make use of the information for avoiding crimes. The typical security information service shows the list of recent incidents and a security map in a web site, or delivers the incident information by e-mail. For example, Hyogo Prefectural Police in Japan provides "Hyogo Bouhan Net". The service publishes incident information that Hyogo prefectural Police recognize on the Web. By registering a personal email address, a user can receive the information by e-mail. Similarly, Tokyo Metropolitan Police Department provides the e-mail delivery service, called "Mail Keishicho". The Department also publishes "Tokyo Crime Map", which is a security map showing where and when every suspicious person appeared.

In these existing security information services, every incident information is uniformly delivered to all users. Various types of incidents occur every day at various locations in the region. However, user's living area varies from one person to another. Therefore, even if an incident is critical for a user, it may not be so serious for another user who is living at distant place. Thus, how the incident is severe depends on individual users. However, this fact is not taken into account in the existing security information services. All information of incident is distributed uniformly to all users. Hence, when much information is delivered in a day, a user may miss important information. Also, it is a time-consuming task for an ordinary user to identify only relevant information from the list of a lot of incidents within the Web portal.

In this paper, we propose a new security information service, called PRISM (Personalized Real-time Information with Security Map), which personalizes the incident information based on living area of individual users. For every incident information provided by the existing security information services, PRISM computes severity of the incident according to the living area of a user. More specifically, based on the distance between the living area and the incident, the time elapsed from the occurrence, and the type of the incident, PRISM adds a weight to the incident, so that closer and newer incidents become more serious for the user. It then visualizes the weighted incidents on a heat map. Crimes have been visualized so far (Tabangin, Flores & Emperador, 2008). In PRISM, however, since the weight of severity varies depending on user's living area, personalized and real-time incident information is visualized on a heat map.

One of technical challenges in implementing PRISM is how to manage incident information in unstructured text. PRISM applies text mining to the incident information originally described in natural language. It then extracts attributes such as date, time, location, and the type of the incident, and stores the attributes in a relational database (RDB). On top of the database, we develop Web-API with which external applications can easily query and retrieve incident data. Furthermore, in PRISM, we exploit facility open data published by local government so that users can easily register own living areas. The facilities include schools, stations, and parks in the region. Even if a user cannot read a map, the user can specify the living area by using the facilities as landmarks.

To show the practical feasibility, we implement PRISM as a Web application and a mobile application. In the implementation, we use "Hyogo Bouhan Net" to obtain incident information, and "Kobe City Facility Open Data" as the facility open data. Finally, we deploy PRISM on the Internet. Using the application, users can browse personalized and real-time security information within Hyogo prefecture.

PRELIMINARIES

Security Information Service

Security information service is an information service that distributes incident information recognized by police to residents. The service aims to promote residents to understand the situation for self-protection against incidents. Typical security information services use e-mail and Web-based security maps to deliver the incident information.

The e-mail-based services send incident information in text message to the subscribers who registered e-mail addresses. The delivered information is usually archived on the web site, where users can browse the past information. In some services, users can register the ward or division of a city to specify the area range to be notified. For example, in Hyogo Bouhan Net, if a user wants information within Nada ward and registers the range, then incidents under the jurisdiction of Nada Police Station are notified.

Figure 1. Example of security map (Kobe city. From January to May, 2016)

Security map is an annotated map showing where incidents occurred. It visualizes geographical occurrences of incidents that are hard to grasp by textural information only. As an example, we show a security map describing street incidents within Kobe City from January to May, 2016. in Figure 1. In the map, a pin represents a place where an incident occurred.

Open Data

Open data is machine-readable data that anyone can freely use and share without limitation of copyright. Recently, various government and municipal bodies have published public data as open data, in order to improve quality of life of people as well as performance of business activities of enterprises (Molloy, 2011). For example, Kobe city in Japan discloses city administration data such as population, information of facilities, time table of subway. These data are represented in CSV or RDF format. Japanese government also has published a data catalog site. We can use various data in this site.

Challenges

In the existing security information services, any incident information is uniformly distributed to all users. Thus, the degree of how severe a given incident is for a user (we call it severity), which varies from one person to another, is not taken into account. As a result, users tend to miss relevant incidents within the flood of information. For this, we try to cope with the following three challenges.

Challenge C1 (Considering Living Area)

If an incident occurs nearby living area of a user, then the incident is very important for the user to be alerted. The existing services, however, do not take how close the incident is. For example, in Hyogo Bouhan Net, incident information of Nada Police Station is distributed to all subscribers of the Nada ward in the same way. However, comparing a user living 200 meters from an incident with the one living 5 kilometers away, the incident should have higher severity for the former user.

Challenge C2 (Considering Real Time)

Although each incident information has date and time of occurrence, the current services do not consider how fresh the incident is. For example, in Tokyo Crime Map, an incident that occurred yesterday and one that occurred two weeks ago are shown in the same marker on the map.

Challenge C3 (Considering Type of Incident)

There are various types of incidents reported from serious ones to just informative ones. In the existing services, however, all incident information is delivered in the same way. For example, witness information of a man with a knife and arrest information of past incident are delivered in the same e-mail format. Since the arrest information is about a resolved incident, it should have lower severity than the information of a man with a knife.

SECURITY INFORMATION SERVICE PRISM

In this paper, we propose a new security information service, called PRISM (Personalized Real-time Information with Security Map), which personalizes the incident information based on living area of individual users.

Overview

In order to cope with the three challenges described in the previous section, we exploit two ideas in PRISM. The first idea is to put a *weight of severity* on every incident, based on the living area, the current time, and the type of the incident. The second idea is to visualize the weighted incidents on a *heat map*.

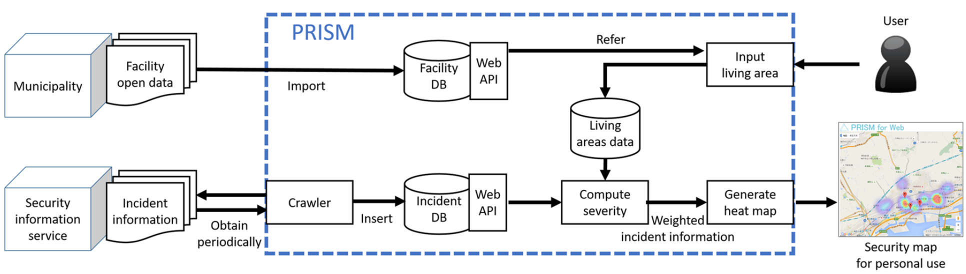
A user of PRISM first registers his/her living areas. The living areas represent places where the user often visits in the daily life, such as a house, a station, a working place, a school of children, and a shopping center. Every user can register multiple places as living areas.

Then, for each delivered incident information, PRISM calculates the *distance* between the point of incident occurrence and the living area of the user. PRISM also calculates the *elapsed time* from date and time of occurrence to the current time. Based on the distance and the elapsed time, PRISM adjusts a weight of the *default severity* pre-determined for each type of incident. The resultant weight is the severity of the incident personalized for the user. Finally, PRISM generates a heat map based on the personalized severity, which achieves a personalized and real-time security map.

Architecture

Figure2 shows the system architecture of PRISM. In the figure, the dotted rectangle represents the system boundary of PRISM. A crawler, at the bottom left of the figure, periodically obtains incident information from an existing security information service. Then, the crawler analyzes the retrieved text, extracts attributes, and inserts the attributes into an incident DB. A user at the top right of the figure registers his/her living areas data. In the registration, the user can refer to a facility DB, where facility open data of the local government is imported. The user can use various facilities in the region as landmarks of the living area. Based on the incident DB and

Figure 2. Architecture of PRISM



the living areas data, PRISM computes the severity of every incident. Finally, PRISM generates a heat map based on the weighted incident information, and presents the map to the user. We will explain the details in the following subsections.

Obtaining Incident Information

PRISM periodically obtains incident information from an existing security information service using the crawler. In general, the incident information is written in natural language. So it is difficult to make queries or take statistics for the original text. Therefore, PRISM analyzes the original text in the crawler, structures the text into attributes, and inserts the attributes into the RDB (i.e., the incident DB).

We explain the flow of the text analysis. First, the crawler applies pre-processing to the original text, where orthographic variants in characters and sentences are corrected. Then, applying a text mining to the pre-processed text, the crawler extracts the following nine attributes.

- **PrefCode:** A code representing the prefecture where the incident occurred
- **ID:** An identifier of an incident
- **Datetime:** Date and time of occurrence of the incident
- **Title:** A title of the incident information
- **Content:** A content of the incident information
- **Severity:** A default severity of the incident
- **Address:** An address of the place where the incident occurred
- **Lat:** Latitude of the place where the incident occurred
- **Lng:** Longitude of the place where the incident occurred

Although the original incident information is given in the natural language text, it basically follows a strict writing convention. Therefore, by applying pattern matching using regular expressions, we can extract datetime, title, content, and address.

The values of lat and lng can be obtained from address using geographic information web services such as Geolocation API. The value of id can be extracted from the article number or URL of the security information service. The value of prefCode can be obtained from security information service. For example, we know that the information from Hyogo Bouhan Net is the incident in Hyogo Prefecture. By using prefCode and id as a composite primary key, information in different prefectures can be handled at the same time even if the incidents have the same id.

The value of severity represents a default severity that the incident has. It is defined by the following four categories, determined by keywords contained in the title and content.

- Alert (severity 3) the most serious incident that can threaten life of citizens. The keywords include murder, robbery, shooting, assault, gun, knife, etc.
- Warning (severity 2) incidents that may cause physical damage to citizens. The keywords include snatching, pick- pocket, theft, stalking, groping, etc.
- Caution (severity 1) incidents to be paid attention, not directly linked to life or physical damage. The keywords include scam, animal, wild boar, etc.
- Notice (severity -1) other information from the police. The keywords include arrest, resolution, notice, etc.

Note that the above default severity represents a default value of each incident, where the situation of individual users is not yet counted. It will be adjusted in the subsequent process based on the living areas of individual users.

Incident DB

The incident DB is a relational database that stores and manages incident information with the nine attributes described in the previous subsection. The data schema is as follows:

[prefCode, id, datetime, title, content, severity, address, lat, lng]

Figure3 shows an example that inserts an incident information text into the incident DB. In this example, PRISM analyzes an incident “Grouping occurred”, extracts the nine attributes, and inserts them as a record.

Figure 3. Example of inserting incident information to incident DB

http://hyogo-bouhan.net/criminalCase/detail.do?...&topicId=21939

Groping occurred

On May 12 (Fri) around 10:05, groping occurred on the street in the vicinity of 6-1, Shinkaichi, Hyogo-ku Kobe-shi, Hyogo. The suspect is a man who was wearing white cap and dark clothes.

Insert

prefCode	Id	datetime	title	content	severity	address	lat	lng
28	21939	2017-05-12 10:05:00	Groping occurred	On May 12 (Fri) around 10:05, groping …	2	6-1, Shinkaichi, Hyogo-ku Kobe-shi, Hyogo	34.676265	135.175308

On top of the incident DB, we develop Web-API, so that external applications can easily retrieve incident data. The Web-API has the following three commands:

- **Latest:** For a given incident ID, the command returns the latest incidents that occurred after the incident specified by the ID.
- **Search:** For a given query of ID, keyword, date, time range, and severity, the command returns incidents that matched the query.
- **Range:** For given coordinates and distance, the command returns incidents that occurred within the range defined by the coordinates as a center and the distance a radius.

We have implemented Web-API as CGI handling JSON. The command and parameters are given in a form of URL, and the result is returned in a JSON format.

Registering Living Area with Open Data

PRISM manages user's living area as a set of coordinates. Accordingly, the user needs to register each living area with coordinates (latitude, longitude). With the help of API of map information service (e.g., Google maps), PRISM allows the user to input the coordinates just by double-clicking a point of a map in a Web browser.

On the other hand, a user, who are not good at reading the map, may not be able to point the exact coordinates on the map. To cope with such cases, we utilize *facility open data* published by local governments. Using nearby facilities as landmarks, the user can easily input places of living areas. The facility open data contains location information of various facilities in the region, including government offices, fire stations, police stations, stations, nursery schools, kindergartens, schools, parks, and cultural facilities. The facility open data is generally structured in the form of CSV or RDF.

In PRISM, we import the facility open data into *facility DB*, which is referred when registering the living area. The data schema of the facility DB is as follows:

- **ID:** An identifier of a facility
- **Name:** A name of the facility
- **PostalCode:** Postal code of the facility
- **Address:** An address of the facility
- **Phone:** A phone number of the facility
- **Lat:** Latitude of a place where the facility is located
- **Lng:** Longitude of a place where the facility is located
- **Ward:** A ward where the facility is located
- **Type:** A type of the facility (e.g. elementary school)

Similar to the incident DB, we develop Web-API for the facility DB as CGI handling JSON. External applications can search the facilities with the attributes and distance.

Computing Personalized Severity

Next, PRISM computes the severity of incidents according to individual circumstances, based on the living areas data. More specifically, PRISM adjusts the default severity of each incident according to the following two viewpoints.

- **Distance:** The closer the distance between the place of incident and user's living area is, the more serious the incident is for the user, since a new incident may happen again nearby. Thus, higher weight is given to the incident. On the other hand, the longer the distance is, the smaller the severity is. When the distance exceeds a threshold Th_d, the severity is set to zero.
- **Time:** The shorter the elapsed time from the incident occurrence, the more serious is for the user, since a new incident may happen again soon. Thus, higher weight is given to the incident. On the other hand, the longer the time is, the smaller the severity is. When the time exceeds the threshold Th_t, the severity is set to zero.

Now, for an incident *x* and a user *u*, let *d* be the distance from living area of *u* to the place where *x* occurred. Also, let *t* be the elapsed time from the time when *x* occurred. Then, we define the severity of *x* for *u*, denoted by *severity(x, u)*, as follows:

$$severity(x, u) = 1/3*(WD(d)+WT(t)+severity(x)*1/3)$$

where *WD(d)* and *WT(t)* are weight functions with respect to distance *d* and time *t*, respectively. *severity(x)* represents the default severity of *x* (ranging over -1, 1, 2 or 3) as defined based on type of incident. As for the definition of functions *WD(d)* and *WT(t)*, there are various methods. In the current version of PRISM, we use the following functions.

$$WD(d) = \begin{cases} 1.0 & (0 \le d < 0.5Th_d) \\ -2(d - Th_d) / Th_d & (0.5Th_d \le d < Th_d) \\ 0.0 & (Th_d \le d) \end{cases}$$

$$WT(t) = \begin{cases} 1.0 & (0 \leq t < 0.5Th_t) \\ -2(t - Th_t) / Th_t & (0.5Th_t \leq t < Th_t) \\ 0.0 & (Th_t \leq t) \end{cases}$$

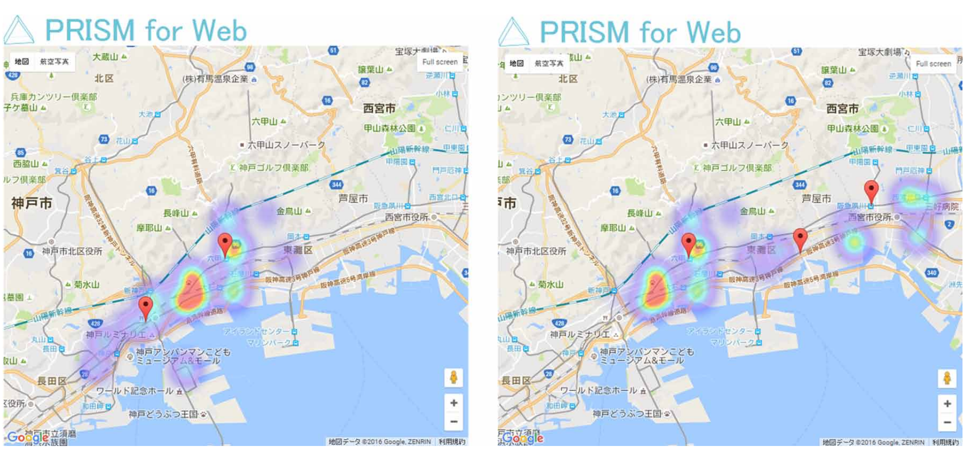
The above functions maintain the weight 1.0 until the given distance (or time) reaches the half of the threshold, and decrease the weight linearly from 1.0 to 0.0 up to the threshold. Currently, Th_d is set to 4.0km, Th_t is set to 14 days. However, they are freely customized according to characteristics of the area as well as the crime situation of the region.

Heat Map

Finally, PRISM visualizes the incident data with personalized severity on heat map. The value of *severity(x, u)*, which is the severity of incident *x* for user *u*, is between 0.0 and 1.0. PRISM creates a heat map such that the severity value is scaled into the seven colors, [purple, indigo, blue, green, yellow, orange, red]. For each incident *x*, PRISM puts a data point on coordinates (lat, lng) of *x* using a color associated with *severity(x, u)*. This generates a heat map adapted to individual living area and the current time.

Figure4 shows two heat maps generated for two users A and B, where the incident information within Kobe City at a certain date is visualized. The pins in the map indicate locations of living areas registered by the users. The colored points indicate the places where incidents occurred. In this example, user A registered Kobe Sannomiya Station and Hankyu Rokko Station as living areas. On the other hand,

Figure 4. Example of outputting heat map (a) User A's heat map (b) User B's heat map



user B registered Hankyu Rokko Station, Shukugawa Station, and Hanshin Fukae Station. We can see that completely different heat maps are generated depending on the living area, even though the map area and the time are the same.

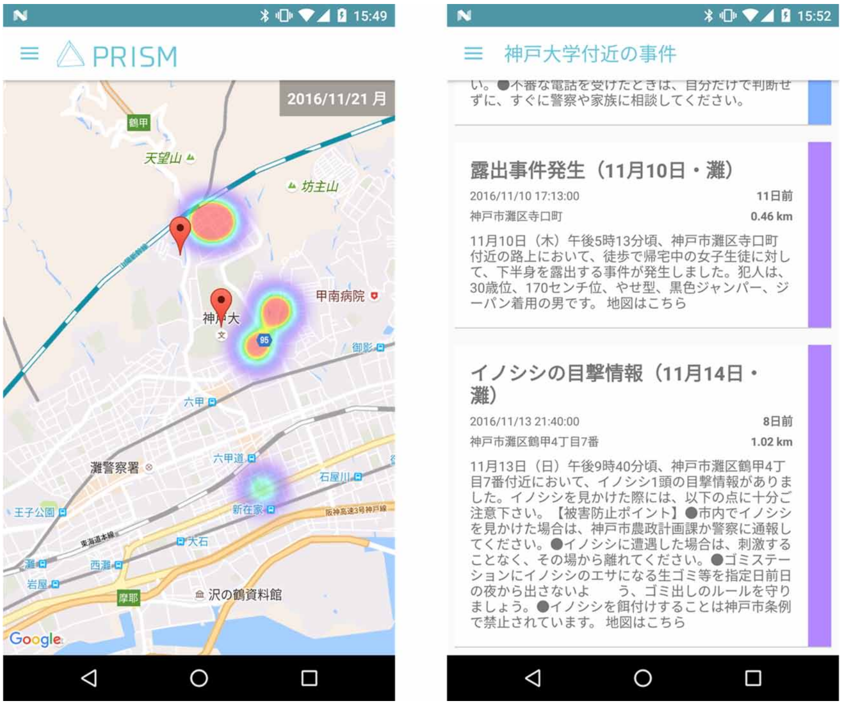
Implementation

We have implemented the proposed PRISM as a web application and a mobile application. Figure5 and Figure6 show screenshots of PRISM for Web and PRISM Android, respectively. In the proposed architecture (see Figure2), the crawler, the incident DB, the facility DB and their Web-API were implemented in the server side. Whereas, the registration of living area and the generation of the heat map were implemented in the client side. Technologies used for the implementation are as follows.

- Security information service: Hyogo Bouhan Net
- Facility open data: facility open data of Kobe City
- Crawler: perl, cron, Yahoo!GeoCoder API
- Incident DB, facility DB: MySQL

Figure 5. PRISM for Web

Figure 6. PRISM Android



- Web-API: perl, CGI.pm, JSON.pm
- Client (Web application): Chrome browser, JavaScript, Google Maps, Google Heatmap Layer
- Client (mobile): Android, Google Maps, Android Heatmap Utility

DISCUSSION

Sufficiency of Requirement

We here discuss how PRISM cope with Challenges C1, C2, and C3. PRISM calculates the severity of incidents based on the living area and the elapsed time of the incident, and visualizes incidents on a heat map. Thus, a security map adapted to every user is generated. A closer and newer incident is shown to be more serious in the map. Thus, C1 and C2 are resolved. Moreover, four types of default severity based on keywords in title of incident information in PRISM, which corresponds to C3. However, it is necessary to verify the validity of the value, which is left for our future work.

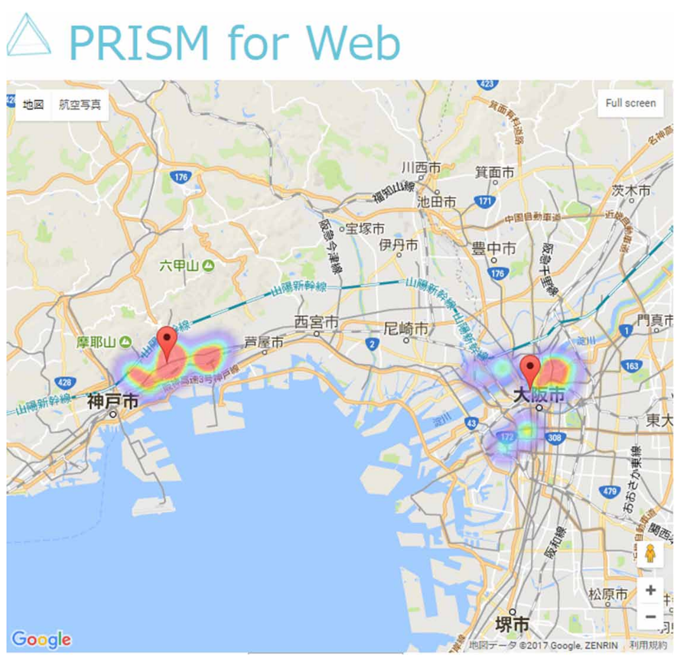
Limitations in Using Open Data

As we mentioned, PRISM is not limited to Hyogo Prefecture since incident information has prefCode. As an example of combining multiple information sources, we display the security map utilizing both Hyogo Bouhan Net and information provided by Osaka Prefectural Police. Figure7 shows the heat map at that time. The right pin of the figure indicates Osaka station and the left pin indicates Hankyu Rokko station in Hyogo Prefecture. As shown in Figure7, PRISM can visualize incident information combining multiple sources. Like this, when we obtain incident information every region of the country, PRISM can be extended nationwide.

On the other hand, regarding the incident information provided by existing security information services, the parser must convert unstructured text data gathered by the crawler into structured data by text analysis. For this, if we switch to another security information service, we have to re-create the document parser. Such tight coupling of the crawler and the security information service limits the extensibility of the system. However, this problem will be alleviated if the incident data is published as structured open data.

We used facility open data of Kobe City in this study. However, the data did not contain the sufficient number of familiar facilities (e.g., railway stations). More facilities are necessary to cover more users living in various places.

Figure 7. Heat map focused on Osaka station and Rokko station



Related Work

"Tokyo Safety Map" is a Web application quite similar to PRISM. The application analyzes incident information of "Mail Keishicho", and display the incident on Google map. However, it does not consider living area or personalization.

CONCLUSION

In this paper, we have proposed a personalized and real-time security information service, called PRISM. Using the incident information provided by the existing security information services, PRISM adapts the incident to individuals based on living area of the user. We introduced a metric, called severity, which quantifies how the incident is serious for the user. The severity is computed based on the distance from the living area and the elapsed time. Incidents weighted with the severity are visualized on a heat map. We also implemented proposed PRISM as a web application and a mobile application.

In our future work, we will verify the validity of the value of the severity, as well as the weight functions. We also plan to have many users actually use PRISM, and evaluate the usability.

ACKNOWLEDGMENT

This research was partially supported by the Japan Ministry of Education, Science, Sports, and Culture [Grant-in-Aid for Scientific Research (B) (16H02908, 15H02701), Grant-in-Aid for Scientific Research (A) (17H00731), Challenging Exploratory Research (15K12020)], and Tateishi Science and Technology Foundation (C) (No.2177004).

REFERENCES

Hipp, J. R., & Kane, K. (2017). Cities and the larger context: What explains changing levels of crime? *Journal of Criminal Justice*, *49*, 32–44. doi:10.1016/j.jcrimjus.2017.02.001

Hyogo Prefectural Police. (n.d.). Hyogo Bouhan Net. Retrieved August 18, 2017, from https://hyogo-bouhan.net/

Japanese government. (n.d.). DATA.GO.JP. Retrieved August 18, 2017 from http://www.data.go.jp/?lang=english

Kobe city. (n.d.). Open Data Kobe. Retrieved August 18, 2017, from https://data.city.kobe.lg.jp

McCall, P. L., Land, K. C., & Parker, K. F. (2011). Heterogeneity in the rise and decline of city-level homicide rates, 1976–2005: A latent trajectory analysis. *Social Science Research*, *40*(1), 363–378. doi:10.1016/j.ssresearch.2010.09.007

McCall, P. L., Parker, K. F., & MacDonald, J. M. (2008). The dynamic relationship between homicide rates and social, economic, and political factors from 1970 to 2000. *Social Science Research*, *37*(3), 721–735. doi:10.1016/j.ssresearch.2007.09.007 PMID:19086112

Molloy, J. C. (2011). The Open Knowledge Foundation: Open Data Means Better Science. *PLoS Biology*, *9*(12), 1–4. doi:10.1371/journal.pbio.1001195 PMID:22162946

Stults, B. J., & Hasbrouck, M. (2015). The Effect of Commuting on City-Level Crime Rates. *Journal of Quantitative Criminology*, *31*(2), 331–350. doi:10.100710940-015-9251-z

Tabangin, D. R., Flores, J. C., & Emperador, N. F. (2008). Investigating Crime Hotspot Places and their Implication to Urban Environmental Design: A Geographic Visualization and Data Mining Approach. *International Journal of Computer, Electrical, Automation, Control and Information Engineering, 2*(12).

Tokyo Metropolitan Police Department. (n.d.). Tokyo Crime Map. Retrieved August 18, 2017 from http://www2.wagmap.jp/jouhomap/Portal?langmode=1

Tokyo Safety Map. (n.d.). Retrieved August 18, 2017, from http://anzn.net/tokyo/safety/index.html

Tulumello, S. (2017). The Multiscalar Nature of Urban Security and Public Safety. *Urban Affairs Review* Yahoo! Geocoder API (n.d.). Retrieved August 18, 2017 from https://developer.yahoo.co.jp/webapi/map/openlocalplatform/v1/geocoder.html

This research was previously published in the International Journal of Software Innovation (IJSI), 6(4); edited by Lawrence Chung and Roger Y. Lee; pages 46-58, copyright year 2018 by IGI Publishing (an imprint of IGI Global).

Chapter 10
Crime Hotspot Detection:
A Computational Perspective

Emre Eftelioglu
University of Minnesota, USA

Shashi Shekhar
University of Minnesota, USA

Xun Tang
University of Minnesota, USA

ABSTRACT

Given a set of crime locations, a statistically significant crime hotspot is an area where the concentration of crimes inside is significantly higher than outside. The motivation of crime hotspot detection is twofold: detecting crime hotspots to focus the deployment of police enforcement and predicting the potential residence of a serial criminal. Crime hotspot detection is computationally challenging due to the difficulty of enumerating all potential hotspot areas, selecting an interest measure to compare these with the overall crime intensity, and testing for statistical significance to reduce chance patterns. This chapter focuses on statistical significant crime hotspots. First, the foundations of spatial scan statistics and its applications (i.e. SaTScan) to circular hotspot detection are reviewed. Next, ring-shaped hotspot detection is introduced. Third, linear hotspot detection is described since most crimes occur along a road network. The chapter concludes with future research directions in crime hotspot detection.

DOI: 10.4018/978-1-7998-2535-7.ch010

INTRODUCTION

Analyzing crime locations and using the spatial information associated with them is a fundamental task of environmental criminology since the main goal of a crime investigation is to locate the criminal and/or prevent more crimes from occurring. Two important spatial theories in environmental criminology are routine activity theory and crime pattern theory. *Routine activity theory* states that a crime location is related to a serial criminal's frequently visited areas (Burn, 1982). *Crime pattern theory* extends routine activity theory on a spatial model (Brantingham & Brantingham, 1993). When crime analysts study the locations of crime sites and make inferences that help track down a serial criminal or that identify areas where extra police presence is needed, they are using these theories. Thus, the motivation of crime hotspot detection can be summarized as:

1. To detect current/emerging crime hotspots to focus the deployment of police forces, and
2. To predict the location of a serial criminal's residence.

Previously, most analysis of crime locations was done manually. However, the task of enumerating potential hotspots by hand and detecting meaningful patterns in the data is arduous, even for experienced analysts. Rising crime numbers in larger cities increase analysts' workload and compound their stress. For example, a typical crime dataset of the continental United States includes around 10^7 crimes annually (FBI, 2015). Therefore, law enforcement agencies need computational tools that can automate hotspot detection. Moreover, these tools should eliminate the chance patterns (false positives). Most police departments and similar entities have limited resources for crime mitigation and prevention. Therefore, false positive results, that is, hotspots that occur only by chance, risk causing real harm. If a police department diverts money and manpower to a chance hotspot location that don't need it, may leave other areas less protected. *Chance hotspots* can have other harmful consequences as well. When police increase their presence in a location identified as a crime hotspot, people naturally begin to avoid the area out of fear for their safety, and the neighborhood may become stigmatized.

Hence there is a growing need for crime hotspot analysis tools which can handle large crime datasets as well as eliminate chance patterns. Such tools may help crime analysts accomplish their law enforcement goals with optimal resource allocation (Eck & others, 2005).

Many computational techniques (Spencer Chainey & Ratcliffe, 2013; Eck & others, 2005; Levine, 2006) are used for hotspot detection. One of the most common methods is to enumerate hotspots with clustering techniques. These techniques are highly scalable and widely used in many societal applications (Ester & others, 1996; Ilango & Mohan, 2010; Liao, Liu, & Choudhary, 2004; Sarmah, Das, & Bhattacharyya, 2007; Wu et al., 2008). Nevertheless, clustering has two important limitations for hotspot detection. First, these techniques require the user to input the number of clusters beforehand. This does not conform well to hotspot detection, whose aim is to search for an abnormality that may or may not exist in the data. In other words, the user does not know beforehand whether a hotspot exists, or if so, how many. A second limitation is that most clustering techniques lack a statistical significance test to eliminate chance occurrences of hotspots.

This chapter focuses on statistically significant hotspot detection techniques that aim to remove chance patterns. The shape of the desired hotspot, determines the enumeration technique used to generate candidate hotspots and spatial scan statistics is used to assess the statistical significance of each candidate.

Three representative techniques for discovering significant crime hotspots are presented and each technique is illustrated using sample case studies on real crime datasets collected from different states in the U.S. However, it is important to note that there are many statistically significant hotspot detection techniques with different outputs that are designed to be used in different application domains, such as epidemiology, animal foraging, medical imaging etc. (Agarwal, McGregor, Phillips, Venkatasubramanian, & Zhu, 2006; Coleman et al., 2009; Janeja & Atluri, 2005a; Kulldorff, Huang, Pickle, & Duczmal, 2006; McCullagh, 2006; Neill & Moore, 2004; Neill, 2009; Patil & Taillie, 2004; Prates, Assunção, & Costa, 2012; Shi & Janeja, 2011; Walther, 2010; Zhang, 2010).

Formally, a crime hotspot can be defined as an area where the concentration of crimes inside is significantly higher than the number of activities in any other place in the study area. The hotspot can be circular (partial/full), rectangular, ring-shaped or linear depending on the goal of the hotspot analysis, the geographic features associated with the study area and the crime type. Circular hotspots occur when the crimes are spread around an anchor point of a criminal. For example, narcotics crimes tend to occur in a circular pattern causing a circular hotspot around the criminal narcotics manufacturer (Belenko & Spohn, 2015). Similarly, linear hotspots can be seen for some crimes that are committed along a road network. For example, street robbery cases can be seen on the road network and crime activities tend to be on specific road segments where a criminal selects as his base crime location. Finally, ring-shaped hotspots can be seen for serial criminals, who try not to commit crimes too close to home and try to spend least effort to travel causing a ring-shaped crime pattern around their residence.

SCOPE

This chapter provides and overview of statistically significant crime hotspot detection and outlines its capabilities for aiding in law enforcement with the primary intent of reducing chance patterns in crime hotspot detection. Hence this chapter does not focus on presenting computational performance evaluation. Also there are a number of clustering techniques that are used for crime hotspot detection, but this chapter just focuses on statistically significant crime hotspot detection using spatial scan statistics.

BACKGROUND

This section reviews basic concepts related to statistically significant hotspot detection and formally define the crime hotspot detection problem.

Basic Concepts

- **Activity Set:** An activity set A is a collection of geo-located points (i.e. crime locations). Each activity $a \in A$ is associated with a pair of coordinates (*Lat, Lon*) representing its location in two-dimensional Euclidean space.
- **Study Area:** Study area S is territorial area of responsibility of a public safety agency. S is assumed to be the minimum orthogonal bounding rectangle of the activity set A in this chapter.
- **Spatial Bi-Partitioning:** Spatial bi-partitioning is the division of an area into two non-overlapping subsets. The key point of spatial bi-partitioning is the notion of “inside” and “outside”. Any activity point $a \in A$ is either inside or outside but not both.
- **Spatial Comparison:** Spatial comparison is the comparing of two populations after spatial bi-partitioning, i.e., the population “inside” and the population “outside” which have been partitioned in the spatial bi-partitioning phase. This comparison can be done by different metrics such as difference or ratio; by different interest metrics such as disease rate, areal density or linear density; or by different significance tests such as parametric (Poisson) test or non-parametric test.

Spatial Scan Statistics

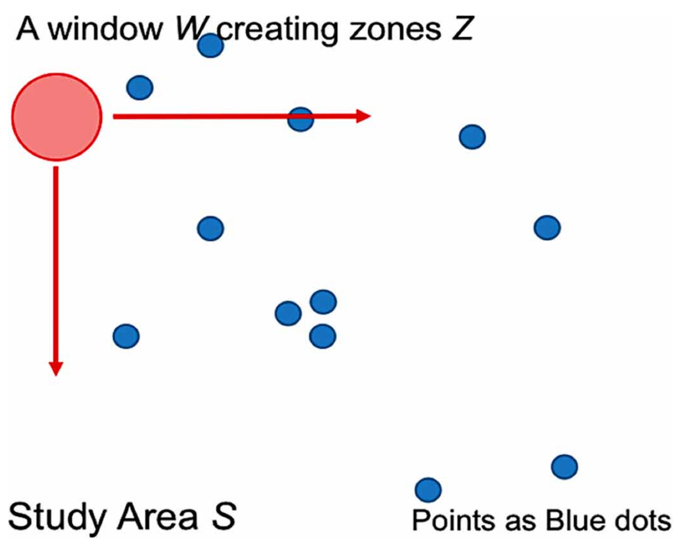
Spatial scan statistics is a widely used tool to detect hotspots in a point process and it’s widely used in epidemiology to determine disease outbreaks (Neill & Moore, 2004). It was first studied for one-dimensional data and then extended to multi-dimensional data (M. Kulldorff, 1999; Kulldorff, 1997). Spatial scan statistics has proved to be the most powerful statistical test to detect hotspots in an activity set (M. Kulldorff, 1999).

Suppose there is a point process *N* in a study area *S*. The aim is to find a hotspot in this point process. First, candidate hotspot regions are enumerated using a window *W*, which moves around the study area and creates candidate hotspot regions referred to as zones *Z*. For each of these zones, the number of observed and expected observations is noted. For example, Figure 1 shows a circular window moving in the study area S and creating zones. Note that each created zone will be a candidate hotspot to be evaluated for being an actual hotspot.

The fundamental question asked for each of the zone Z is "Is there any difference between inside the zone and outside?" In order to answer this question, a Hypothesis Test is constructed with two outcomes. The null hypothesis (H_0) states that the activity points are distributed randomly according to a homogeneous Poisson process over the study area *S*. The alternative hypothesis (H_1) states that the inside of a zone *Z* has higher activities than outside (Martin Kulldorff, 2014).

The hypothesis test has two important requirements. The first is a metric to give a score for each zone *Z*. If the window had a fixed size and thus all zones *Z* had the same size, then the test statistic would be the count of the points inside the zone. Since the actual size of the hotspot in a crime scenario is not known beforehand,

Figure 1. A circular window enumerating zones in a study area



the window should have a variable size and thus created zones Z will not have the same size. Therefore, a *log likelihood ratio test* is the metric used to determine the test statistic. The second requirement of hypothesis testing is a distribution of the test statistic under the null hypothesis of no clusters. This distribution will show what one should expect when there is no hotspot in the dataset. This distribution is acquired using a *randomization test*. Finally, the test statistic score of each zone is compared with the distribution of the test statistic to determine the statistical significance (*p-value*). Given a required significance level (α_p), if a zone Z has a *p-value* lower than α_p, it can be concluded that the zone Z is a significant hotspot (Kulldorff, 1997b). These concepts are described in more detail next.

Likelihood Ratio Test

The likelihood ratio test determines the test statistic of a candidate zone Z. It is computed by dividing the likelihood of the activities in zone Z under the alternative hypothesis (H_1) by the likelihood of the zone Z under the null hypothesis (H_0). This comparison gives the following equation:

$$LR_Z = \frac{L\left(Z\right)_{H_1}}{L\left(Z\right)_{H_0}}$$

In order to find the maximum likelihood of a zone Z, the parameters in $LR(Z)$ are selected to maximize the likelihood ratio. These terms are used as the supremum (least upper bound) when likelihood ratios are computed. Thus, the Likelihood Ratio is derived as follow. Note that *Log* values are used to make the interpretation easier.

$$Log\ LR_Z = Log\left(\left(\frac{c}{B}\right)^c \left(\frac{\left|A\right| - c}{\left|A\right| - B}\right)^{\left|A\right| - c} I()\right),$$

where $B = \frac{\left|A\right| area\left(Z\right)}{area\left(S\right)}$ and $I() = \begin{cases} 1, & if\ c > B \\ 0, & otherwise \end{cases}$.

Here, B is the expression of the expectation of number of activities in a particular zone Z. The observed number of activities is denoted as c. Total number of activities is the cardinality $|A|$ of set A. The final term $I()$ denotes the indicator function. $I()=1$ when a zone Z has more activity points than expected ($c > B$) and otherwise it is set to 0 to prevent the detection of low activity areas (Martin Kulldorff, 2014).

Randomization Test

Once the enumeration of the candidate hotspots (zone Z) is done and the test statistic of each candidate is computed, a randomization test is done to determine the distribution of the test statistic under the null hypothesis (H_0). This distribution later helps to determine the statistical significance of a candidate hotspot and will help determine whether the candidate hotspot occurred by chance or is truly anomalous. Although other methods exist, in this chapter the randomization test with Monte Carlo simulations will be explained.

For Monte Carlo simulation, m random activity sets $A_{1...m}^{random}$ are created in the same study area S. The locations of the activities are determined using complete spatial randomness (CSR). In other words, points inside each activity set are randomly thrown into the study area. For each of these random activity sets $A_{1...m}^{random}$, new zones Z are generated and their test statistics (log likelihood ratio) are computed using almost the same method as for the original activity set A. The only difference is that only the maximum log likelihood ratio is stored. Thus, at the end of this process a list of m test statistic values are obtained from m random activity sets $\left(A_{1...m}^{random}\right)$. These values are used to determine the statistical distribution of the log likelihood ratios.

Hypothesis Test

The null hypothesis states that activity points are distributed randomly according to a homogeneous Poisson process over the study area S (Kulldorff, 1997a). In order to accept or reject the null hypothesis (accept H_1), we need to determine the significance level (*p-value*) of the candidate hotspots. We do this by comparing a candidate's test statistic with the distribution of test statistics obtained from the randomization test, and then dividing its position by the number of Monte Carlo simulation trials m. If the computed p-value is higher than the desired significance level (α_p), the H_1 hypothesis is rejected; otherwise, it is said that H_1 can't be rejected, indicating the detected hotspot is significant.

With this background, we are ready to consider three representative approaches to statistically significant hotspot detection. Case studies on real crime data are included to illustrate each approach. We also briefly explain each method's limitations.

CIRCULAR HOTSPOT DETECTION

Criminal activity in an area tends to spread in a circular process similar to that described by the diffusion model in physics and chemistry. Diffusion means that molecules or heat will move away from their sources once they are discharged. The diffusion model provides a natural way to describe the circular spreading of cases (i.e. crimes). This gives rise to the notion of circular footprints of hotspots in isotropic geographies. Therefore, the ability to detect a circular hotspot is an important task in environmental criminology.

In formal terms, circular hotspot detection can be defined as follows: Given a set of geo-located points (e.g. crime reports) and a significance threshold, circular hotspot detection finds circular shaped areas where the concentration of points inside a circle is significantly higher than the number of points outside. Circular hotspot detection requires the following inputs specified by an analyst:

1. A spatial crime dataset with a collection of crimes, each associated with geo-location information (i.e., latitude, longitude),
2. A statistical significance threshold (α_p).

Based on the above inputs, the goal of circular hotspot detection is to report a collection of circular hotspot areas with p-values lower than the specified statistical significance threshold (α_p).

Case Study on a Real Crime Data

A typical input to circular hotspot detection is a spatial crime dataset that contains crime reports each associated with geo-location. For example, Figure 2 shows a crime dataset from Chicago, Illinois (City of Chicago, 2013). The dataset includes 384 homicides (by first degree murder) crimes committed in Chicago, Illinois between March 2013-March 2014. Each crime location is shown as blue dots and the map is created using QGIS Software (Quantum GIS Development Team, 2012), and the Open Street Plugin (Haklay & Weber, 2008). Study area is selected as the minimum orthogonal bounding rectangle of the crime dataset. Note that the study area could be the territorial area of responsibility for a public safety agency. The aim is to find circular hotspots with a statistical significance level of $\alpha_p = 0.001$. Figure 3 shows the output of SaTScan with two hotspot areas having log likelihood ratio of 107.10 and 48.26 respectively. These hotspots have p-value = 0.001 which indicates statistical significance at the 99.9% confidence level.

Figure 2. First degree murder cases in Chicago between March 2013 and March 2014; dataset includes 384 Homicide cases shown in blue dots

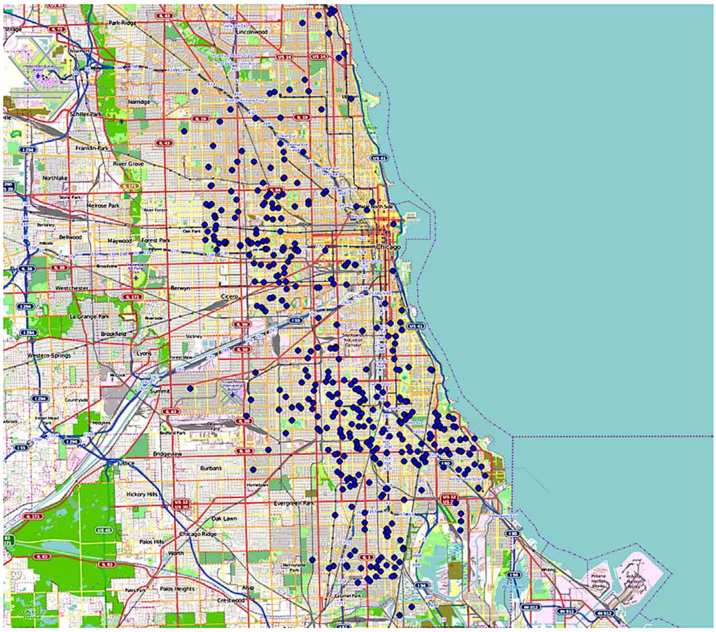
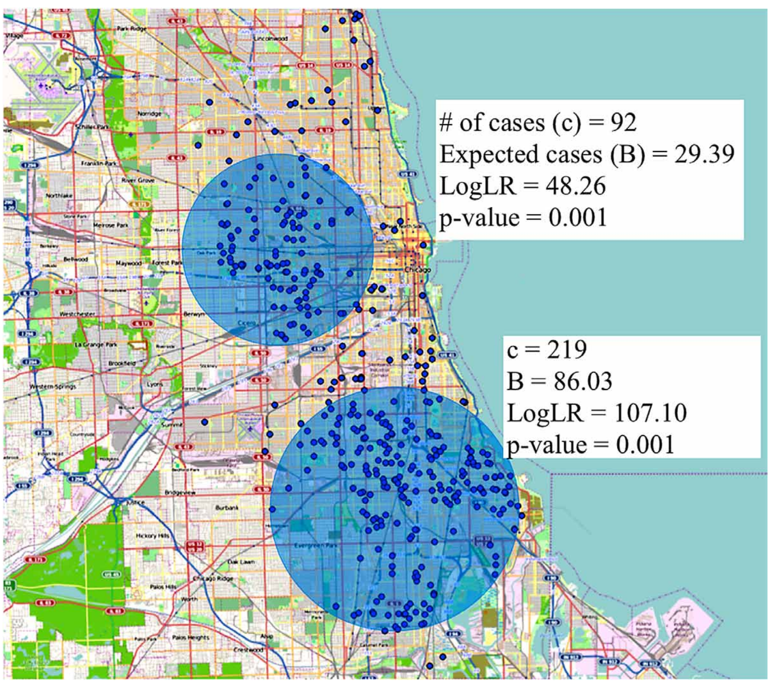


Figure 3. Output of SaTScan with two circular hotspots shown in blue



SaTScan Circular Hotspot Detection Algorithm

SaTScan is a state-of-the-art software package that uses spatial scan statistics to detect circular hotspots. It is used extensively in epidemiology to detect circular disease hotspots.

In its simplest form SaTScan uses a three-step approach to detect statistically significant circular hotspots:

1. Enumeration of Circles,
2. Log likelihood ratio test, and
3. Monte Carlo simulation and Hypothesis test.

Although indexing and optimization techniques exist for the circle enumeration and Gumbel Approximation (Martin Kulldorff, 2014) and Early Monte Carlo termination for the Monte Carlo simulation step can be used to improve the scalability of the SaTScan algorithm, this chapter describes these three steps without any algorithmic refinements.

Step 1: Enumeration of circles.

When enumerating candidate circular hotspots, SaTScan uses activity points in the activity set ($a \in A$) as the centers. In other words, SaTScan searches only the circles centered on each of the activity points in the dataset. Whenever a point is selected as a circle center, distances from the rest of the points to this center are used as radii to enumerate the circles. For example, given an activity set with $|A| =$ 100 activity points, $|A|(|A|-1) = 10099 = 9900$ circles are enumerated.

Step 2: Log likelihood ratio test.

The computation of $Log\ LR_Z$ requires the area and the number of points inside a zone Z. Suppose the zones are enumerated as circles in Step 1. Using the area of each circle and number of activity points inside, Log Likelihood Ratio of circles are computed. Note that among the overlapping circles, SaTScan returns only the circle with the highest Log Likelihood Ratio since most clusters of this type provide little additional information, but their existence means that while it is possible to pinpoint the general location of a cluster, its exact boundaries must remain uncertain (Kulldorff, 2010).

For example, the crime dataset set in Figure 2 includes 384 crime locations and the study area S is a 0.09 square degrees. The area of the circular hotspot in the north is $\pi r^2 = 3.140.047^2 = 0.0069$ and thus B = 29.39 and likelihood ratio is 48.268

Step 3: Monte Carlo Simulation and Hypothesis Test.

For the circles created in Step 1, a p-value is computed by doing a Monte Carlo simulation. First, *m* random datasets with Poisson distribution are generated. For each random dataset, new circles are enumerated and the maximum log likelihood ratio of each random dataset is stored in decreasing order. Then, log likelihood ratio of each circle enumerated in Step is compared with this list and its corresponding position is determined. This position is divided into the number of Monte Carlo simulations *m* to determine the p-value of a circle. Finally, all non-overlapping circles with p-value lower than the specified significance threshold α_p, are returned by the algorithm.

Limitations

As demonstrated, SaTScan relies on points as the centers. However, in cases where the center is sparse, SaTScan may not recognize a hotspot. Therefore, in cases when the contiguities of circular hotspots are disturbed by geographic features (i.e. rivers, roads, jurisdiction boundaries), these hotspots may not be detected by SaTScan. In addition, elliptical or imperfect circular (i.e. quarter/half circle) hotspots caused by geographic features may also be missed by this approach.

Another issue arises when two points occur too close to each other. SaTScan may detect them as significant hotspots since the log likelihood ratio function depends on the number of activity points and the area of the hotspot.

Finally, a hotspot detected by SaTScan has strict boundaries. However, most crimes tend to show a diffusion process where moving further from the center results in fewer observations of activities. Therefore, strict boundaries may not fully represent a crime hotspot. For these reasons, SaTScan should not be thought of as the sole tool to determine crime hotspots.

RING-SHAPED HOTSPOT DETECTION

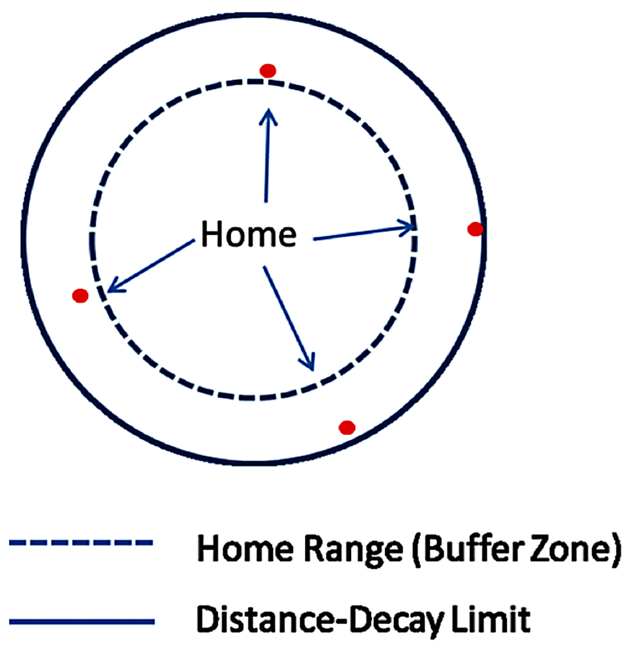
In this section, ring shaped hotspot detection with a statistical significance will be defined and it will be illustrated with an example based on a crime dataset from San Diego, California. Formally, given a set of geo-located points (e.g. crime reports) and a significance threshold, ring-shaped hotspot detection aims to find ring-shaped hotspot areas where the concentration of points inside is significantly higher than the number of points outside. Ring-shaped hotspot detection requires the following inputs specified by an analyst:

1. A spatial crime dataset with a collection of crimes each associated with geo-location information (i.e. Latitude, Longitude).
2. A statistical significance threshold (α_p).

Based on the above inputs, the goal of ring-shaped hotspot detection is to report a collection of ring shaped hotspot areas with p-value lower than the specified statistical significance threshold (α_p).

In geographic profiling, two concepts are widely used to predict a potential location for a criminal. These concepts are distance decay and buffer zone as shown in the Figure 4. Distance decay is the result of a basic behavior caused by the requirements of time, effort and money to travel. Distance decay explains why most crimes occur relatively close to the offender's home (Brantingham & Brantingham, 1993). For example, 70% of arson crimes occur within two miles of a serial arsonist's home (Estepp, 1987). Second concept is the buffer zone, which is the basic result of the anonymity principle. In other words, buffer zone is an area where crimes are less likely, because of the increased risk of recognition by the neighbors. Geographic profiling uses the opposing effects of distance decay and buffer zone to predict the potential residence (location) of a criminal. Ring-shaped hotspots are also known as doughnut hole patterns or distance-decay zones.

Figure 4. Distance decay and buffer zone as described in environmental criminology
Burn, 1982.



Previous work on doughnut hole patterns focused on serial crime and used a formulation known as Rossmo's formula (Rossmo, 1995). Although it is a widely accepted method to determine the search area for a serial criminal's residence, Rossmo's formula has some limitations. It assumes a single crime source (e.g. serial criminal) and it lacks a statistical significance test.

Case Study on a Real Crime Data

Similar to the Circular Hotspot Detection, Ring-shaped hotspot detection (RHD) uses an activity set (i.e. crime locations) as input to detect ring-shaped hotspots in the study area. For example, Figure 5 shows a methamphetamine crime dataset collected from Chicago, Illinois (Chicago, 2014). The study area is selected as the minimum bounding orthogonal rectangle of the activity set. Activity set includes a sample of 48 methamphetamine possession and 6 methamphetamine manufacture/deliver crimes committed in Chicago, Illinois between March 2013 and March 2014. Note that the study area could be the territorial area of responsibility for a public safety agency. The aim is to find ring-shaped hotspots with a statistical significance level of $\alpha_p = 0.001$. Figure 6 shows the output of ring shaped hotspot detection with

Figure 5. Methamphetamine possession (48 cases shown in red dots) and methamphetamine manufacture/deliver crimes (6 cases shown in yellow stars) committed in Chicago between March 2013 between March 2014

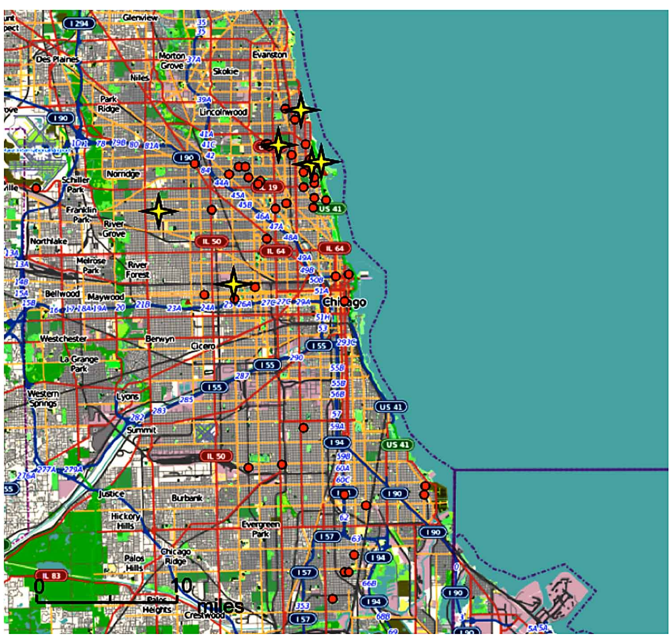
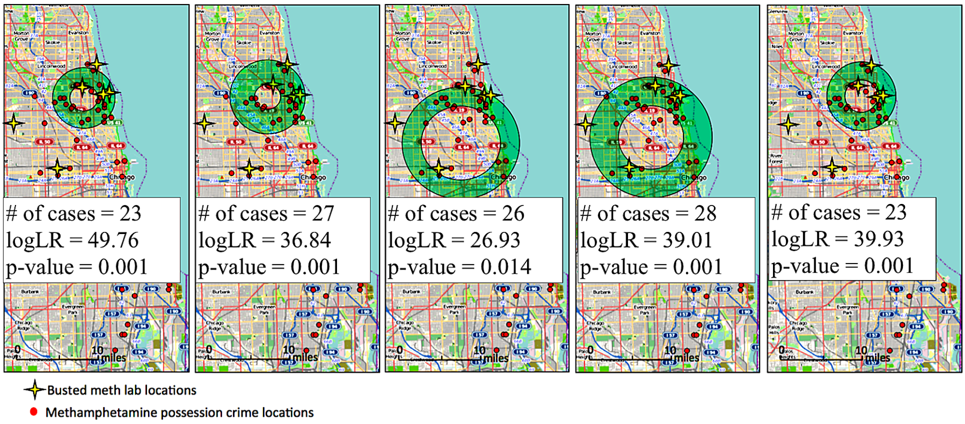


Figure 6. Output of ring shaped hotspot detection with 5 ring-shaped hotspots enumerated from the methamphetamine crime dataset in Figure 5



5 hotspot areas with high log likelihood ratios. Four of these hotspots have p-value = 0.001 which indicates statistical significance at 99.9% confidence level.

Ring-Shaped Hotspot Detection Algorithm

A ring shaped hotspot can be defined by a variety of techniques; here a ring is defined as a concentric ring (c-ring) (Eftelioglu et al., 2014) in this section.

Basic Concepts

- **C-Ring:** Any three non-collinear activities $a_1, a_2, a_3 \in A$ can uniquely identify a circle $circle_i$. For any activity point $a \in A$ outside $circle_i$, we can identify another circle $circle_o$ where a is on the circle and $circle_o$ is concentric with $circle_i$. The shape between any pair of such concentric circles $circle_i$ and $circle_o$ is defined as a C-Ring, denoted as *R*. Each C-Ring *R* has four parameters: the *x* and *y* coordinate of the center, the outer circle radius r_o, and the inner circle radius r_i. The area of the shape *R* is *area (R)*. Note that, for a given inner circle $circle_i$ with (x, y, r_i), there are many outer circles $circle_o$ (each defined by a distinct activity point *a* outside inner circle) and many c-rings *R*. (Eftelioglu et al., 2014)

Naïve Ring Shaped Hotspot Detection Algorithm

A naïve approach to ring shaped hotspot detection uses a three-step algorithm to detect statistically significant hotspots: (1) Enumeration of C-Rings, (2) Log likelihood ratio test and (3) Monte Carlo simulation and Hypothesis test. This chapter describes these three steps without any algorithmic refinements. In addition to the naïve algorithm, a faster approach with prune and refine steps will be shown.

Step 1 - Enumeration of Rings: Every three non-collinear points can define a unique circle. Using this notion, RHD enumerates every three non-linear points to generate the inner circles ($circle_i$) of c-rings. Once the inner circles are enumerated, using every activity point out of the inner circle, the outer circles are enumerated by using the distances from the inner circle center as outer circle radii. Using inner circles and outer circles c-rings *R* are generated. In RHD, since every three activity point creates an inner circle, the enumeration space for candidate c-rings is much larger than the enumeration space of circular hotspot detection.

Step 2 - Log Likelihood Ratio Test: Similar to the circular hotspot detection, the computation of $Log\ LR_Z$ requires the area and the number of points inside a zone *Z*. Suppose the zones are enumerated as ring-shaped hotspots in Step 1. Using the area of each c-ring and number of activity points inside, Log Likelihood Ratio of c-rings are computed.

Step 3 - Monte Carlo Simulation and Hypothesis Test: Monte Carlo simulation uses as similar algorithm to get the distribution of the log likelihood ratios under the null hypothesis. However, in Monte Carlo simulation, instead of the original input activity set A, random activity sets are generated under the null hypothesis and then Step 1 and Step 2 of the algorithm are run on these datasets. Among all c-rings enumerated using the random activity sets, only the c-ring with the highest likelihood ratio is stored for each random activity set. Then, the log likelihood ratio of each c-ring enumerated from the original activity set A is compared with this list and its corresponding position is determined. This position is divided into the number of Monte Carlo simulations *m* to determine the p-value of a c-ring. Finally, all non-overlapping c-rings with a p-value lower than the specified significance threshold α_p, are returned by the algorithm.

In a naïve approach to RHD problem, c-rings are enumerated by using circumcircle of all possible triplets of activities. Since each inner circle is created by three activities, outer circles are enumerated starting from the fourth activity. Thus the total number of inner circles is $\binom{|A|}{3}$ where |A| is the cardinality of the activity set A. For example, given an activity set with $|A| = 100$ activity points, $\binom{100}{3} = 161700$ inner circles are enumerated. Additionally, outer circles are enumerated using every point outside every inner circle. Therefore, the total number of candidate c-rings is high. For example, using an activity set of 1000 crime incidents, this number increases to approximately 10^{12} c-rings and computation time becomes exorbitant.

Dual Grid Based Pruning Algorithm

In order to address scalability limitation caused by the high number of c-rings generated by a naïve approach, Dual Grid based Pruning (DGP) algorithm namely DGP is proposed (Eftelioglu et al., 2014).

Simply, DGP algorithm defines an upper bound on the likelihood ratio of the c-rings. *The pruning phase* uses a dual grid approach, which keeps the number of activities in a geometric grid and enumerates c-rings in a parametric grid. For each ring enumerated in the parametric grid space an upper bound likelihood ratio is computed. Note that a c-ring in the parametric space represents a collection of actual c-rings in Euclidean space. Once the upper bound likelihood ratios are computed, the parametric grid cells which survive a given log likelihood ratio threshold are saved and the associated activity points are sent to the refine phase. *Refine phase* enumerates the actual c-rings and computes their likelihood ratios using the same enumeration technique described in the naïve approach. Finally, the candidate c-rings are tested for statistical significance using *Monte Carlo simulation phase.*

Limitations

The enumeration technique used in ring-shaped hotspot detection is costly. Although the DGP algorithm reduces the cost significantly, its refine phase still uses the same enumeration technique whereby triplets of points are used to enumerate inner circles and a fourth point to enumerate outer circles. An algorithm, which does not do extensive enumeration of rings, would be beneficial for efficient detection of c-rings.

A second limitation of RHD is that rings are assumed to be concentric. This is a very restrictive assumption. Imperfect rings and non-concentric rings which have occurred due to geographic features should be taken into account.

Finally, a ring shaped hotspot detected by Ring Shaped Hotspot Detection has strict boundaries. However, the diffusion of crimes described in circular hotspot detection holds in ring-shaped hotspots as well. Therefore, most crimes tend to show a diffusion process where moving further from the inner circle will cause less observation of activities.

Finally, a hotspot detected by Ring Shaped Hotspot Detection has strict boundaries. However, the diffusion of crime activity described in circular hotspot detection holds for ring-shaped hotspots as well. Since most crimes tend to show a diffusion process, moving further from the inner circle will cause less observation of activities. However, ring shaped hotspot detection does not take this into account.

LINEAR HOTSPOT DETECTION

The problem of linear hotspot detection (LHD) focuses on hotspots on network space. This problem is motivated by the fact that many types of crime only happen on road networks (e.g., street robbery). This section is organized as follows: First, a formal definition to the linear hotspot detection is introduced. Second, a motivating example for Linear Hotspot Detection is shown by a Case study on real data. Next, algorithms to solve the linear hotspot detection problem are introduced. Finally, the limitations of the proposed approaches are discussed.

Formally, given a spatial network (i.e. road network), a set of geo-located activities (i.e. crime reports), and a significance threshold, linear hotspot detection aims to find linear hotspots where the concentration of activities is significantly higher than other road segments. Detection of linear hotspots requires the following inputs specified by an analyst:

1. A spatial network (i.e. road network)
2. A spatial crime dataset with a collection of crimes each associated with a road segment,
3. A statistical significance threshold (α_p).

Based on the above inputs, the goal of linear hotspot detection is to report a collection of linear hotspot areas with p-value lower than the specified statistical significance threshold (α_p).

Case Study on a Real Crime Data

Linear hotspot detection will be illustrated with an example based on a crime dataset collected from Orlando, Florida in May 2015. Linear hotspot detection (LHD) uses activity locations and road network as input to detect the paths (road segments) where the number of activities is significantly higher than other road segments. For

Figure 7. Street robbery cases in Orlando, Florida in May 2015. Crime dataset includes 44 reported theft cases as shown in red

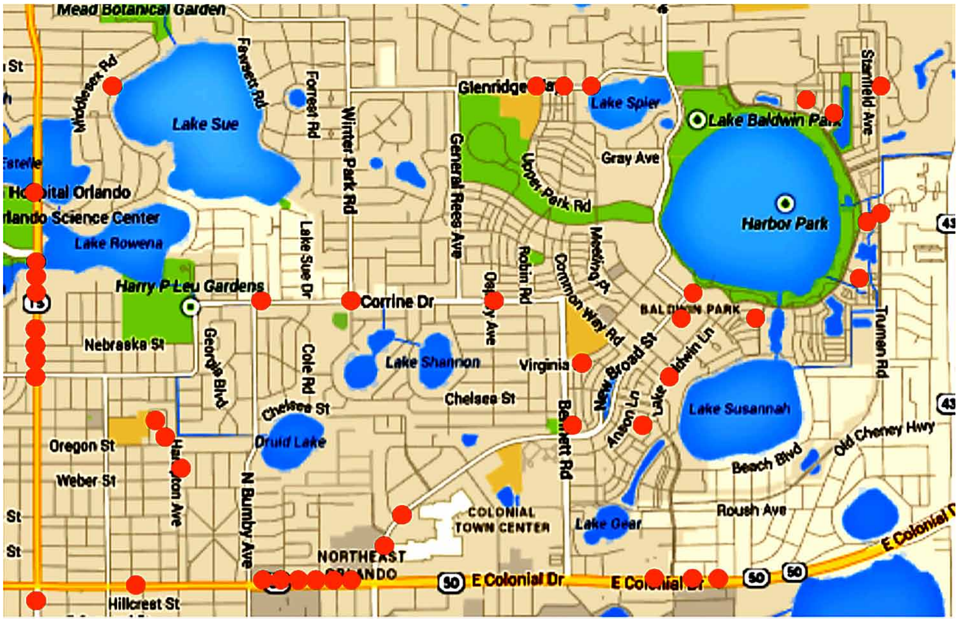
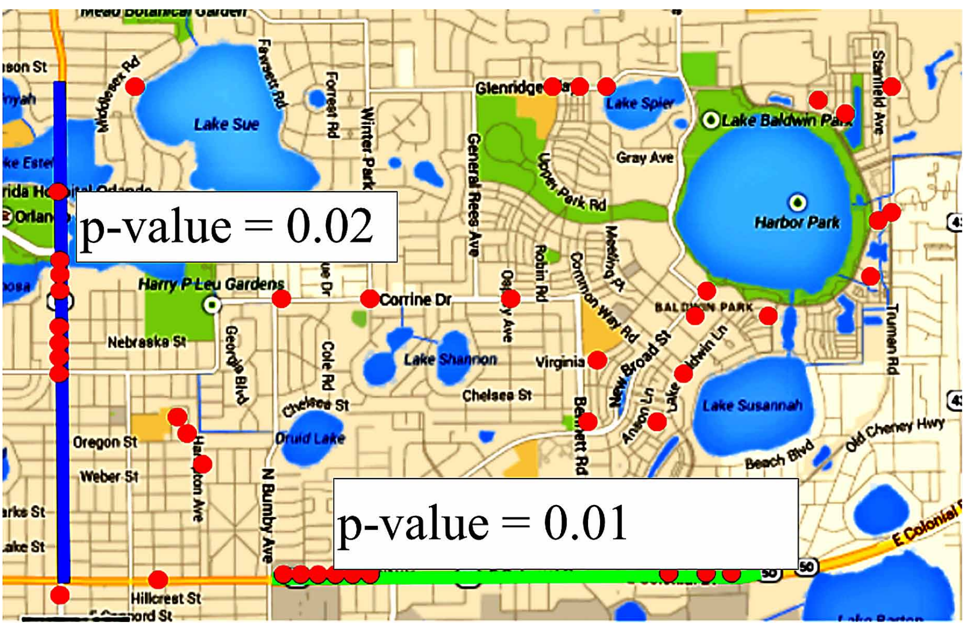


Figure 8. Output of linear hotspot detection



example, Figure 7 shows 44 street robbery crimes occurred in Orlando, Florida in May 2015. In this example, crime activities are shown by red dots (Orlando & FL, 2014). The input spatial network is the road network of the Orlando area. The aim is to find the linear hotspot areas with a statistical significance level of $\alpha_p = 0.03$. Figure 8 shows the output of Linear Hotspot detection with two significant paths. These paths are shown in blue and green and p-value is 0.02 and 0.01 respectively, which indicates statistical significance at 97% confidence level.

Linear Hotspot Detection Algorithm

Since linear hotspot detection is slightly different from hotspot detection in Euclidean space, related basic concepts will be introduced first, then a naïve and enhanced algorithm will be presented.

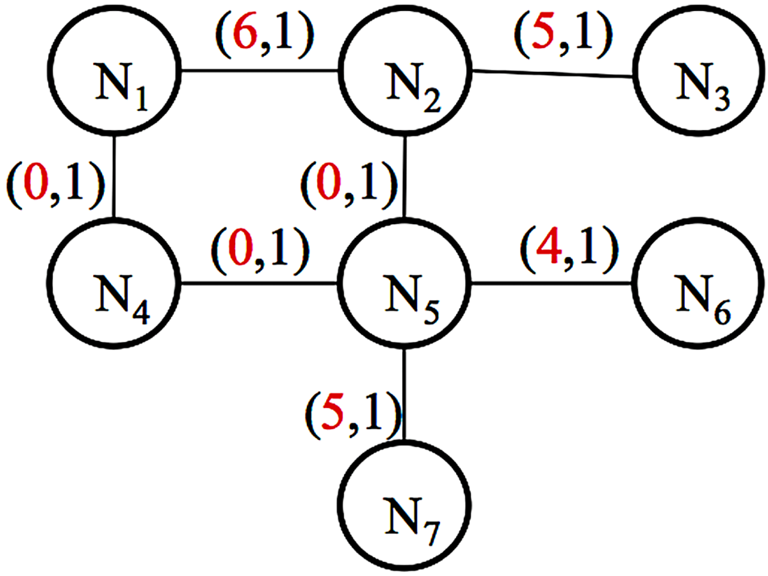
Basic Concepts

- **Spatial Network:** $G = (N, E)$ consists of a node set N and an edge set E, where each element u in N is associated with a pair of real numbers (x, y) representing the spatial location of the node in a Euclidean plane. Edge set E is a subset of the cross product N x N. Each element $e = (u, v)$ in E is an edge that joins node u to node v. Each edge has a weight w, which may represent its length or traffic density, etc. Note that each activity in the activity set A is associated with a specific edge in the spatial network $G = (N, E)$.
- **Distance:** Distance between any nodes in the spatial network is defined by the shortest path between the nodes. The triangle inequality of distance metric holds for this definition. Note that, the shortest path between two nodes could be not unique because there may be several paths with the same weight. However, the distance between two nodes is unique.

Figure 9 shows an example of spatial network, which contains 7 nodes denoted by 1, $N2 \ldots N7$ and 7 edges. Each edge is associated with *2* numbers (a, w), where a represents the number of activities associated with that edge, and w represents the weight of the edge. For the simplicity, the edge weights are set 1. For example, edge $(N1, N2)$ has 6 activities and a weight of 1.

- **Likelihood Ratio of a Path:** In the linear hotspot detection, the likelihood ratio function is used as described in Linear Semantic Likelihood Ratio computation (Janeja & Atluri, 2005b). The linear semantic likelihood ratio (LR_p) function is described as following:

Figure 9. An example spatial network



$$LR_p = \frac{\frac{a_p}{w_p}}{\frac{|A| - a_p}{|W| - w_p}}$$

As can be seen from the equation, the likelihood ratio of a path *p*, is the ratio of the activity density inside path *p* to the activity density outside *p*. In Figure 9, likelihood ratio of the path N_1, N_2, N_3, can be computed as

$$LR_p = \frac{\frac{11}{2}}{\frac{9}{5}} = 3.05$$

Note that although likelihood ratio of a path described in this section is different that the log likelihood ratio function described in Circular and Ring-Shaped Hotspot Detection, both functions can be used to assess the test statistic of an enumerated path.

Naïve Linear Hotspot Detection Algorithm (Oliver et al., 2014)

The basic idea behind linear hotspot detection algorithm is to find all statistically significant shortest paths in the spatial network whose likelihood exceeds θ. Note that the shortest paths returned are constrained so that they are not sub-paths of any other path in the output. This constraint aims to improve solution quality by reducing redundancy in the paths returned. The output is also constrained such that the shortest paths returned start and end with active nodes. This constraint also aims to improve solution quality by ignoring edges at the start and/or end of a path that do not have any activities.

Similar to the previous algorithms Naïve Linear Hotspot Detection algorithm (Oliver et al., 2014) consists of three steps.

Step 1 - Enumeration of Road Segments: In its first step naïve linear hotspot detection algorithm gets the spatial network as input and calculates the all pair shortest path for this spatial network.

Step 2 - Log Likelihood Ratio Test: For each enumerated road segment, this step computes the likelihood ratio if the starting and ending nodes are active nodes, meaning that the road segments should have activities associated with them. If any of the road segments has likelihood ratio higher than the specified threshold, they are saved into a candidate list for hypothesis test.

Step 3 - Monte Carlo Simulation and Hypothesis Test: In the Monte Carlo simulations, each activity in the original spatial network graph G is randomly associated with an edge so that the number of activities on each edge is shuffled, forming a new graph G_s. Note that all the activities in G are present in G_s, with no activities added or removed; the original activities in G are now shuffled so they may be on different edges in G_s. Then the highest likelihood of randomized G_s is compared with the highest likelihood ratio of original G. If the original one is smaller, then $p = p + 1$. The above process repeats m times and after it terminates, the p-value is subsequently p/m. Paths whose p-values are less than or equal to the given p-value threshold are deemed statistically significant and the null hypothesis is rejected.

LHD problem is challenging from computational perspective for several reasons. First, given a spatial network, the computation of all pair shortest paths is a costly operation. Moreover, the randomization test with Monte Carlo simulations (typically with 1000 trials) multiplies this cost. Second, log likelihood ratio function does not have monotonicity, which means given a path, its log likelihood ratio depends on both the number of activities and the weight of the path. Thus, monotonicity based pruning algorithms do not apply in LHD problem.

Smart Significant Route Miner Algorithm (Oliver et al., 2014)

A likelihood ratio pruning based algorithm is proposed to overcome the challenges of LHD problem. SmartSRM proposes an upper bound pruning approach to avoid computing all shortest paths of a graph. The framework of SmartSRM is similar to Dijkstra's algorithm, which uses a shortest path tree to represent the shortest paths from a source node (root of the tree) to all the other nodes. It stops growing a branch in the tree if the likelihood ratios of any shortest path on that branch must smaller than a specified likelihood ratio threshold $\alpha 1$. SmartSRM proposes a novel linear likelihood ratio upper bound to determine such branches. In addition, a Monte Carlo Simulation (MCS) early stop algorithm is used in SmartSRM. The key idea is stopping a MCS trial once a linear likelihood ratio is found higher than the highest one in the candidate paths.

Limitations

Linear hotspot detection (LHD) has a high computational cost due to the extensive all pair shortest path enumeration. Moreover, Monte Carlo simulation multiplies this cost. Another problem with LHD arises from the definition of a Linear Hotspot. LHD defines linear hotspots as starting and ending with Nodes. However, long paths between two nodes may cause missing a dense linear hotspot if the activities are in a specific part of a path. For instance, in Figure 9, although activities are dense in a part of the returned path LHD returned a longer path which starts and ends with Nodes in the Spatial Network. Finally, some road crimes occur when a criminal travels from one location to another, causing a linear hotspot, which moves in the network over time. However, LHD described in this section cannot evaluate linear hotspots that take the temporal dimension into account.

CURRENT HOTSPOT DETECTION TOOLS

This chapter focused on three representative techniques that use spatial scan statistics for crime hotspot detection. However, these are just the tip of the iceberg and there are many tools that modern police enforcement uses for crime mitigation as well as research on hotspot detection that are going on. In the following paragraphs, those tools will be presented. More detailed information on spatial aspect of crime can be found in (Brimicombe, 2005; Cohen & Felson, 1979; Gonzales, Schofield, & Hart, 2005; Levine, 2006; Ratcliffe & McCullagh, 1999; Wang et al., 2013; Yu, Ward, Morabito, & Ding, 2011).

Today, public security officials use crime analysis software for to improve their efficiency and reaction time (Spencer Chainey & Ratcliffe, 2013; Gonzales et al., 2005). Software, which are used by public security officials, depends on the crime type (i.e., fraud, cyber crime, gun related crime). For example, a fraud detection software may audit the stock exchange movements and determine fraudulent activity on stock market whereas a cyber crime software may focus on the detection of cyber crimes. Since this chapter is focused on crime hotspot detection, the following examples will focus on the “spatial” aspect of crime.

GIS tools (ESRI ArcGIS, QGIS, Python GDAL/OGR, etc.) can be used to determine locations for new police deployment, detect suspicious activities, integrate 911 emergency call locations, perform resource (i.e. patrol) allocation to incidents, and analyze the crime locations (Mitchell, 1999). Modern GIS software integrates the statistical analysis tools in order to determine hotspots of crime as well as the days and times of high crime activities. Although some crime specific features may be added to those GIS software (Goetz, n.d.), they are not specialized in crime activities. Therefore, several softwares (i.e. CrimeStat) were developed to analyze the spatial aspect of crime. CrimeStat (Lavine, 2013), a software package for spatial analysis of crime locations, incorporates several methods to determine the crime hotspots in a study area. CrimeStat package has k-means tool, nearest neighbor hierarchical (NNH) clustering, Risk Adjusted NNH (RANNH) tool, STAC Hot Spot Area tool, and a Local Indicator of Spatial Association (LISA) tool that are used to evaluate potential hotspot areas (Leong K, 2015). Urban Growth Simulator (UGS), which is developed at Kent State University, aims to estimate changes in crime rates as induced by urban growth (Lee, Brody, Zhang, Kim, & Bradac, 2002). Rigel software, which depends on Rossmo’s Formula, uses crime locations, suspect information, case details and investigator details to analyze a series of linked crimes and determine the most probable locations of the offender’s residence (Beauregard, Proulx, & Rossmo, 2005; Devlin & Lorden, 2007). Hotspot Detective, which is (was) an add-on for MapInfo Software, uses a grid based approach together with kernel density estimation to determine hotspot locations (S Chainey, Tompson, & Uhlig, 2008).

Apart from the software above, several spatial statistical analysis tools are also used for the analysis of the spatial aspect of crime. For example, GeoDa, a spatial data analysis software, can be used to do multivariate exploratory data analysis, global and local spatial autocorrelation analysis, and basic linear regression with crime data (Anselin, Syabri, & Kho, 2006). In addition, several R software packages (spatstat, geoR, spdep, etc.) are widely used for spatial analysis of point referenced data (e.g. crime locations) (R Development Core Team, 2011). Finally, it is worth noting that there are many web-based crime analysis and visualization tools thanks to the spatial abilities of HTML5 (Holdener, 2011).

FUTURE RESEARCH DIRECTIONS

Although there are a variety of techniques (Ester & others, 1996; Ilango & Mohan, 2010; Karypis, Han, & Kumar, 1999; Levine, 2006; Wu et al., 2008) which are developed to be used in different domains, the techniques described in this chapter are representative approaches to detect circular, ring-shaped and linear hotspots given an activity set. In this section, some important research topics that include methodological advancements that may be needed to analyze crime hotspots are reviewed.

Crime occurrences are always associated with a population. However, the techniques described here do not take the population into account. For example, in most of the crime datasets used in this chapter, crime activities are dense near downtowns since these locations are dense in population. When detecting crime hotspots, the underlying population should be taken into account to reflect this.

In addition, the circular and ring-shaped hotspot detection techniques described here are based on the Euclidean space. However, people tend to use road networks to travel. Similarly, criminals tend to use the road network to travel to the crime sites. Thus, even a hotspot detection technique which focuses on circular hotspots should take road network distances into account. Detecting hotspots on a road network may provide additional insights that crime analysts can use to identify patrolling districts after taking a variety of other factors into consideration. Linear hotspot detection technique described in this section considers spatial network nodes as the starting and ending nodes of a significant road path. In order to detect partial road segments with high number of activities, activities on a spatial network can be considered as dynamic nodes, and the edges can be segmented accordingly. Linear hotspot detection on this new "dynamic segmented" spatial network may be able to give more precise location of hotspots. Techniques described in this chapter focus on the spatial dimensions of crime hotspots in either in Euclidean Space or Spatial Networks. However, new hotspot detection techniques are required which can evaluate the temporal space and detect hotspots using a constant flow of new crime activities.

Furthermore, fuzzy statistically significant hotspot detection techniques are needed to better represent the diffusion of crimes. Techniques described in this chapter detect crime hotspot areas with strict boundaries. Since the crime activities are similar to the diffusion processes in Physics and Chemistry, the crime activities become sparser when moving further from the center. Therefore, new fuzzy hotspot detection techniques are needed.

Given the current rate of crimes each year (e.g. annual 10^7 crimes U.S.), any crime hotspot detection technique should also consider the scalability of the designed algorithms. For example, the circular hotspot detection technique (i.e. SaTScan) described in this chapter is limited to a couple of thousands of activity points (i.e. crimes) due to the extensive circle enumeration using points as centers. Therefore, there is a need for new scalable algorithms to handle the high number of crime activities.

In this chapter, hotspot detection using the locations of crime incidents (geo-located crimes) is discussed. However, in the light of the technological advances, digital crimes (i.e. cyber crimes) are starting to get prevalent among crimes (Fei, Eloff, Olivier, & Venter, 2006). Such crimes include child abuse, hacking, financial theft, stealing private and/or confidential data etc. (Robert W. Taylor, Tory J. Caeti, D. Kall Loper, Eric J. Fritsch, 2006). Although these crimes do not have a specific location information (i.e., longitude, latitude), an approximate location can be captured from suspects' internet address (i.e. IP address) (Kao & Wang, 2009). However, since the locations of these crimes will be approximate (unlike a crime location in geographic space), new hotspot detection techniques are required to capture these events. Moreover, social media posts (Twitter, Facebook etc.) and geo-tags can be leveraged as well as the social network connections (i.e. friends, buddies) to have a sense of a criminal's location (Surette, 2010). Such opportunities can be new frontiers for hotspot detection.

CONCLUSION

This chapter explored crime hotspot detection methods, which is an important task in environmental criminology. When evaluating hotspot detection techniques, this chapter focused on the statistically significant hotspot detection techniques, to reduce false positive rates (i.e. hotspot areas which are occurred by chance). The chapter started with the foundations of Spatial Scan Statistics and the applications using Spatial Scan Statistics to find statistically significant circular hotspots. Next, ring-shaped hotspot detection is described. Finally, since most crimes occur and diffuse along a road network, linear hotspots are illustrated. Finally, chapter is concluded with future directions and opportunities for the crime hotspot detection task.

ACKNOWLEDGMENT

This material is based upon work supported by the National Science Foundation under Grant Number 1029711, IIS- 1320580, 0940818 and IIS-1218168, USDOD under Grant Number HM1582-08-1-0017, HM0210-13-1-0005, and University of Minnesota via U-Spatial. We would like to thank Kim Koffolt and the members of the University of Minnesota Spatial Computing Research Group for their comments.

REFERENCES

Agarwal, D., McGregor, A., Phillips, J. M., Venkatasubramanian, S., & Zhu, Z. (2006). Spatial scan statistics. In *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '06* (p. 24). http://doi.org/10.1145/1150402.1150410

Anselin, L., Syabri, I., & Kho, Y. (2006). GeoDa: An introduction to spatial data analysis. *Geographical Analysis*, *38*(1), 5–22. doi:10.1111/j.0016-7363.2005.00671.x

Beauregard, E., Proulx, J., & Rossmo, D. K. (2005). Spatial patterns of sex offenders: Theoretical, empirical, and practical issues. *Aggression and Violent Behavior*, *10*(5), 579–603. doi:10.1016/j.avb.2004.12.003

Belenko, S. R., & Spohn, C. (2015). *Drugs, crime, and justice*. Academic Press.

Brantingham, P. L., & Brantingham, P. J. (1993). Environment, Routine, and Situation: Toward a Pattern Theory of Crime. *Routine Activity and Rational Choice: Advances in Criminological Theoy*, *5*, 259–294.

Brimicombe, A. J. (2005). *Cluster Detection in Point Event Data having Tendency Towards Spatially Repetitive Events*. Intl. Conf. on GeoComputation.

Burn, O. (1982). *Environmental criminology. Journal of Criminal Justice* (Vol. 10). Sage Publications. http://doi.org/ doi:10.1016/0047-2352(82)90028-9

Chainey, S., & Ratcliffe, J. (2013). *GIS and Crime Mapping*. GIS and Crime Mapping; doi:10.1002/9781118685181

Chainey, S., Tompson, L., & Uhlig, S. (2008). *The Utility of Hotspot Mapping for Predicting Spatial Patterns of Crime*. http://doi.org/ doi:10.1057j.2008.6

City of Chicago. (2013). *City of Chicago Data Portal*. Retrieved from https://data.cityofchicago.org/

City of Chicago. (2014). Methamphetamine Possession Cases Chicago 2013. Chicago.

City of Orlando, FL. (2014). *Orlando Crime Dataset*. Author.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588. doi:10.2307/2094589

Coleman, M., Coleman, M., Mabuza, A. M., Kok, G., Coetzee, M., & Durrheim, D. N. (2009). Using the SaTScan method to detect local malaria clusters for guiding malaria control programmes. *Malaria Journal*, *8*(1), 68. doi:10.1186/1475-2875-8-68 PMID:19374738

Devlin, K., & Lorden, G. (2007). *The Numbers Behind NUMB3RS: Solving Crime with Mathematics.* Academic Press.

Eck, J., & others. (2005). *Mapping crime: Understanding hotspots*. Academic Press.

Eftelioglu, E., Shekhar, S., Oliver, D., Zhou, X., Evans, M. R., & Xie, Y., … Farah, C. (2014). Ring-Shaped Hotspot Detection: A Summary of Results. In *2014 IEEE International Conference on Data Mining* (pp. 815–820). 10.1109/ICDM.2014.13

Estepp, I. (1987). Motived-based Offender profiles of arson and fire-related crimes. *FBI Law Enforcement Bulletin*, *56*(4), 17–23.

Ester, M., & ... (1996). *A density-based algorithm for discovering clusters in large spatial databases with noise* (pp. 226–231). AAAI Press.

Fei, B. K. L., Eloff, J. H. P., Olivier, M. S., & Venter, H. S. (2006). The use of self-organising maps for anomalous behaviour detection in a digital investigation. *Forensic Science International*, *162*(1-3), 33–37. doi:10.1016/j.forsciint.2006.06.046 PMID:16876359

Goetz, S. L. (n.d.). *ArcGIS Tool Implementation of Risk Terrain Modeling.*

Gonzales, A. R., Schofield, R. B., & Hart, S. V. (2005). Mapping Crime: Understanding Hot Spots. National Institute of Justice, 79.

Haklay, M., & Weber, P. (2008). OpenStreetMap – User Generated Street Map. *IEEE Pervasive Computing / IEEE Computer Society [and] IEEE Communications Society*, *7*(4), 12–18. doi:10.1109/MPRV.2008.80

Holdener, A. T. (2011). HTML5 Geolocation. *Online*, 114. Retrieved from http://books.google.com/books?id=9aIA5P6dp2cC&pgis=1

Ilango, M., & Mohan, V. (2010). A survey of grid based clustering algorithms. *International Journal of Engineering Science*, *2*(8), 3441–3446. Retrieved from http://www.ijest.info/docs/IJEST10-02-08-17.pdf

Janeja, V. P., & Atluri, V. (2005a). LS3: a Linear Semantic Scan Statistic technique for detecting anomalous windows. *Proceedings of the 2005 ACM Symposium on Applied Computing*, (pp. 493–497). http://doi.org/http://doi.acm.org/10.1145/1066677.1066790

Janeja, V. P., & Atluri, V. (2005b). LS3: a Linear Semantic Scan Statistic technique for detecting anomalous windows. In *Proceedings of the 2005 ACM symposium on Applied computing* (pp. 493–497). http://doi.org/http://doi.acm.org/10.1145/1066677.1066790

Kao, D.-Y., & Wang, S.-J. (2009). The IP address and time in cyber-crime investigation. *Policing: An International Journal of Police Strategies & Management*, *32*(2), 194–208. doi:10.1108/13639510910958136

Karypis, G., Han, E.-H. H. E.-H., & Kumar, V. (1999). Chameleon: Hierarchical clustering using dynamic modeling. *Computer*, *32*(8), 68–75. doi:10.1109/2.781637

Kulldorf, M. (1999). *Spatial Scan Statistics: Models, Calculations and Applications. Scan Statistics and Applications*. Springer; doi:10.1007/978-1-4612-1578-3_14

Kulldorff, M. (1997). A spatial scan statistic. *Communications in Statistics. Theory and Methods*, *26*(6), 1481–1496. doi:10.1080/03610929708831995

Kulldorff, M. (2010). *SaTScan User Guide v. 9.0*. Academic Press.

Kulldorff, M., Huang, L., Pickle, L., & Duczmal, L. (2006). An elliptic spatial scan statistic. *Statistics in Medicine*, *25*(22), 3929–3943. doi:10.1002im.2490 PMID:16435334

Lavine, N. (2013). *Introduction to CrimeStat IV (CrimeStat IV: A Spatial Statistics Program for the Analysis of Crime Incident Locations, Version 4.0)*. Academic Press.

Lee, J., Brody, T. M., Zhang, R., Kim, H., & Bradac, M. (2002). *Simulating Urban Growth on the Web*. Academic Press.

Leong K, S. A. (2015). A review of spatio-temporal pattern analysis approaches on crime analysis. *International E-Journal of Criminal Sciences, 9*.

Levine, N. (2006). Crime mapping and the crimestat program. *Geographical Analysis*, *38*(1), 41–56. doi:10.1111/j.0016-7363.2005.00673.x

Liao, W., & Liu, Y., & Choudhary, A. (2004). A grid-based clustering algorithm using adaptive mesh refinement. *Proc. of the 7th Workshop on Mining Scientific and Engineering Datasets*.

Maguire, M. (2008). *Crime statistics*. Retrieved January 1, 2015, from https://www.fbi.gov/stats-services/crimestats/

Martin Kulldorff. (2014). *SaTScan User Guide for Version 9.3*. StatScan. Retrieved from http://www.satscan.org/

McCullagh, M. (2006). Detecting hotspots in time and space. *Isg06*, 1–18. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.158.2442&rep=rep1&type=pdf

Mitchell, A. (1999). The ESRI guide to GIS analysis. Volume 1: Geographic patterns & relationships. *Annals of Physics*, *54*, 87–88. Retrieved from http://books.google.com/books?id=FOj8L-iDMq0C&pgis=1

Neill, D. B. (2009). An empirical comparison of spatial scan statistics for outbreak detection. *International Journal of Health Geographics*, *8*(1), 20. doi:10.1186/1476-072X-8-20 PMID:19371431

Neill, D. B., & Moore, A. W. (2004). Rapid detection of significant spatial clusters. In *Proceedings of the 2004 ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '04* (p. 256). http://doi.org/10.1145/1014052.1014082

Oliver, D., Shekhar, S., Zhou, X., Eftelioglu, E., Evans, M. R., & Zhuang, Q. … Farah, C. (2014). Significant Route Discovery: A Summary of Results. In Proc. of GIScicence (pp. 284–300). Springer.

Patil, G. P., & Taillie, C. (2004). Upper level set scan statistic for detecting arbitrarily shaped hotspots. *Environmental and Ecological Statistics*, *11*(2), 183–197. doi:10.1023/B:EEST.0000027208.48919.7e

Prates, M. O., Assunção, R. M., & Costa, M. (2012). Flexible scan statistic test to detect disease clusters in hierarchical trees. *Computational Statistics*, *27*(4), 715–737. doi:10.100700180-011-0286-9

Quantum GIS Development Team. (2012). Quantum GIS Geographic Information System. *Open Source Geospatial Foundation Project*. Retrieved from http://qgis.osgeo.org

R Development Core Team. (2011). R Language Definition. *Web*, *0*, 62. doi:10.1016/0164-1212(87)90019-7

Ratcliffe, J. H., & McCullagh, M. J. (1999). Hotbeds of crime and the search for spatial accuracy. *Journal of Geographical Systems*, *1*(4), 385–398. doi:10.1007101090050020

Rossmo, D. K. (1995). *Geographic profiling: Target patterns of serial murderers. ProQuest Dissertations and Theses. Theses (School of Criminology)*. Simon Fraser University.

Sarmah, S., Das, R., & Bhattacharyya, D. K. (2007). Intrinsic Cluster Detection Using Adaptive Grids. *15th International Conference on Advanced Computing and Communications (ADCOM 2007)*. http://doi.org/10.1109/ADCOM.2007.18

Shi, L., & Janeja, V. P. (2011). Anomalous window discovery for linear intersecting paths. *IEEE Transactions on Knowledge and Data Engineering*, *23*(12), 1857–1871. doi:10.1109/TKDE.2010.212

Surette, R. (2010). *Media, Crime, and Criminal Justice*. Retrieved from http://books.google.com/books?id=geK4L1Q7fqAC&pgis=1

Walther, G. (2010). Optimal and fast detection of spatial clusters with scan statistics. *Annals of Statistics*, *38*(2), 1010–1033. doi:10.1214/09-AOS732

Wang, D., Ding, W., Lo, H., Stepinski, T., Salazar, J., & Morabito, M. (2013). Crime hotspot mapping using the crime related factors - A spatial data mining approach. *Applied Intelligence*, *39*(4), 772–781. doi:10.100710489-012-0400-x

Wu, X., Kumar, V., Ross Quinlan, J., Ghosh, J., Yang, Q., Motoda, H., … Steinberg, D. (2008). Top 10 algorithms in data mining. *Knowledge and Information Systems* (Vol. 14). http://doi.org/ doi:10.100710115-007-0114-2

Yu, C.-H., Ward, M. W., Morabito, M., & Ding, W. (2011). Crime Forecasting Using Data Mining Techniques. *2011 IEEE 11th International Conference on Data Mining Workshops*, (pp. 779–786). http://doi.org/10.1109/ICDMW.2011.56

Zhang, Y. (2010). *Hotspot Analysis of Highway Accident Spatial Pattern Based on Network Spatial Weights*. Academic Press.

This research was previously published in Data Mining Trends and Applications in Criminal Science and Investigations edited by Omowunmi E. Isafiade and Antoine B. Bagula; pages 82-111, copyright year 2016 by Information Science Reference (an imprint of IGI Global).

Chapter 11
Novel First Responder Digital Forensics Tool as a Support to Law Enforcement

Mitko Bogdanoski
Military Academy "General Mihailo Apostolski", Macedonia

Marjan Stoilkovski
Ministry of Interior, Macedonia

Aleksandar Risteski
Ss. Cyril and Methodius University, Macedonia

ABSTRACT

There are many freeware and commercial tools which can be used to provide forensics information based on dead and live forensics acquisition. The main problem with these tools is that in many cases the investigator cannot explain the script functionality and generated results and information during the trial. Because of this reason there is an increased need for developing and using script which can be easy explained and adapted to any analysis which should be made by the examiners. The chapter presents a novel developed First Responder script which can be used to perform a live and dead forensics analysis in support of Law Enforcement during the investigation process.

DOI: 10.4018/978-1-7998-2535-7.ch011

INTRODUCTION

Nowadays, the security of information systems is crucial. There is almost no organization that does not take appropriate security measures on its own level in order to protect systems from external and internal attacks. To ensure an adequate level of security, the organizations have started establishing special CERT (*Community Emergency Response Team*) teams whose key objective is to increase information security in the organization. In case if there are no such teams established, this role is undertaken by system administrators, who must *attend specialized training* to perform those unique duties connected with cyber security.

In order to increase the information security and users' awareness, all the users of the information systems in the organization should be trained about the secure usage of the systems, ethics in information system, and the way of reporting for any registered computer incident. The need for this training is because each of them can, intentionally or unintentionally, harm the security of the information systems, and consequently harm the security of the organization.

However, no matter how much the companies invest in information security and no matter how much the staff is trained, there will always be malicious users, which driven by different motives will try to exploit vulnerabilities in hardware and software solutions in the company, as well as employees' negligence. Very often, the attackers in their intentions are supported by internal attacks made by employees in companies (insiders).

The goal of the companies is to stop attackers in the perimeter network, i.e. not to allow them to enter the internal network of the company/organization. The reason for this is that when the attacker enters in the internal network and systems the only thing left is to resist malicious users using computer forensics. However, very often the responsible for information security in the companies cannot catch the attackers at the perimeter network, so after registering intrusion into the system they must react immediately and analyze the intentions of the attackers. In order the analysis to be at the highest level the responsible for information security must be trained to make a detailed analysis of the attack and, if it is possible, to discover as much information about the attacker. Sure that, even the attacker is discovered, the intrusion must be reported and companies need to ask for assistance from the competent authorities to tackle cyber threats (law enforcement), and to initiate appropriate action against the attackers.

In this whole process of discovering the intentions of the attack, as well as detection of offenders, the computer forensics takes a main role. In the process of information gathering basic analysis will be performed using traditional forensics, but if there is the slightest chance, live forensics should be performed on the running computer systems. Using the live response the investigator can capture all the volatile data that will be lost as soon as the machine is powered down, such as the current configuration of the machine and the data in its RAM memory. It should be noted that, whether traditional or live forensics is performed, during the entire process of systems' analysis the investigators should avoid possible corruption of the original data.

The purpose of this chapter is to provide basic concepts for live forensics and to explain its advantage when instead of automated software tools for computer forensics the investigators are using specially created scripts that are easy to adapt as necessary, i.e. accordingly to the needs of the forensic examiners. For this purpose, the rest of the chapter is organized as follows. Section 2 gives a brief overview of live computer forensics investigation process. Moreover, Section 3 explains how other disciplines are impacted by computer forensics. Section 4 shows the classification of the digital forensics as well as different models and frameworks for digital investigation process. Section 5 outlines the process of analysis of the RAM. In Section 6 the functionality and capabilities of the developed First Responder script are explained. Finally, the Section 7 concludes our work.

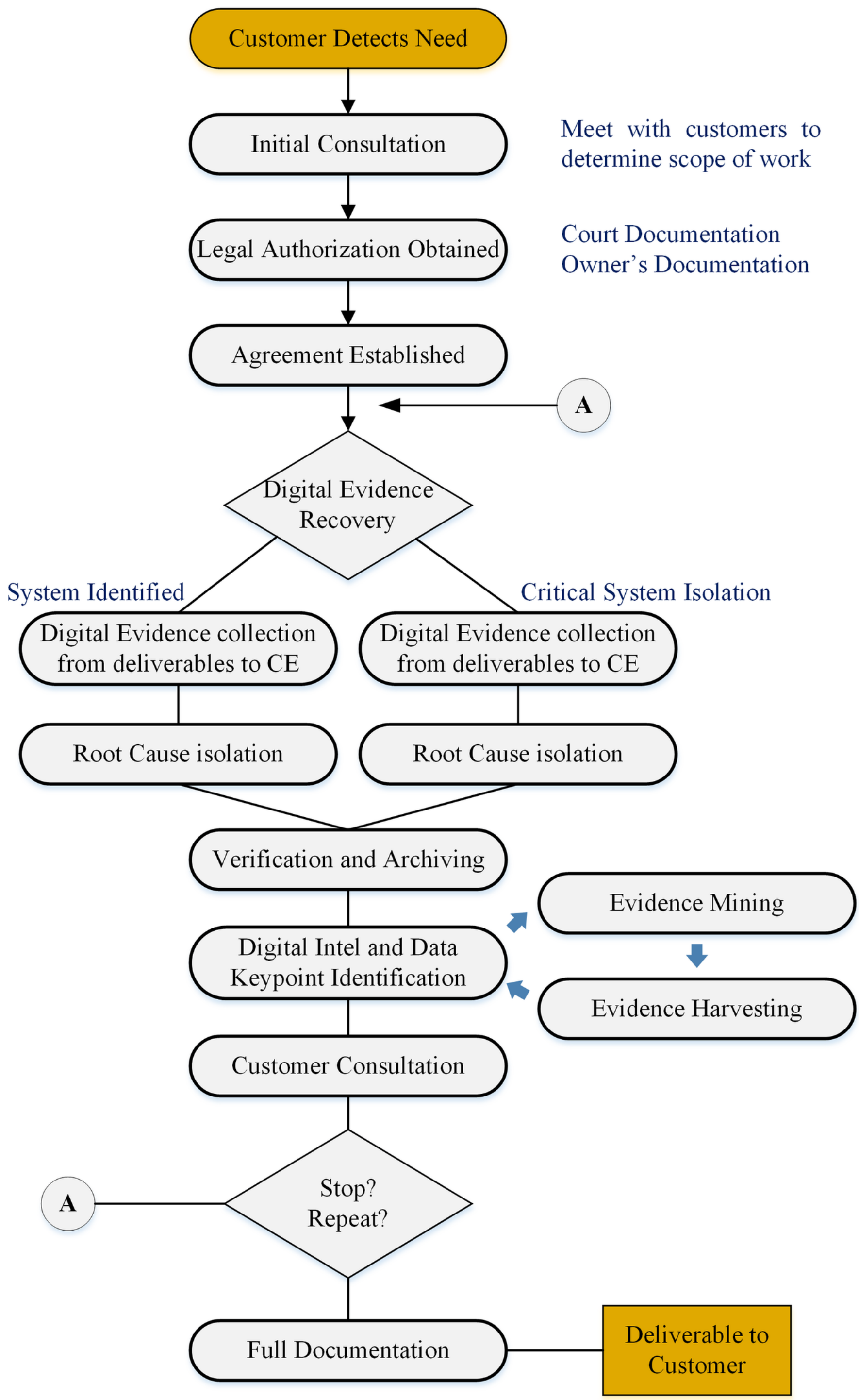
COMPUTER FORENSICS INVESTIGATION PROCESS

Digital forensics, as a branch of forensic, is a process of discovering and interpreting of the electronic data that would later be used in court. In fact, according to (Politt, 2004), the digital forensics is not just a process, but a group of processes used in the investigation. The purpose of these processes is to provide evidence in its most original form while performing investigation by collecting, identifying and validating the digital information in order to reconstruct some events from the past. On the other hand, the computer forensics is a branch of digital forensic pertaining to legal evidence found in computers and digital storage media.

There are many definitions about computer forensics, but according to us the most acceptable definition is that given by the US-CERT team, who defines the computer forensics as a discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law (US-CERT, 2008).

Computer forensics investigation processes take a lot of time to conduct, and this time for investigation is constantly going up. The reason for this primarily is because of the constant increase of the size of storage media that is being encountered. In addition, the amount of devices and data storage that must be searched and analyzed is also increasing. As it can be seen in the Figure 1, the main steps during

Figure 1. Computer forensic investigation process



the computer forensic investigation process are the following (Chaudhay, 2013) (Ashcroft, Daniels, & Hart, 2004):

- **Assessment:** During this step, the digital evidences are assessed thoroughly with respect to the scope of the case. This is done in order to determine the course of action to be taken. Forensic analysts can also perform cross drive analysis, which correlates information found on multiple hard drives (Garfinkel, 2012).
- **Acquisition:** The analysts should properly conduct the handling process with the aim not to alter, damage or destroy any digital. In order to make sure that the original evidence will not be affected, the analysts are making a complete image copy of the original evidence using the MD5 algorithm, making sure that original evidence is not tampered with. In the case when some of the files are deleted the analysts can recover the files using a special forensics tool like Encase. They can reconstruct the data from physical disk sectors by searching of known file headers within the disk image and reconstructing the deleted information.
- **Examination:** During this step an analysis of the digital evidence from the media is conducted. Analyzed data from the recovered information should be put in a useful and logical format. In order to conduct quality analysis and interpretation, the analyst can use various tools, for example, tools discovering and cracking passwords, for windows registry, extracting emails and pictures, keyword searches, etc. One of the hardest analyzes to be made by forensic analysts is deducing stenographic images to excavate what is hidden in those images (Bogdanoski, Risteski, & Pejoski, 2012).
- **Documentation and Reporting:** All the actions and observation analysis conducted by the forensic analysts should be promptly documented. The end product from the evidence handling process which must be done by the analysts is a written report of the findings.

DISCIPLINES IMPACTED BY DIGITAL FORENSICS

There are several disciplines impacted in some way by the digital forensics. Table 1 shows these disciplines as well as the way digital forensics impacts on these disciplines.

Table 1. Disciplines impacted by digital forensics

Discipline	Impact
Law	Computer forensic practitioners are consulted to determine changes in the law which could aid investigations. An ongoing example of this is Part III of the Regulation of Investigative Powers Act (RIPA) (RIPA, 2000). This makes the act of not proving a known cryptographic key to the police when requested a criminal offense. RIPA Part III was formulated in direct response to criminals' use of encrypted files to hamper forensic analysis.
Computer Science	A large proportion of the work of a forensic practitioner is the analysis of traces left behind by software. Software developed by computer scientists may have an impact on the analytical value and evidential integrity of that data.
Forensic Science	The goals and restrictions placed upon evidence are the same for computer forensics as forensics in general. When computer forensic practitioners work with forensic scientists, they must be aware of the effects of the other's actions. For example, the techniques used to lift fingerprints from surfaces can damage computer hardware (Johnson, 2005).
Criminal Investigation	Any improvements in computer forensics give investigators the greater flexibility to conduct inquiries.
Computer Security	Computer networks and systems can be configured with consideration for forensic readiness. Effective preparation, such as logging maximizes the chances of a successful prosecution
System Administrator	First responders to security incidents are often system administrators. If they act in a forensically safe manner they are able to collect evidence for possible future prosecutions.
Businesses	Advances in computer forensics, which reduce the disruption caused by an investigation are advantageous.

CLASSIFICATION OF THE DIGITAL FORENSICS

Digital forensics is an important part of the computer investigation process of data recovering. Although there are many classifications of this discipline, this chapter adopted one of the most common used classification in the literature which includes: post mortem digital forensics, live digital forensics, network forensics, and mobile forensics.

- Post mortem digital forensics (also known as dead digital forensics) is the process of conducting an investigation on an unpowered device (Ademu, 2011).
- Live digital forensics, on the other hand, deal with extracting system data before disconnecting the digital device's power source, in order to preserve memory and information that would be lost using the post mortem approach (McDougal, 2007).

- Network forensics deals with preserving and collecting digital evidence in a connected digital environment (Jansen, 2006).
- Mobile forensics is the science of recovering digital evidence from a mobile device like a smart phone (Jansen, 2006).
- GPS (Global Positioning System) forensics (also known as SatNav forensics) is the reliable and repeatable process of acquiring, examining and analyzing GPS devices for evidence of a criminal act or information of interest. (Arbelet, 2014), (Last, 2009)

Table 2. Digital forensic investigation process models and frameworks

Process Model Name	References	Number of Phases
A Road Map for Digital Forensic Research	(Palmer, 2001)	7 phases
An examination of digital forensic models	(Reith, 2002)	9 phases
Electronic Crime Scene Investigation - A Guide for First Responders	(Justice, 2001)	8 phases
Getting Physical with the Digital Investigation Process	(Carrier, 2003)	5 groups, 17 phases
Incident Response & Computer Forensics	(Mandia, Prosise, & Pepe, 2003)	11 phases
A Hierarchical, Objectives-Based Framework for the Digital Investigation Process	(Beebe N. L., 2005)	6 phases
An Extended Model of Cybercrime Investigations	(Ciardhuain, 2004)	12 phases
Fundamentals of Digital Forensic Evidence	(Cohen, 2011)	11 phases
A Chapter in Forensic Analysis, in: Handbook of Digital Forensics and Investigation Digital Forensics and Investigation.	(Casey, 2010)	4 phases
Good Practice Guide for Computer-Based Evidence	(ACPO, 2008)	13 phases
Harmonized Digital Forensic Investigation Process (HDFIP) model	(Valijarevic & Venter, 2012)	14 phases
End-to-End Digital Investigation Process	(Stephenson, 2003)	9 phases
The Enhanced Digital Investigation Process	(Baryamureeba, 2006)	5 major phases including sub-phases
The Lifecycle Model	(Harrison, 2004)	7 phases
The Investigation Framework	(Kohn, Eloff, & Olivier, 2006)	7 phases
The Forensic Process	(Kent, Chevalier, Grance, & Dang, 2006)	4 phases
Digital Forensics Investigation Procedure Model	(Yong-Dal, 2008)	10 phases
The Computer Forensics Field Triage Process Model	(Roger, Goldman, Mislan, Wedge, & Debrota, 2006)	6 major phases including sub-phases

Due to the vast number of digital forensic investigation process models, the standardization of an investigation process model in digital forensics has become a matter of priority. Existing digital forensic investigation process models show notable disparities, such as the number of phases and the scope of models (Valijarevic & Venter, 2012); hence the need for standardization. Table 1, for example, presents some of the process models developed over the years, with different models comprising different numbers of phases.

From Table 2, it is clear that there exist a number of digital forensic investigation process models, stemming from different researchers and organizations. The different number of phases in each proposed model adds to the disparities among the investigation models.

The following section will consider the advantages and limitation of the first two mentioned types of digital forensics: Traditional (dead) and Live computer forensics.

TRADITIONAL (DEAD) VS. LIVE DIGITAL FORENSICS

Traditional (Dead) Forensics

In order forensic acquisition to be more reliable, it must be performed on computers that have been powered off. This type of forensics is known as ‘traditional’ or ‘dead’ forensic acquisition. The whole process of dead acquisition, including search and seizure flowchart and acquisition of the digital evidence flowchart is shown on Figure 2 and Figure 3 respectively.

During this process the investigators should carefully search for all forms of potential electronic evidence that they do have permission to take, such as: USB (*Universal Serial Bus*) storage media, optical discs, mobile phones, tablets, laptops, SD (Secure Digital) and similar cards, NAS (Network-Attached Storage). Other forms of forensic evidence should be also considered such as: fingerprints and DNA before collection of devices, passwords, notes, paper documents, and other information relevant to the investigation.

The process of dead forensic is simple, reliable and thorough. The main strength of the dead forensic is precisely defined process of acquisition. The acquisition process can be verified at any time. The process of dead forensic acquisition is simple and does not require very strong programming knowledge. If the acquisition process is strictly followed by the examiners it is impossible to alter the data on the hard disk.

However, if the analysts conduct only simple file copying, the files from some locations such as kernel and process memory, unallocated disk space, removed files, swap files, peripherals, and other will not be collected. Because of this reason

Figure 2. Search and seizure flowchart

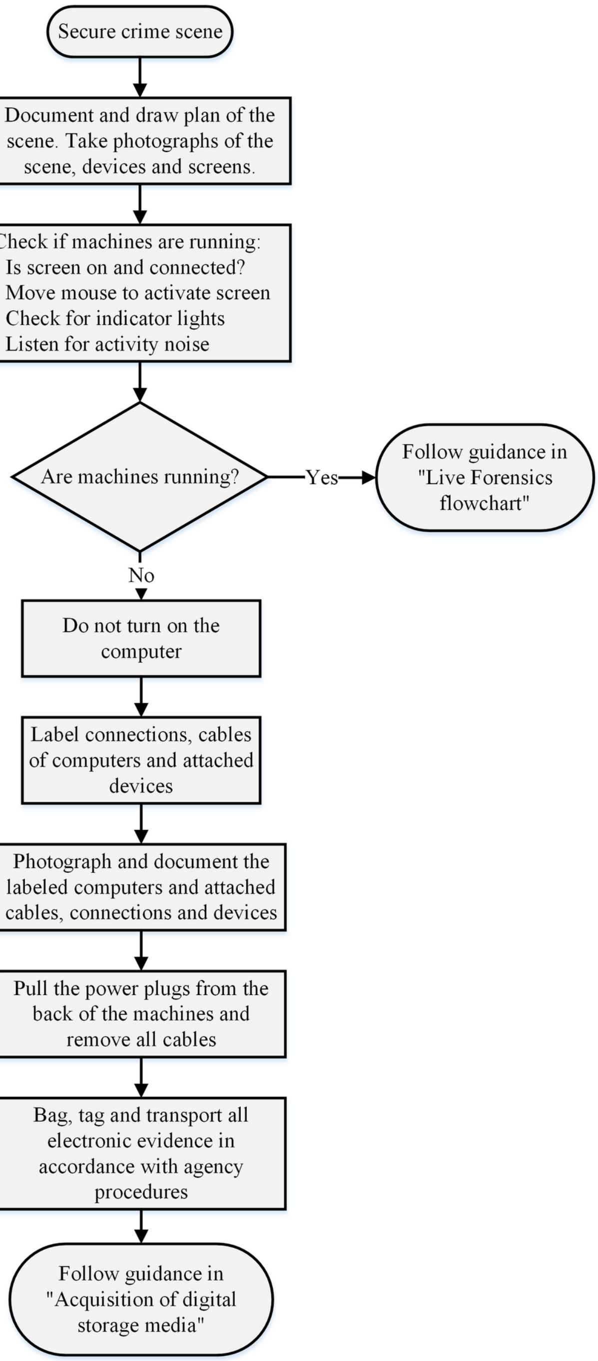
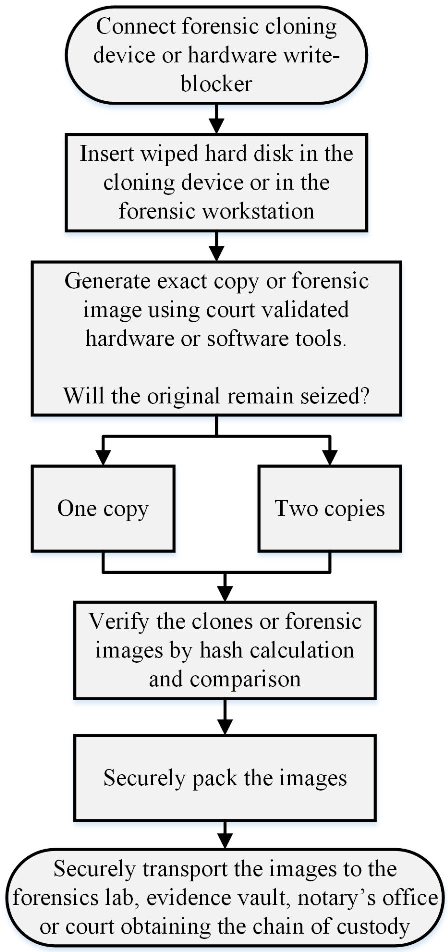


Figure 3. Acquisition of digital evidence flowchart



the dead forensic process must be very deep, which mean that the full process of acquisition requires copying all files in the disc.

According to the previously mentioned about the dead forensics it can be concluded that this process can be useful in the case of acquiring information from the hard disk. However, this type of forensic cannot be used to collect and analyze the information which is not on the hard disk. Also in today's world criminals and terrorists more often use encryption as a response to the advances in the computer forensics. The problem of encrypted files is that even the examiner has an exact copy of an encrypted file, the analysis is not possible because of seemingly random data. There are many tools for disk and file encryption that can be used, for example TrueCrypt, ArchiCrypt Live or BestCrypt. However, the encryption in not useful for the criminals if the forensic acquisition is conducted while the volume on the investigated computer is still mounted.

Shutting down the computer can cost losing other valuable data, as for example some important network data (i.e. open ports), decryption file for encrypted files, which can be stored in the volatile memory.

Positive Aspects of Dead Acquisition Analysis

Under normal circumstances, the chance of forensic investigators accidentally overwriting or modifying evidentiary data is slim. Generally, sufficient precautions are in place to ensure that the computer allows *no modification during the copying process* to either the original or the copied image of the original hard disk (Jones, 2007).

A distinguishing characteristic between dead and live forensics is that dead forensics cannot acquire live, volatile data. Once the computer is unplugged, the machine loses all the volatile memory in the RAM. However, a little known fact is that most modern *RAMs retain their contents for several seconds* after power is lost. The system does not immediately erase the volatile memory, but its content becomes less reliable when not refreshed regularly. A forensic investigator that is aware of this can therefore make use of this small window of opportunity to do a forensic acquisition (Halderman, et al., 2009).

Limitations of Dead Acquisition Analysis

There are a number of limitations and problems associated with dead acquisition analysis. Some problems are more serious than other problems, but it is necessary to look at all instances.

- In response to the efficiency of dead acquisition analysis, criminals have resorted to the widespread use of *cryptography*. Now, even though forensic examiners have a complete bit for bit hard drive image of the suspect system, it is encrypted and of no practical value. In this scenario, the drive can only be decrypted with a unique password. Since investigators cannot always rely on a suspect's cooperation in supplying this password, the method of acquisition should be adjusted – if the same encrypted disk was acquired with live forensic acquisition, investigators would be able to access the disk. This whole-disk encryption is not only limited to criminals, but is now also a default feature of some operating systems.
- Another limitation of traditional forensic acquisition has surfaced in the light of *network data*. The need for acquiring network related data (such as currently

available ports) grew dramatically. This type of information is volatile, and is lost in the event that the computer powers down - the foundation of traditional digital forensic analysis (Jones, 2007).

- To comply with traditional forensic requirements, *all data must be gathered and examined* for evidence. However, modern computers consist of gigabytes, and even terabytes, of data to be analyzed (Leigland & Krings, 2004). These complex technologies, coupled with cyber crimes becoming more advanced, lead to more complex and time-consuming digital investigations. It is increasingly difficult to use modern tools to locate vital evidence within the massive volumes of data. Log files also tend to increase in size and dimension, complicating a Cyber Forensic investigation even further (Fei, 2007).
- A *lack of standardized procedures* leads to uncertainties about the effectiveness of current investigation techniques. In turn, this has led to the suboptimal use of resources. In some instances, investigators gather worthless data that take unnecessary time. In addition, these data have to be stored and takes up valuable space (Leigland & Krings, 2004).
- Many unique *practical and legal constraints* make the application of Cyber Forensics both interesting and defiantly complex. An example of a practical constraint would be if the suspect system where a public machine in an internet café with the owner claiming a possible loss of income for the duration of the forensic investigation. An example of a legal constraint is the restriction of the methods in which forensic investigators can obtain data. This is especially relevant when practicing live forensic acquisition.
- If forensic investigators do not follow these restrictions exactly, data acquired in certain ways may be *inadmissible in court* and not allowed as intelligence (Jones, 2007). This negates the criminal investigation completely. For this reason, it is important that forensic practitioners are equipped with tools and mechanisms that can result in the acquisition of forensically sound system images. Only when this is possible, can data be seen as evidence and be admissible in a court of law.
- Dead forensics *cannot be considered as a method to acquire live, volatile data*. Although modern RAMs allows a couple of second grace period in which the volatile data is not erased, this time is often too little to do a proper acquisition.

Due to the many limitations of traditional forensics, live forensic acquisition seems a likely alternative. This allows forensic practitioners to access a variety of invaluable information that would have been lost in traditional forensic analysis (Jones, 2007). Unfortunately, the practice of live acquisition brings about its own limitations, especially with regard to legal implications. The next section addresses this acquisition mode.

Live Forensics

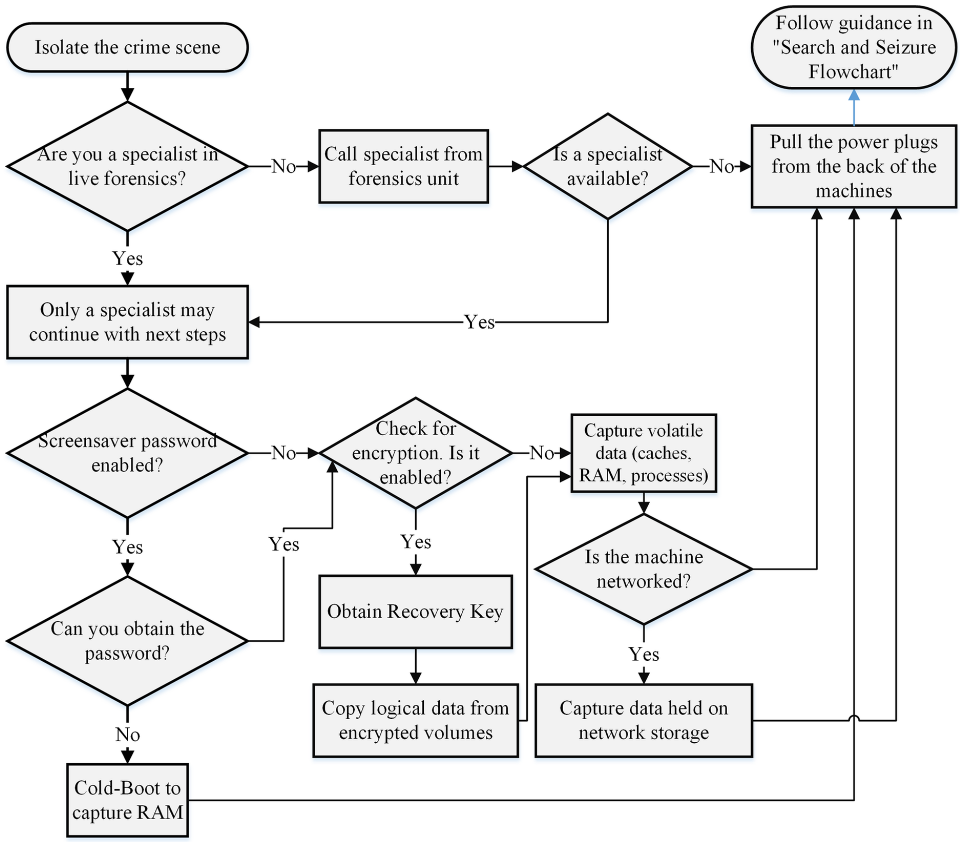
Digital forensics, as a branch of forensic, is a process of discovering and interpreting of the electronic data that would later be used in court. In fact, according to (Politt, 2004) the digital forensics is not just a process, but a group of processes used in the investigation. The purpose of these processes is to provide evidence in its most original form while performing investigation by collecting, identifying and validating the digital information in order to reconstruct some events from the past. On the other hand, the computer forensics is a branch of digital forensic pertaining to legal evidence found in computers and digital storage media.

In order to respond to the disadvantages of the dead acquisition against disk encryption and loss of the data from the volatile memory the live forensics acquisition was developed. The volatile data can be recovered and safely stored only using live forensics. This type of forensics gives chance to the analysts to collect volatile evidence in a format which can be read by the humans, instead of binary format. Live response is vital because after shutting down the computer all the information (evidence) from the volatile memory, which can be crucial during the analysis, will be lost. Actually, live response offers the ability to peer into the runtime state of the system providing valuable context for an investigation that had been historically lost with “snatch and grab methods”. Live data forensics requires a higher level of specialism than the procedures in the search and seizure of dead boxes. The live forensics process is shown in Figure 4 (Europe, 2013).

In the most of the cases the live response is conducted using response toolkits (Waits, Akinyele, Nolan, & Rogers, 2008) (Mandia, Prosise, & Pepe, 2003) (McDougal, 2007) (Moeller, 2007) (Kornblum, 2002). The easiest way for live response is by usage of automated wrapped programs. These programs are generic system administration tools that are utilized with few changes to support digital utilization. Similar information can also be collected using existing commercial agent-based systems. More advance method for live forensic response is by using of specially created scripts that run a series of command-line programs and redirect the output to a forensic workstation or peripheral media. Creating of these scripts requires advance programming knowledge, but can be very useful and can be adapted depending of the evidences which should be analyzed.

However, it must be noted that a live analysis is very sensitive, especially at risk getting false information because the software could maliciously hide or falsify data. The other problem is that the analysts might not have the appropriate level of access to the investigated system.

Figure 4. Live data forensics flowchart



Also, the attacker might have modified the system in a way that prevents detection of attacks and modifications (Mrdovic, Huseinovic, & Zajko, 2009).

It is obvious that live data forensics requires a higher level of specialism than the procedures in the search and seizure of dead boxes. As the possibility of altering or even overwriting evidence during the investigation with live data forensics is very high it is more likely to be carried out by someone who is well educated and trained, as well as experienced.

Positive Aspects of Live Acquisition Analysis

In response to the limitations of dead acquisition analysis, live acquisition analysis has surfaced as a remedy. This analysis allows forensic examiners to *retrieve volatile information* specific to the suspect system's network settings. In many instances, this information is invaluable to the prosecution of a cyber-criminal. It is thus possible to view the development of live acquisition analysis as an improvement of current methods of both dead and live acquisition (Nikkel, 2006).

In contrast with the procedural deficiency of traditional forensic acquisition, live forensic acquisition limits the amount of data gathered. Often, investigators investigate large parts of the system, but only gather the relevant pieces of information (Leigland & Krings, 2004). Live acquisition *addresses this procedural deficiency*, but it introduces a number of other problems.

Limitations of Live Acquisition Analysis

Although live acquisition addresses most of the problems associated with dead forensic acquisition, it brings about additional problems:

- *Every computer installation is different*. Although there are many common components and aspects, computer users can compile their system to their own desire. For this reason, it is the forensic examiner's job to ensure that s/he has sufficient knowledge of a wide variety of hardware, software and operating systems. It is indeed possible to come across any combination of these components, and the examiner should be prepared to handle all of these. Due to the range of possibilities provided by live forensic analysis, forensic examiners only learn the principles of live acquisition and the effect that specific actions may have on the validity of the evidence. It is further up to the interpretation of the examiner to analyze the situation, and apply the forensic principles in such a way that his/her actions can be justified in a court of law.
- *Data modification* during the acquisition process and the dependence of the forensic acquisition of the suspect system's operating system is two of the more prominent concerns regarding a live forensic acquisition. If the acquisition process alters the data, courts will dismiss the data as forensically unsound. Part of the live acquisition forensic examination process is to execute code running on the CPU of the suspect system. This can potentially change data in the CPU registers, RAM or the hard drive itself. Even if the forensic system specifies no explicit write commands, the suspect system's operating system may decide to swap the program to hard disk. This inherent operating system feature may complicate the incentive for allowing the concerned evidence in a court case and the evidence may be ruled inadmissible. In addition, inappropriate action taken by forensic examiners may ruin evidence. In the event that a forensic examiner handles a situation incorrectly, a preventable

amount of data may be changed. For example, running an application on the suspect hard drive may overwrite some of the associated properties, such as recent actions. If the specifics of this application were critical to the case, it will cause many issues in court (Jones, 2007).

- Linked to the problem of data modification, are *slurred images*. Similar to when you take a photo of a moving object, slurred images is the result of acquiring a file system while some program modifies it. The smallest modification may cause a problem, since the file system first reads the meta-data section of the hard disk. If the files or folders on the file system change after the file system have read the meta-data, but before the file system acquires the data, the meta-data and sectors do not correlate anymore (Jones, 2007). Similarly, volatile memory does not represent a single point in time, but rather a time sliding view. When acquiring volatile data, investigators cannot always use write blockers, nor is there always a MD5 comparison to the original data (Vidas, 2006).
- Another recurring problem concerning live forensic analysis, especially network evidence from untrusted networks, is *authenticity and reliability*. Anti-forensic toolkits are also widely available, and may obstruct the collection of evidence from live network sources (Perklin, 2012), (Nikkel, 2006). By applying anti-forensic measures, clued-up criminals may reduce the effectiveness of a potential forensic investigation. It is, for example, possible to write a program that destroys evidence when the operating system detects a forensic acquisition program (Jones, 2007). These types of programs are developed by individuals or organizations that want to thwart legit forensic investigations, and aims to delete all incriminating evidence on the victim computer and computer system. Some of these programs include Evidence Eliminator, The Defiler's Toolkit, Diskzapper, CryptoMite, Tracks Eraser Pro and Invisible Secrets (Defence, 2007). Another type of anti-forensic software, developed by the Metasploit Project, targets specific functionalities of legitimate forensic investigation tools. These anti-forensic wares interfere with the forensic software's results during an investigation (Hilley, 2007). Anti-forensic tools work on a variety of platforms, and perform a number of functions.
- In some instances of live forensic acquisition, *limited amounts of information are gathered*. This may not always constitute a complete representation of the original affected system, and can be interpreted as possible data corruption (Leigland & Krings, 2004). The investigation into this aspect will contribute to a comprehensive model for live acquisition.

DIGITAL FORENSICS TOOLS

It is obvious that live data forensics requires a higher level of specialism than the procedures in the search and seizure of dead boxes. As the possibility of altering or even overwriting evidence during the investigation with live data forensics is very high it is more likely to be carried out by someone who is well educated and trained, as well as experienced.

There are many available freeware and commercial tools used in computer forensics or to obtain computer data and information from computer systems. This section lists some of the most used software tools by forensics investigators.

Some of the existing tools are multifunctional, which means that they can be used for many types of investigations and analysis, whereby the others are more focused, serving a fairly limited purpose. These software tools are focused on every specific type of digital evidence, deleted files, e-mails, network traffic, etc. During the software selection, a choice needs to be made between open source tools or commercial products. Both of them have their advantages and disadvantages. Factors such as cost, functionality, capabilities, and support are some of the criteria that can be used to make this decision.

One of the more popular open source tools is SIFT, or the SANS Investigative Forensic Toolkit. SIFT Workstation is a powerful, free, open source tool. It is built on the Linux Ubuntu operating system. This tool is capable of file carving as well as analyzing file systems, web history, recycle bin, and even more. It can also analyze network traffic and volatile memory. Furthermore, the tool can be used to generate a timeline, which can be immensely helpful during the investigation process. SIFT supports almost all file systems.

The two most popular general commercial tools are Forensic Toolkit (FTK®) from Access Data and EnCase® from Guidance Software. No matter which of these tools are used by the examiner it is sure that the analysis will be easy and efficient. These forensic tools consist of many integrated capabilities, but what is more important they can be further upgraded to advance the computer forensic work. Even those most used and popular GUI-based forensic tools can perform forensics at very efficient way, they are not always the most useful solution. The reason for this is that they do not give a possibility to the examiner to understand what is going on behind the interface. Examiners need to understand not only what the tool is doing, but also how the tools are working in the background.

Previously it was mentioned that the live forensic process or obtaining a digital evidence and information from live computers. This is the complex process and depends from the case and the information that should be collected.

The main purpose why forensics experts decide to perform live data forensic are: encryption, malware, remote storage, cloud computing, etc. The digital evidences and information that could be obtained with live data forensics in general are the volatile data as the data from RAM (Random-Access Memory), system processes, and network activities. Moreover, the live data forensic tool could also analyze the dump of the disks and the images.

There are many available free tools for Live data forensics. Most of them are Linux based live CD's as Caine, Deft, Helix, Microsoft COFEE (Computer Online Forensics Evidence Extractor is a Microsoft tool for live forensic for Law Enforcement Agencies-LEA) etc. The Linux based live CD's for live forensic use the same Linux base tools and commands.

The most performed action in the live forensics is the acquisition of the RAM. There are many freely available tools and live CD's which can be used to complete this task. The following example shows how *win32dd/win64dd* can be used for making a dump of the RAM memory (Figure 5).

Figure 5. Using of win32dd/win64dd for making a dump of the RAM memory

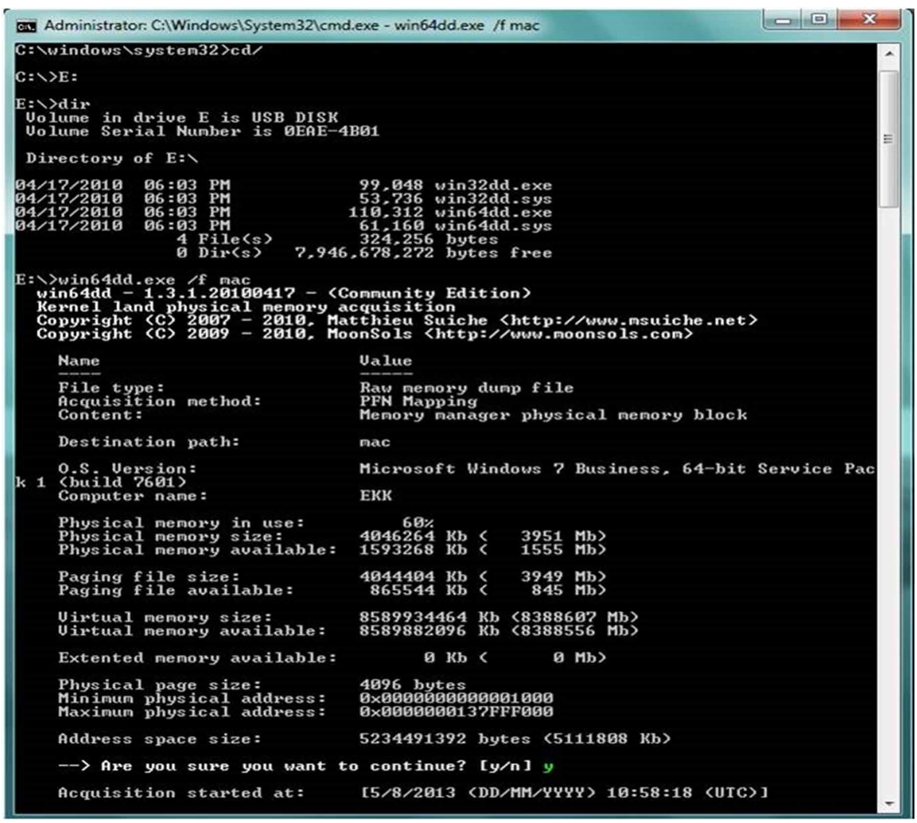
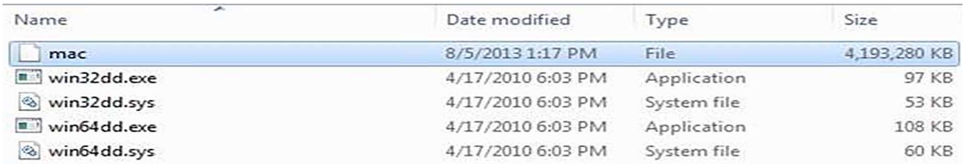


Figure 6. Created file after the process of RAM acquisition



win32dd.exe is a free kernel land tool to acquire physical memory, Executable can run as a command line tool, user prompt or from a configuration file. The Win64dd.exe can be run from a USB drive that is plugged into the target machine. The tool collects RAM and places the collected information into an .E01 file. There is a 32-bit version as well as a 64-bit version.

After the RAM acquisition a file (max 4GB) is created on the destination path that is defined when win64dd.exe from CMD (run as administrator) is executed.

Search action through this file can be executed and analysis of its complete content can be done. From the analysis, we could expect to find the encryption passwords, unsaved documents or part of the documents, internet activities, mail messages and other information.

FIRST RESPONDER SCRIPT

As we already mentioned, usage of the commercial forensics software can be more effective in the process of computer forensics and obtaining digital evidences, because they are professionally made, easy to use with a GUI and have much functionality Also the usage of the freeware well known forensic software sometimes can really improve the work of the forensic examiner, and can help in the process of collection of evidence (Stoilkovski, Bogdanoski, & Risteski, 2013). The practical inconvenient comes when the examiner need to explain how he get the information and when he should explain to the not technical person the complete process of computer forensics. The problem also comes when he need to explain the work of the used software in order to obtain the digital evidence.

Building and developing the scripts for the concrete purpose and case, for many examiners is difficult because it need a time for building and testing, but also there are many cases that make difficult to predict what scripts and software they will need. That is one of the reason why they usually use the commercial or some well know free forensic toolkit.

In this chapter, we are presenting a novel developed tool for first responders used for obtaining digital evidence on the scene. The script is bin/bash Linux based program that integrate some commands and tools from Linux.

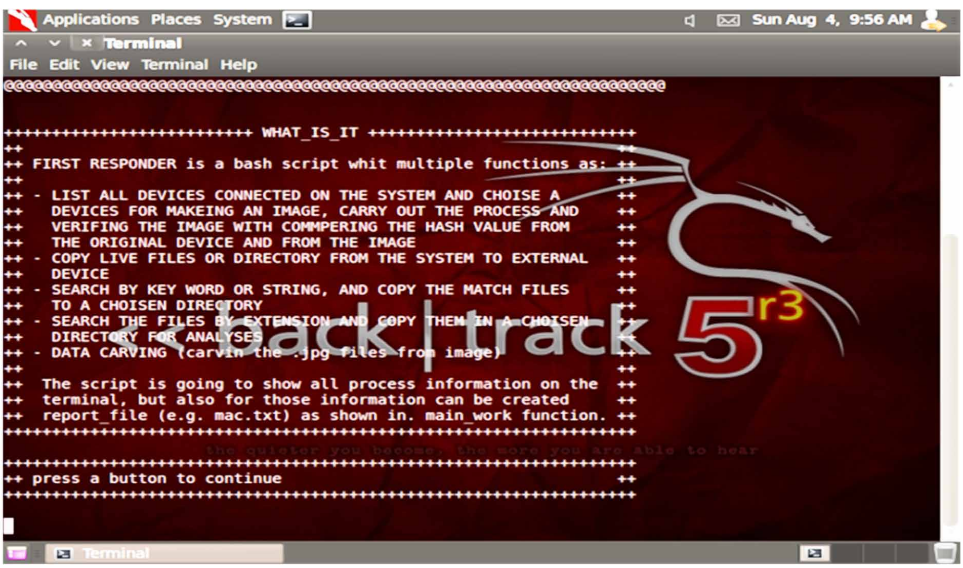
```
MAIN_WORK () {
  echo "*******************************************************"
>/tmp/mac.txt
  echo "********************** FIRST RESPONDER
********************" >>/tmp/mac.txt
  echo "*******************************************************
*****" >>/tmp/mac.txt
        echo "               REPUBLIC OF MACEDONIA          "
>>/tmp/mac.txt
        echo "                 MITKO BOGDANOVSKI            "
>>/tmp/mac.txt
        echo "                 MARJAN STOILKOVSKI
"
>>/tmp/mac.txt
        echo "                         ALEKSANDAR RISTESKI
" >>/tmp/mac.txt
        echo " " >>/tmp/mac.txt
        echo " " >>/tmp/mac.txt
        echo " "
```

The Script is menu driven multi-functional software prepared to meet the basic needs of the first responders in order to collect digital evidence and information (Figure 7).

```
echo "++++++++++++++++++++++++++ WHAT_IS_IT
++++++++++++++++++++++++++"
echo "++                                                  ++"
echo "++ FIRST RESPONDER is a bash script whit multiple
functions as:                          ++"
echo "++                                                  ++"
echo "++ - LIST ALL DEVICES CONNECTED ON THE SYSTEM AND CHOISE
A            ++"
echo "++ DEVICES FOR MAKING AN IMAGE, CARRY OUT THE PROCESS AND
++"
echo "++ VERIFING THE IMAGE WITH COMMPERING THE HASH VALUE FROM
++"
```

```
echo "++ THE ORIGINAL DEVICE AND FROM THE IMAGE          ++"
echo "++ - COPY LIVE FILES OR DIRECTORY FROM THE SYSTEM TO
EXTERNAL           ++"
echo "++ DEVICE                                             ++"
echo "++ - SEARCH BY KEY WORD OR STRING, AND COPY THE MATCH
FILES            ++"
echo "++ TO A CHOISEN DIRECTORY                             ++"
echo "++ - SEARCH THE FILES BY EXTENSION AND COPY THEM IN A
CHOISEN           ++"
echo "++ DIRECTORY FOR ANALYSES                             ++"
echo "++ - DATA CARVING (carving the .jpg files from the image)
++"
echo "++                                                   ++"
echo "++ The script is going to show all process information on
the                                  ++"
echo "++ terminal, but also for this information can be created
++"
echo "++ report_file (e.g. mac.txt) as shown in. main_work
function.                                ++"
echo
```

Figure 7. Script purpose and functionalities



The first menu allows choosing an option (see below). The users can choose to:

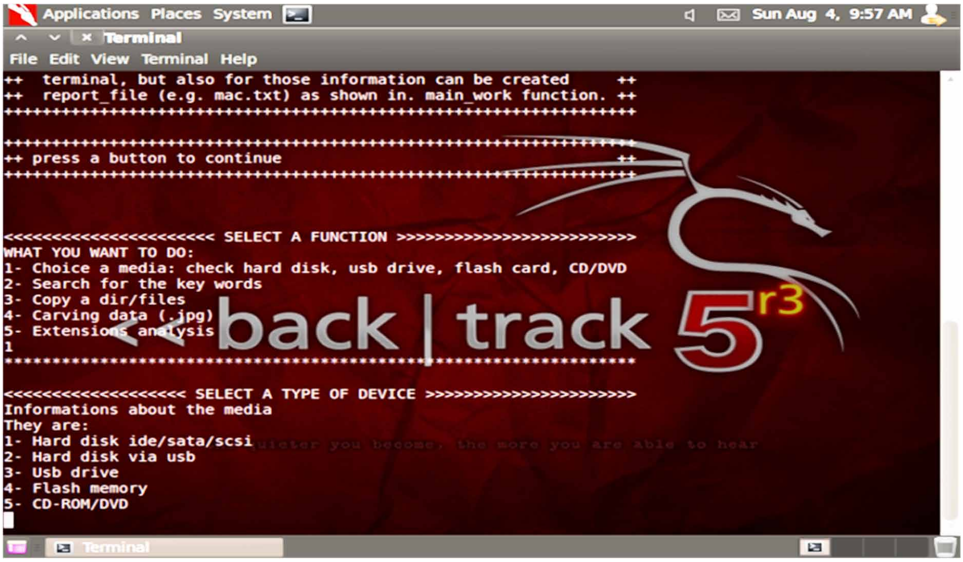
- Make an image of all attached storage devices on the system,
- Search the system for the key words or the search the image file for the key words,
- Copy files and folder for one destination on the system to another one or on remote storage,
- Make a pictures carving from the image file,
- Make an analysis of the extensions.

```
echo "WHAT YOU WANT TO DO:"
 echo "1- Choice a medium for Image: check hard disk, USB
drive, flash card, CD/DVD"
 echo "2- Search for the key words"
 echo "3- Copy a dir/files"
 echo "4- Carving data (.jpg)"
 echo "5- Extensions analysis"
```

If the first responder chooses the first option and he is planning to make an image of some attached media, the script will execute the function where will ask precise information about the type of the device for making an image (Figure 8).

```
if [ "$MACHINE" -eq 1 ]
        then
                B=0
                while [ "$B" -eq 0 ]
                do
echo "<<<<<<<<<<<SELECT A TYPE OF DEVICE >>>>>>>>>>>>>>>>>"
                echo "Information about the media"
                echo "They are: "
                echo "1- Hard disk ide/sata/scsi"
                echo "2- Hard disk via USB"
                echo "3- USB drive"
                echo "4- Flash memory"
                echo "5- CD-ROM/DVD"
                read MEDIA
                echo
```

Figure 8. Menu of the script functionalities



After identifying the type of the device for making image using *while-done* loop the script will list all the device from chosen type that are attached on the system (*df -h | grep "/dev")* and will give a choice to the first responder to choose the SOURCE and DESTINATION path for creating an image.

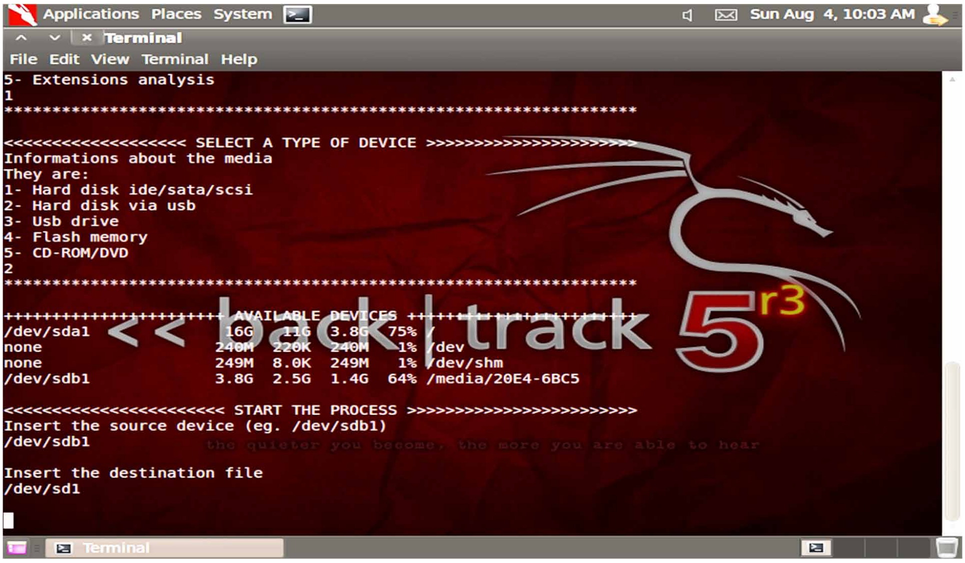
With the line dd if="$SOURCE" of="$DESTI" bs=512 the image will be created with default values of bits per sector (Figure 9). In the end the hash value of the source and destination file will be generated in order to be checked if the imaging process ended successfully and if the destination file is imaged from the source file.

```
while [ "$D" -eq 0 ] && [ $MEDIA -ne 5 ]
        do
        echo "+++++++++++++++++++ AVAILABLE DEVICES
++++++++++++++++++++++++"
        df -h | grep "/dev"
        echo " "
        echo "<<<<<<<<<<<<<<<<<<< START THE PROCESS
>>>>>>>>>>>>>>>>>>>>>>>>"
        echo "Insert the source device (e.g. /dev/sdb1)"
        read SOURCE
        echo " "
        echo "Insert the destination file"
```

```
        read DESTI
        echo ” “
        if (df -h | grep “$SOURCE” >/dev/null)
        then
                 D=1
                if (mount | grep “$SOURCE” >/dev/null)
                then
                        sudo dd if=”$SOURCE” of=”$DESTI”
bs=512
                        MD5_SOURCE=$(sudo md5sum “$SOURCE”)
                        SHA1_SOURCE=$(sudo sha1sum “$SOURCE”)
                        echo “The checksum of the original is”
                        echo “MD5 = “$MD5_SOURCE
                        echo “SHA1 = “$SHA1_SOURCE
                        MD5_DESTI=$(sudo md5sum “$DESTI”)
                        SHA1_DESTI=$(sudo sha1sum “$DESTI”)
                        echo “The checksum of the image is”
                   echo “MD5 = “$MD5_DESTI
                        echo “SHA1 = “$SHA1_DESTI
                else
                        echo “the source device is not
mounted”
                            echo $SOURCE”, is not mounted”
                        echo “mount options details:”
                        mount | grep “$SOURCE”
                        fi
        else
                echo “The source device seems to not exist”
                echo “repeat the choice”
        fi
done
```

The second option of the script is to search the system or the image file by key word. The script will allow to the first responder to define the file or destination where the search should be performed, and where results from the search to be created (by default will be Desktop). At the end of this part the first responder will have all the results (copied files) in the folder.

Figure 9. List of all attached storage devices and settings of the image creation




```
if [ "$MACHINE" -eq 2 ]
         then
         echo "Write the output directory where you save
the files (name of dir, by default will be created on the
Desktop):"
         read OUTDI
         mkdir $OUTDI
         OUTDIR=$OUTDI
         echo "This is the directory for your repository:
".$OUTDIR
         echo "Write directory contains the files where you
want to look for the keyword:"
         read INDIR
         echo "Write the keyword search:"
         read KEY
         grep -aR -i $KEY $INDIR/*.* > $OUTDIR/macsearch.txt
         FN="$(cat $OUTDIR/macsearch.txt | awk -F ":" '{print
$1}'|sed 's/*//')"
         cp $INDIR/$FN $OUTDIR 2>/dev/null
         cd $OUTDIR
         ls -l
```

```
        echo "The search is finished, all the files are in
your directory"
fi
```

The third available option in the script gives a possibility for any file or directory to be copied from one destination to another if the first responder decides to copy any file.

```
if [ "$MACHINE" -eq 3 ]
        then
        echo "Enter the source dir/file"
        read SOURCE
        ls -l $SOURCE
        echo " "
        echo " "
        echo "Enter the file or dir that you would like to
copy"
        read SOURCENAME
        echo " "
        echo " "
        df -h
        echo " "
        echo "Enter the destination dir/file"
        echo " "
        read TARGET
        [ ! -d "${TARGET}" ] && mkdir -p ${TARGET}
        echo " "
        cp /$SOURCE/$SOURCENAME $TARGET
        echo "successful copied" $SOURCENAME "to" $TARGET
        fi
```

The fourth option from the script actually is data carving. With this script the first responder could find, copy and analyze all the images (jpg) on the image file.

```
if [ "$MACHINE" -eq 4 ]
 then
        echo "Enter the path where is the image"
        read PAT
        ls $PAT
        echo " "
```

```
   echo -n "Please enter the name of the image to carve from: "
         read IMAGENAME
         STARTLINE=`xxd $IMAGENAME | grep ffd8`
         echo "Possible start of JPEG found here:"
         echo $STARTLINE
   OFFSET=`echo $STARTLINE | awk -F: '{print $1}' | tr a-f A-F`
         DECOFFSET=`echo "ibase=16;$OFFSET" | bc`
         echo -n "Please enter how many bytes from the start of
the line ffd8 appears at: "
         read BYTES
         START=`echo "$DECOFFSET+$BYTES" | bc`
         echo "Possible end of JPEG found here:"
         ENDLINE=`xxd -s $START image_carve.raw | grep ffd9`
         echo $ENDLINE
         OFFSET=`echo $ENDLINE | awk -F: '{print $1}' | tr a-f
A-F`
         DECOFFSET=`echo "ibase=16;$OFFSET" | bc`
         echo -n "Please enter how many bytes from the start of
the line ffd9 ends at: "
         read BYTES
         END=`echo "$DECOFFSET+$BYTES" | bc`
         SIZE=`echo "$END-$START" | bc`
   echo -n "Please enter the name of the JPEG file extracted: "
         read JPEGNAME
         dd if=$IMAGENAME of=$JPEGNAME skip=$START bs=1
count=$SIZE
fi
```

The fifth option in the script for the first responder is extension analyses. The user could filter all the files with the same "suspect" extension and then copy it in a particular folder for extended analyses.

```
if [ "$MACHINE" -eq 5 ]
 then
         echo "Enter the file extension"
         echo "If the needed extension is specified in the
script, live this filed blank"
         read EXTENSIONS
         echo " "
         echo "Enter the source dir/file"
```

```
        read SOURCEDIR
        ls $SOURCEDIR
        echo " "
        echo " "
        df -h | grep "/dev"
        echo " "
        echo "Enter the destination dir/file"
        read TARGETDIR
        echo " "
        #cp $(find $SOURCEDIR -type f | grep -iE
'\.($EXTENSIONS)$') $TARGETDIR
        cp $(find $SOURCEDIR -type f | grep -iE '\.(jpg|tif|bm
p|psd|pdd|gif|pdf)$') $TARGETDIR
        echo " "
        echo "the suspect files are in the TARGET directory,
for contents analyze process"
        fi
```

To complete all functionalities, a log file (mac.txt) will be created that records every step and any activity on the target computer using the script.

The developed script contains five main functions, and provides an easy to use functions allowed by the easy accessible integrated menu. This script is open to upgrade and improve with additional functionality that can contribute for more effective work of the first responders.

CONCLUSION

The aim of this chapter is to show the importance of the live computer forensics during the computer incident analysis. In order to show the importance of the live forensics the chapter firstly shows the flowchart for the live data forensics, describing all the steps which should be taken by the examiners during the analysis. Then the chapter gives an explanation of the process of RAM analysis. At the end the chapter presents the new developed First Responder script for live forensics, which is bin/bash Linux based program that integrate some commands and tools from Linux. The developed script is menu driven multi-functional software prepared to meet the basic needs of the first responders in order to collect digital evidence and information. It actually contains five main functions, and provides an easy to use functions allowed by the easy accessible integrated menu. It is an open platform which can be easily upgraded and improved with additional functionality that can contribute to more effective work of the first responders.

REFERENCES

ACPO. (2008). *ACPO Good Practice Guide for Computer-Based Evidence*. Retrieved from http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

Ademu, I.O., Imafidon, C.O., & Preston, D.S. (2011). A new approach of digital forensic model for digital forensic investigation. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 2(12), 175-178.

Ashcroft, J., Daniels, D. J., & Hart, S. V. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. U.S. Department of Justice, Office of Justice Programs.

Ayers, R., Brothers, S., & Jansen, W. (2014, May). *Guidelines on cell phone forensics.* National Institute of Standards and Technology (Special publication). Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Baryamureeba, V. (2006). The Enhanced Digital Investigation Process Model. *Asian Journal of Information Technology*, *5*, 790–794.

Beebe, N. L., & Clark, J. G. (2005). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. *Digital Investigation*, *2*(2), 147–167. doi:10.1016/j.diin.2005.04.002

Bogdanoski, M., Risteski, A., & Pejoski, S. (2012). Steganalysis—A way forward against cyber terrorism. Proceedings of the *20th Telecommunications Forum (TELFOR),* Belgrade (pp. 681-684). IEEE.

Carrier, B.A. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence,* 2(2).

Casey, E. (2010). A Chapter in Forensic Analysis. In *Handbook of Digital Forensics and Investigation*. Elsevier. doi:10.1016/B978-0-12-374267-4.00002-1

Chaudhay, M. M. (2013). *Cyber Forensics and Areas of Focus* (White Paper).

Ciardhuáin, S.Ó. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence,* 3(1).

Cohen, F. (2011). Fundamentals of digital forensic evidence. In F.B. Cohen (Ed.), Handbook of Information and Communication Security (pp. 790-808). Springer Berlin Heidelberg.

The U.S. Department of Justice. (2001). *Electronic crime scene investigation: A guide for first*.

Europe, C. o. (2013). *A basic guide for police officers, prosecutors and judges Version 1.0.* Proceedings of Joint EU/COE Project on Regional Cooperation against Cybercrime .

Fei, B. (2007). *Data Visualisation in Digital Forensics* [Thesis]. University of Pretoria. Retrieved from http://upetd.up.ac.za/thesis/submitted/etd-03072007-153241/unrestricted/dissertation.pdf

Garfinkel, S. L. (2012). *Cross-Drive Analysis with bulk_extractor and CDA tool. OSDF 2012*. Open Source Digital Forensics.

Halderman, J., Schoen, S., Heninger, N., Clarkson, W., Paul, W., Calandrino, J., ... Felten, E. (2009). Lest We Remember: Cold Boot Attacks on Encryption Keys. Proceedings of the *USENIX Security Symposium* (pp. 1-16). 10.1145/1506409.1506429

Harrison, W. (2004). The digital detective: An introduction to digital forensics. *Advances in Computers*, *60*, 75–119. doi:10.1016/S0065-2458(03)60003-3

Hilley, S. (2007). Anti-forensics with a small army of exploits. *Digital Investigation*, *4*(1), 13–15. doi:10.1016/j.diin.2007.01.005

Johnson, T. (2005). *Forensic Computer Crime Investigation*. CRC. doi:10.1201/9781420028379

Jones, R. (2007). *Safer Live Forensic Acquisition.* University of Kent at Canterbury. Retrieved from http://www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication. doi:10.6028/NIST.SP.800-86

Kohn, M., Eloff, J., & Olivier, M. (2006). Framework for a digital forensic investigation. *Proceedings of Information Security South Africa (ISSA) 2006 from Insight to Foresight Conference.*

Kornblum, J. (2002). Preservation of Fragile Digital Evidence by First Responders. *Proceedings of 2002 Digital Forensic Research Workshop (DFRWS).*

Leigland, R., & Krings, A. (2004). A Formalisation of Digital Forensics. International. *Journal of Digital Evidence*, *3*(2), 1–32.

Mandia, K., Prosise, C., & Pepe, M. (2003). Incident Response and Computer Forensics (2nd ed.). McGraw-Hill Osborne Media.

McDougal, M. (2007). Windows Forensic Toolchest. *Fool Moon Software & Security*. Retrieved from http://www.foolmoon.net/security/wft/

Moeller, J. (2007). Windows Vista Forensic Jumpstart Part I and Part II. *Proceedings of DoD Cyber Cryme Conference 2007.*

Mrdovic, S., Huseinovic, A., & Zajko, E. (2009). Combining Static and Live Digital Forensic Analysis in Virtual Environment. *Proceedings of the 22nd International Symposium on Information, Communication and Automation Technologies*. 10.1109/ICAT.2009.5348415

Nikkel, B. (2006). Improving evidence acquisition from live network sources. *Digital Investigation*, *3*(2), 89–96. doi:10.1016/j.diin.2006.05.002

Palmer, G. (2001). *A Road Map for Digital Forensic Research* [Technical Report DTR-T001-01]. Digital forensics research workshop DFRWS.

Politt, M. (2004). *Six blindmen from Indostan. Digital forensics research workshop*. DFRWS.

Reith, M. C. (2002). *An examination of digital forensic models. International Journal of Digital Evidence*, 1(3).

RIPA. (2000). *Regulation of Investigatory Powers Act 2000.* Parliament of the United Kingdom.

Roger, M.K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. *Journal of Digital Forensics, Security and Law*, 1(2), 27-40.

SecurityWizardry.com. (2007). Anti-Forensic Tools. Retrieved from http://www.networkintrusion.co.uk/foranti.htm

Stephenson, P. (2003). A comprehensive approach to digital incident investigation. *Information Security Technical Report.*

US-CERT. (2008). *Computer Forensics.* US-CERT. Retrieved from https://www.us-cert.gov/sites/default/files/publications/forensics.pdf

Valijarevic, A., & Venter, H. (2012). Harmonised digital forensic investigation process model. *Proceedings of the Annual Information Security for South Africa (ISSA, 2012) Conference.*

Vidas, T. (2006). Forensic Analysis of Volatile Data Stores. *Proceedings of CERT Conference.* Retrieved from http://www.certconf.org/presentations/2006/files/RB3.pdf

Waits, C., Akinyele, J. A., Nolan, R., & Rogers, L. (2008). *Computer Forensics: Results of Live Response Inquiry vs. Memory Image Analysis*. Carnegie Melon Software Engineering Institute.

Yong-Dal, S. (2008). New Digital Forensics Investigation Procedure Model. *Proceedings of the Fourth International Conference on Networked Computing and Advanced Information Management NCM '08* (pp. 528-531).

KEY TERMS AND DEFINITIONS

Digital Forensics: The process of uncovering and interpreting electronic data for use in a court of law.

First Responder: Refers to those individuals who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment.

Law Enforcement: The activity of making certain that the laws of an area are obeyed.

Linux: Unix-like operating system that was designed to provide personal computer users a free or very low-cost operating system comparable to traditional and usually more expensive Unix systems.

Script: A program or sequence of instructions that is interpreted or carried out by another program rather than by the computer processor (as a compiled program is).

This research was previously published in the Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare edited by Metodi Hadji-Janev and Mitko Bogdanoski; pages 352-376, copyright year 2016 by Information Science Reference (an imprint of IGI Global).

Chapter 12
Detecting Individual-Level Deception in the Digital Age:
The DETECT Model ©

Eugenie de Silva
University of Leicester, UK & Virginia Research Institute, USA

ABSTRACT

This chapter presents a discussion of a new model titled, "DETECT (Determining and Evaluating Truthfulness through Explicit Cue Testing) which relies upon the assessment of verbal and non-verbal cues. The author presents the argument that the digital age has posed novel challenges to law enforcement and intelligence personnel; hence, the author further explains the ways in which the DETECT model (©, Eugenie de Silva, 2014) can be used to determine deceptive activities at the individual-level even in a technologically advanced society. The chapter touches upon Denial and Deception (D&D), and how the detection of deception must be carried out in the twenty-first century, especially through rigorous monitoring within the established legal framework.

INTRODUCTION

It seems counterintuitive that deception could be detected, since the very act is executed to mislead others. Yet, this chapter expands upon the notion of utilizing verbal (e.g. spoken) and non-verbal (e.g. body movements) cues to detect deception to precisely explicate the extent to which deception can be detected in the twenty-first century.

DOI: 10.4018/978-1-7998-2535-7.ch012

Denial and Deception (D&D) is an all-inclusive term that commonly refers to activities that involve distorting information, manipulating facts to establish a false story, or even withholding data from an adversary. Whilst denial and deception can be utilized as two individual terms, they are undoubtedly interlinked and can be used to strengthen operations aimed at feeding false information to adversaries. In 2000, Roy Godson and James Wirtz explicitly reinstated this information by denoting that denial and deception are intertwined terms that work uniquely as a blend to essentially pull wool over the eyes of opponents or enemies (2000, 5). The denial of information results in a misinformed perception of an event, whereas deception can result in a completely distorted view of a scenario or the distortion to various degrees of specific aspects of cases. Accordingly, when used in combination, an individual can relay a completely false story to a targeted opponent to whom it would seem completely feasible and truthful. The use of realistic characteristics is what makes D&D such a dominating tool.

With regard to the disciplines of law enforcement and intelligence, deception must be identified at its earliest stages in order to avert any possible dangers aimed at damaging the national security of the U.S. This being the case, it is imperative to recognize that a successful deceptive story will commonly take advantage of the opponent's weaknesses and/or known perceptions of the world. Through the recognition of these weaknesses, an opponent may specifically tailor a deception activity to ensure that the false story is believable to his/her adversary. As a result, if one seeks to identify deception, then one should not be oblivious to the actual facts that may have been hidden or altered, based on the given set of data. Further, as history has shown, it is necessary to take into consideration all activities as they relate to other on-going operations.

Indubitably, officials who have daily interactions with individuals will encounter acts of trickery and guile. For an officer specialized in the recognition of deception, there is assuredly a higher probability of having the ability to detect duplicity at a faster rate than in cases of untrained individuals. Thus, there is a necessity to establish a model that would aid in the prediction and/or identification of deception solely by observing, and then analyzing an individual's actions or inactions, in addition to their spoken words. For the purpose of distinguishing the truth from lies without requiring an in-depth background in the field, any proposed model must not necessitate any outside or previous knowledge. Thus, the DETECT model in this chapter simply requires that individuals study the requirements of the model itself, which lessens the responsibility of having to learn an entirely new subject in order to know how to detect deception.

One scenario that explicates the necessity of a more personal approach to solving problems is the 2001 U.S. terrorist attacks. During this period, intelligence analysts in the U.S. had devoted much time to conduct research and finalize reports to determine when and where an imminent attack would take place. For those working in the Central Intelligence Agency (CIA), the identification of several suspects had already been successful. The list of these individuals had been sent to the Federal Bureau of Intelligence (FBI), yet it had not been transferred to local state troopers, and the information that had been sent were not the complete lists (de Silva, 2003, 113). As a result, although the suspected terrorist was stopped for traffic violations, he was not detained due to the troopers' lack of knowledge on the topic (de Silva, 2003, 113). This should be deemed a noteworthy instance of a failure to share information among intelligence officers and law enforcement personnel, in addition to the ways in which even advanced technology did not offer support; however, this also represents a perfect scenario in which the utilization of verbal and non-verbal cues could have been effective. Whilst the troopers were not made aware of the suspected individuals, had they been provided information about the ways to detect deception, there could have been a higher probability that they would have at least asked the individuals more pressing questions to determine the truthfulness of their statements which would have possibly led to further inquiry, recognition, and then detainment of the terrorists prior to the attacks. Although it is not certain whether the application of the DETECT model would have resulted in the definitive detainment of the terrorists prior to the attack, it is certain that offering greater opportunities to investigate and determine deception can always improve the probabilities of accurate and effective detection and handling of situations.

Unfortunately, there is no factually significant way in which to determine the most probable success rate of the troopers' utilizing verbal and non-verbal cues to either make an arrest or gather more information on the suspects. Nevertheless, based on the success of the DETECT model in prior research and in practical situations (especially the testing on "rehabilitated" terrorists), it has been herein assumed that the model would have, at the very least, provided the law enforcement officers with a more concrete basis to prevent the terrorist attacks.

Along these lines, this chapter has focused on the applicability of the DETECT model to evaluate truthfulness in the twenty-first century by taking into consideration the technologically-dependent and advanced culture of present society. The author of this chapter has sought to provide readers with a basic understanding of D&D, how it can be detected at an individual-level, and the ways in which technology may make the detection of deception an easier process, whilst simultaneously highlighting greater challenges than were previously present.

BACKGROUND

It has been reported that for average individuals and even specialists, detecting deception can be a strenuous challenge (Da Silva & Leach, 2013, 116). For instance, it has even been established that for average individuals without a background in the field the "accuracy rate [of detecting deception for laypersons] […] was 54%: 61% of truths and 47% of lies [that] were correctly identified" (Da Silva & Leach, 2013, 115). In the research, it was established that the detection of deception for specialists was only marginally higher than those without a background in the discipline. Accordingly, although it can be a struggle to recognize deception, there have been researchers who have taken the initiatives to establish and verify a list of verbal and non-verbal cues that have been explicitly linked to deceptive practices. These lists, as illustrated later in this chapter, were utilized as the exhaustive lists of cues for personnel who are interested in detecting deception in the DETECT model.

Biometrics has also been a major point of focus for other researchers in the field. According to the U.S. Federal Government's biometrics website, the term biometrics can be used to refer to either a process or a characteristic. A biometric, as a process, is defined as, "an automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics" ("Biometrics," 2006). On the other hand, a biometric, as a characteristic, is a measurable biological characteristic that may be utilized for "automated recognition" ("Biometrics," 2006). Accordingly, whereas there has been research elsewhere that specifically focuses on the study of biometrics through advanced technology, such as live-scan facial recognition systems, voice recognition, and retina recognition, the DETECT model primarily focused on the detection of deception without a reliance on such resources. These technologies can certainly be practical for officers who wish to conduct concrete analyses of individuals, yet these resources do not aid in the timely identification of deception on a daily basis for personnel without access to these systems. This leads to an important point pertaining to the usefulness of DETECT in a technologically-advanced society. Take for instance a police officer who must monitor a major highway and stop individuals who are driving over the limit, driving with faulty brake lights, failing to follow legal regulations, etc. This officer must, within a few minutes, determine whether the individual at-hand is trying to establish a deceitful story or is actually telling the truth. In such instances, it may be impractical to expect the law enforcement officer to utilize advanced technologies. The process of detecting deception should be made easier, not complicated for those who have dedicated their lives to ensure the safety of the nation. The use of social media may be useful for intelligence officers who require an understanding of the social, political, or even economic dynamics of a certain region or seek background information of a specific individual; however, law enforcement officers who work at a fast-pace in dangerous situations do not have the freedom or opportunities to take advantage of such social advancements in order to carry out their responsibilities. Thus, having an understanding of specific cues that can be used to ascertain the truthfulness of an individual's statements can make easier the responsibilities that are allocated to law enforcement personnel.

Since the 9/11 attacks of 2001, there has been a progressive shift in threats aimed at the U.S. Whereas al-Qaida and other religiously/politically motivated terrorists groups may have been at the forefront of intelligence and law enforcement analyses in 2001, one of the most prominent threats in 2013 were cyber-attacks. In fact, in 2015, the Worldwide Threat Assessment from the Office of the Director of National Intelligence (ODNI) did not even highlight Iran or Hezbollah as terrorist threats (Clapper, 2015). Therefore, it is undeniable that the threats that were previously present, no longer pose as harsh threats in the current time. In fact, a simple glance at the threat assessment proves that many of the current threats relate to cyber security, economic espionage, and other insider threats aimed at damaging the U.S. critical infrastructure. However, amidst these threats are two specific forms of terrorism that could render the U.S. virtually victim to countless domestic attacks; Homegrown Violent Extremism (HVE) and lone-wolf terrorism. For those who are radicalized within the nation, their goals are made easier by the civil rights, protections, and constitutional guarantees that are granted to those in the U.S. Accordingly, these individuals do not have to be concerned about issues that would have otherwise been raised, such as gaining security clearances and passing through border control, had they been based in another country and wanted to enter the U.S. to initiate an attack.

According to reports, HVE has essentially become the "'new face' of terrorism" (*Homegrown Violent Extremism,* n.d.). Threats of radicalization, extremism, and/or lone-wolf terrorism rise amidst political, social, and economic turmoil. When individuals feel as though they are not accepted, they commonly seek acceptance and find it in terrorist, radical, or extremist groups. The propaganda and deception used by such groups to recruit individuals, especially through the use of advanced technology and social media make it quite simple to convince individuals that their own objectives and goals can be achieved by joining the group. Disgruntled citizens who yearn to find ways to feel as though their ideologies are respected are at risk of falling victim to the D&D of the aforementioned groups. These individuals align their activities with the groups (which further criminal activities) in the process of trying to improve their own situations.

U.S. law enforcement personnel at the local, state, and federal levels are explicitly accountable for protecting the nation from these individuals who have been radicalized. Of course, the utilization of the intelligence cycle to gather, analyze, and then disseminate reports can be a useful tool; yet, it does not always foster the necessary protection to predict, and then prevent such attacks. In addition, placing high reliance on technology is a less personal/human means of handling intelligence issues, which may not always allow the government to attain their intelligence goals. In 2015, these issues are particularly pressing, due to the ways in which social media has provided terrorist organizations with the opportunity to recruit and radicalize individuals to carry out actions from within the U.S.; in fact, Islamic State of Iraq and Syria (ISIS) is one terrorist group that has significantly taken advantage of these resources to further its agenda.

For years, the topic of detecting deception has been investigated by researchers who have developed academic reports on the ways in which interviewing strategies can be improved to increase the likelihood of distinguishing the truth from the lies. Whereas other topics have been diligently researched for years, the detection of deception through verbal and non-verbal cues has not been at the forefront of recent discussions in the fields of political science and law enforcement. As was previously mentioned, the recognition of deceit is a necessary and useful tactic for law enforcement personnel who must work with individuals on a daily basis.

Verbal and non-verbal cues have been analyzed in the field as early as 1987, yet a common weakness of the research has been the lack of rigorous testing of the effectiveness of the utilization of the cues as a means of recognizing deception. In addition, there has been a failure to identify the applicability and usefulness of both cues in law enforcement and intelligence environments. Accordingly, in 2013, the author of this chapter conducted a rigorous research project wherein individuals were interviewed and tested to detect their truthfulness based on the author's novel model "DETECT." This model was based on several verbal and non-verbal cues that had been carefully identified through an extensive review of existing literature. There are many verbal and non-verbal cues that can be used to detect deception as has been highlighted through research over the years. Moreover, since there are cues that are specific to individuals of certain genders, each of the cues have been listed below with either M to indicate that it is predominately noticed in males, F to indicate that it is commonly recognized in females, or M/F to highlight that it is commonly noticed in both males and females. The cues that are listed below form the basis of the DETECT model:

Verbal Cues:

1. Speech Stumbles (M/F) = Use of filler words (e.g. "umm" or "uhh") sign of deception.
2. Including long pauses before answering (M/F) = High probability of deception
3. Evading answering the question (M/F) = High probability of deception
4. Beginning answers with the word "well" (M/F) = Major sign of deception

5. Utilizing negative statements (M/F) – Use of words, such as "no," "do not," or "cannot" are signs of deception.
6. Using higher tone and pitch of voice (M/F) – Associated with deception

Nonverbal Cues:

1. Maintaining steady eye contact (M/F) = Habitual liars believe looking away will lead the interviewer to suspect they are lying.
2. Rubbing nose (M/F) = Stress causes an increase of blood to the extremities which causes tingling in the nose; hence, individuals rub their nose when they feel discomfort.
3. Crossing/Folding arms (M/F) = A barrier in communication.
4. Touching/Placing hand on suprasternal notch or the base of throat (F) = Researcher Joe Navarro recognized women do this when they are stressed (2012).
5. Using item to cover themselves (e.g. jacket, cup, paper) (M/F) = Barrier in communication
6. Holding hands together or clasping hands (M/F) = Barrier in communication
7. Positioning feet at the closest exit (M/F) = Represents where an individual actually wants to be at the time.
8. Using hand gestures that do not explicitly match what is being stated (M/F) = Liars must juggle conflicting information to present a believable story; hence, hand gestures are not in synch with their statements.
9. Not using hand gestures (M/F) = Focus is on establishing a truthful story, so the individual forgets to use hand gestures as they would in general situations.
10. Fanning themselves with their hands or other items (M/F) = Stress causes individuals to feel hot, which forces them to fan themselves to cool down.
11. Pupil dilation increasing (M/F) = Sign of deception
12. More blinking (M/F) – Researcher note this as a sign of deception
13. Moving fingers – Identified later in research as being a common movement
14. Crossing legs – Sign of barrier in communication

In an effort to establish a general outline of basic qualifiers of deception, John L. Waltman and Golen published "Detecting Deception during Interviews" in 1993, which pertained to the identification of deception during interviews when auditing. Waltman and Golen were both faculty members at Eastern Michigan University ("EMU Faculty Publications," 2001). The combination of their expertise and backgrounds in the field substantially aided in the establishment of a body of work focused on leakage and the common non-verbal behavioral patterns or body movements of liars. Moving forward, the work provided assessments that determined that many advanced liars have learned to control their faces; hence, the author discussed the importance of assessing situations through the analysis of other areas of an individual's body (Waltman & Golen, 1993, 61.) Furthermore, the authors also brought their work to an end by identifying that the behavioral norms of individuals vary from person-to-person (Waltman & Golen, 1993, 63.) Based on this information, the importance of identifying the norm of an individual prior to judging their actions and assessing for deception was confirmed.

The data offered by these authors acted as the guiding factors in the development of "DETECT." Although the articles may not have been written in relation to the technological advances of the twenty-first century, they establish the underlying basis that is necessary to understand deception activities. Along these lines, it was also necessary to take into consideration that by being objective and not generalizing each individual, one can improve the chances of successful detection of deception. Complete reliance on current technology would thus require one to generalize most individuals; this would further exacerbate issues in detecting deception.

In 2000, Barton Whaley and Jeffrey Busby developed "Detecting Deception: Practice, Practitioners, and Theory," which provided readers with an introduction to deception, a description of the practitioners of deception, and how deception can be detected. Whaley and Busby's work significantly contributed to the field by making known that although experts are the individuals who commonly have more success in detecting deception due to the organized manner in which they approach situations, non-experts could also be deemed detectives since every individual applies skills of detection to identify deception on a daily basis (2000, 73).

Along these lines, the author of this chapter reflected upon the notion of how technological advancement plays a role in the extent to which members of the public feel that they are apt and adequately prepared to counter deceptive ploys, and detect any propaganda if it were being aimed at them. These beliefs are typically what make deception campaigns successful, since unrealistic beliefs that one can easily detect deception, and ill-informed views of deception and propaganda allow one to be more easily swayed.

As more research was conducted, it was found that in 2007, Kevin Colwell published an article known as "Assessment Criteria Indicative of Deception (ACID): an integrated system of investigative interviewing and detecting deception." Colwell's background as a professor of psychology specialized in detecting deception clearly aided in the development of a foundation for the work ("Kevin Colwell," 2014). Consequent to providing a brief overview of the extent to which content analyses have been conducted to determine patterns in deceptive statements during interviews, Colwell further explicated that interviewing strategies that can increase the cognitive load of the individuals being interviewed can improve the effort to detect deception (2007, 168).

This also leads back to the issue of the public view of D&D. What is portrayed in the media (e.g. news, television, movies, dramas, etc.) is certainly not always the most credible or accurate information. However, if one takes into consideration the extent to which most individuals rely on the media for their information, without conducting outside, academic research, then it becomes possible to realize the ways in which the public makes D&D campaigns easier. With the knowledge that experts and practitioners hold with regard to D&D campaigns, and the lack of understanding by a majority of the public, influencing views to attain tactical and strategic success can be a simple process. For instance, it is understood that by increasing the cognitive load of individuals, the detection of deception is made easier, since the individual must make an effort to manage more cognitive processes; thus, whilst an individual is forced to increase their cognitive load, the lack of knowledge on how their ideologies could be manipulated sets the path for the interrogator/researcher/practitioner to easily detect the common signs of deception. The increase in cognitive load ensures that an individual is unable to maintain deceptive stories in ways that would have otherwise been possible. In the cyber arena, this increase in cognitive load is difficult to carry out; yet, it can be possible through extensive online discussions that require the subject at-hand to become emotionally or psychologically involved in the discussion(s). Detecting individual-level deception is made easier on a face-to-face basis, especially through the application of the DETECT model, which allows practitioners to assess based on verbal and physical cues; however, it is also certainly possible to detect deception through cyber systems by gaining essential background information, and tactically questioning an individual to gather information.

Moving forward, in 2012, an FBI article written by Joe Navarro was published. It was titled, "Detecting Deception." Navarro briefly touched upon the necessity of law enforcement officials to have an adequate understanding of human behavior, since it would provide more opportunities to gather data and conduct assessments (2012). Subsequently, he pondered on several non-verbal characteristics that were known to be associated with deception (Navarro, 2012). However, Navarro also spoke about the importance of having an adequate setting to conduct an interview of an individual to determine deception (2012). This is a point that was taken into consideration through the research to establish the DETECT model; the model was designed to have the flexibility to be tailored according to the needs of individual officers. Technology can be used to detect deception as has been proven through other research; however, without generalizing all individuals or understanding human behavior, technology itself cannot be the sole or primary identifier of deception. The individuals who program the technology may understand human behavior, yet if the technology is not appropriately programmed or fine-tuned, then the technology simply becomes an assistive maneuver, rather than a primary technique in the detection of deception. This is the reason why this chapter promotes the use of the

DETECT model to make the initial determinations of deception at an individual-level. Technology can be used in combination with the model, yet it is not required.

Furthermore, Walter Weintraub's 2005 work "Verbal Behavior and Personality Assessment" explicated that if verbal trait analyses are to be conducted, the speech samples must be collected from speech under conditions that are only moderately stressful (2005, 140). He also explained that if the verbal samples were collected from scenarios in which the stress levels were too high or too low, any analyses of the data would not be rendered useful or applicable (Weintraub, 2005, 140). Further, Weintraub did include information about grammatical commonalities and the utilization of verbal patterns to recognize personality norms for individuals. Weintraub explicitly focused on the grammatical ways in which sentences are structured; yet, the DETECT model relies on previously identified specific verbal cues on which to focus. Thus, the main point that has been derived from Weintraub's work was the necessity of focusing on spontaneous material that was presented by the individuals being interviewed.

Later in 2011, Maria Hartwig, Par A. Granhag, Leif Stromwall, Ann G. Wolf, Aldert Vrij, and Emma Roos Hjelmsater published an article titled "Detecting deception in suspects: verbal cues as a function of interview strategy" which was dedicated to the utilization of verbal cues as a way of detecting deception. By conducting observations of ninety-six undergraduates, Hartwig, et. al. were able to highlight the veracity of the extent to which verbal cues could be used to recognize deceptive practices (2011, 654). The study concluded by also stating that many innocent suspects believed that "telling the truth is sufficient for exoneration" whereas officials mainly require corroborating evidence to determine an individual's innocence (Hartwig, et. al., 2011, 645). Furthermore, it was also made clear that the accuracy rate was not as high as predicted when the basis was the verbal cues; accordingly, the authors hinted to the possibility that the examination of non-verbal cues may have provided greater insight. This acted as further impetus in the development of the DETECT model.

On another note, the work of Lara Warmelink, Aldert, Vrij, Samantha Mann, and Par Anders Granhag from 2013 titled "Spatial and Temporal Details in Intentions: A Cue to Detecting Deception" was able to emphasize that individuals have a tendency to provide a wealth of detail in describing their intentions, whereas details were minimized when one was not discussing their intentions (Warmelink, Vrij, Mann, Granhag, 2013, 105). For the purposes of Warmelink, et. al.'s work, it was hypothesized, and then verified that the individuals tested in their research offered significantly more detail in their answers to questions when being truthful about their intentions, whilst less details were provided when the individuals were lying (Warmelink, et. al., 105).

With the aforementioned research taken into consideration, in 2011, David Matsumoto, Hyi Sung Hwang, Lisa Skinner, and Mark Frank published an article in the Federal Bureau of Investigation (FBI) bulletin entitled, "Evaluating Truthfulness and Detecting Deception." The article relayed the ideas that law enforcement should recognize that there is not one standard, nor perfect technique or model to detect deception; however, the authors did mention that through systematic awareness of non-verbal cues, individuals could more easily recognize deception (Matsumoto, Hwang, Skinner, and Frank, 2011). For example, the authors made clear that many law enforcement officers commonly focus on what an individual is saying, rather than also being aware of how the individual is saying the information (Matsumoto, et. al., 2011). However, the work relayed the notion that the officers should not just focus on non-verbal characteristics, but should also try to multitask and take into consideration both cues, while assessing how they are working in coordination with one another (Matsumoto, et. al., 2011). Accordingly, the work was useful to highlight the actual importance of the DETECT model; the model is not to be applied as a perfect model that will provide continuous, accurate results. Rather, the model provides practitioners with greater opportunities to detect deception, which further makes the probability of successfully detecting deception much higher.

MAIN FOCUS OF THE CHAPTER

DETECT Model: Application

The application of the DETECT model was simplified during inception in order to ensure that law enforcement and intelligence officers would not be required to undergo intense training. To successfully apply the model, the practitioner (the individual applying the model) must be aware of the verbal and non-verbal cues. Since most practitioners will not be able to mentally remember each of the cues, the tables below may be used to provide the practitioners with easier ways in which to

Figure 1. Verbal Cue Checklist Outline

Date	Time	Name	Cue 1: Speech Stumble	Cue 2: Long Pauses Prior to Answering	Cue 3: Answers Begin w/ "Well."	Cue 4: Negative Statements	Cue 5: Higher Tone and Pitch of Voice	Cue 6: Evading Answering	Total Cues Out of 6

Figure 2. Non-Verbal Cue Checklist Outline – Part 1

Date	Time	Name	Cue 1: Steady Eye Contact	Cue 2: Rubbing Nose	Cue 3: Crossing Arms	Cue 4: Touching Suprasternal Notch/Base of Throat	Cue 5: Using Item to Cover Themselves	Cue 6: Holding Hands Together / Clasping Hands	Total Cues Out of 6:

Figure 3. Non-Verbal Cue Checklist Outline – Part 2

Date	Time	Name	Cue 1: Positioning Feet at Closest Exit	Cue 2: Hand Gestures Do Not Match Statements	Cue 3: Not Using Hand Gestures	Cue 4: Fanning Themselves w/ Hands or Other Items	Cue 5: Pupil Dilation Increasing	Cue 6: More Blinking	Total Cues Out of 6:

Figure 4. Non-Verbal Cue Checklist Outline – Part 3

Date	Time	Name	Cue 1: Crossing Legs	Cue 2: Moving Fingers	Total Cues Out of 2:

Figure 5. Final Cue Evaluation

Date	Time	Name	1. Number of Verbal Cues	2. Number of Non-Verbal Cues	3. 3 or More Verbal Cues Detected? YES/NO	4. 7 or More Non-Verbal Cues Detected? YES/NO	If You Entered "YES" in Boxes 3 or 4, Enter Check Mark in This Box. 50% or More Signs of Either Cues Equals High Probability of Deception. Seek Further Investigation.

note any identified cues. Due to the fact that there are more non-verbal cues than verbal cues, the non-verbal cue table may be broken into three separate components, and then totaled in the final "Cue Evaluation" table (see Figures 1-5).

As can be determined from the above tables, the application of the model is quite simple. Once the practitioners become comfortable with the system, the time it takes to enter the information into the tables will lessen. The DETECT model was developed through non-parametric, statistical analyses that further relied on the McNemar Test. Furthermore, the evaluation of participants in the initial Institutional Review Board (IRB) approved investigations for the development of the model resulted in the determination that if an individual displayed fifty-percent or more of either of the cues (e.g. 3 out of 6 verbal cues or 7 out of 14 non-verbal cues), then that individual was more likely to be deceiving the practitioner.

Issues, Controversies, and Problems

The U.S., in 2015, is faced with the challenges that arise due to the evolving times, such as increased cyber threats, homegrown violent extremism, insider threats in intelligence agencies, etc. Therefore, those who are involved in security sectors are presented with the challenges of identifying appropriate strategies to counter the threats, while also maintaining the standards of the institution according to the relevant legal regulations. The extensive reliance on cyber infrastructure further exacerbates the threats by allowing criminals to carry out activities that would not have been possible without advanced technology. Although this poses a wide array of challenges to intelligence and law enforcement personnel, it particularly makes the detection of deception less feasible. The DETECT model focuses on face-to-face interaction that provides individuals with opportunities to assess verbal and non-verbal cues; the application of this model in the cyber arena would ultimately rely on written words, which would ultimately require an expansion of the model to train practitioners with regard to understanding how grammar, punctuation, and other written characteristics can be used to first gain an understanding of an individual's personality, and then begin to detect deception.

Deception strategies vary depending on the area of the world in which they are executed. To date, investigations and analyses into the subject have resulted in the determination that "[t]errorist sympathizers will probably conduct low-level cyber-attacks on behalf of terrorist groups and attract attention of the media, which might exaggerate the capabilities and threat posed by these actors" (Clapper, 2015, p.2). As aforementioned, HVE and lone-wolf terrorism are growing threats. In fact, HVE related to ISIS and the fight to carry out the objectives of ISIS by traveling to Syria and/or conducting illegal activities in the U.S. have clearly been major threats to U.S. homeland security (Clapper, 2015, p.5). Although the monitoring of social media will be vital in the determination of whether individuals are being radicalized, it will be important to find ways for law enforcement at all levels to be integrated in a manner that will be conducive to the maintenance of national security. Therefore, social media not only poses issues pertaining the radicalization in individuals, but it also creates a barrier when law enforcement or intelligence personnel want to investigate the verbal and non-verbal cues.

Another issue with which practitioners of detecting deception are faced is the cooperation between the public and law enforcement. The Edward Snowden case resulted in much uproar amongst U.S. citizens, and individuals across the globe; although law enforcement and intelligence personnel could have used the situation as a basis of reform to regain the public's trust, more issues arose after this time. In particular, in recent months, law enforcement have been involved in the shooting and killing of many unarmed citizens. These killings have led to protests pertaining to tactics employed by law enforcement and the motives behind the shootings. Therefore, individuals may hide their true intentions or purposefully react in irregular ways when questioned by law enforcement personnel. This could lead to incorrect determinations based on the assessment of verbal or non-verbal cues.

Solutions and Recommendations

Overall, the application of the DETECT model allows practitioners to detect deception at early stages without having to gather much background data in order to make an initial determination. With regard to the issue of terrorist activities and terrorist sympathizers, the management of these threats may include the application of the DETECT model. Law enforcement personnel at all levels (e.g. local, state, and federal), whilst carrying out their allocated responsibilities, should maintain awareness of common signs of deception. Thus, law enforcement should go beyond what is required of them in order to ensure that they do not allow an individual with malicious intentions to slip through their grip without notice. This also relates back to the mistakes made prior to 9/11 by the law enforcement officer who did not appropriately investigate the terrorist who had been stopped while driving.

Along these lines, through social media, it can be difficult for law enforcement to determine whether or not an individual is being deceitful through verbal/non-verbal cues. The ways in which individuals type may not be the ways in which the individuals verbally speak. Therefore, it will always be more useful to take advantage of the advancements in social media through voice and video chat. Take for instance the popular social networking site Facebook, which allows users to use their webcams and microphones to speak, rather than solely relying on the messenger feature within the site. In cases wherein there are reasonable suspicions of criminal activity, law enforcement/intelligence personnel may befriend an individual through a fake profile, and then initiate contact with the individual in question. The process may take time, since the officer must gain the trust of the individual in question; however, once a appropriate time has passed, the use of Facebook's webcam and microphone chat features will be useful for the officer to hear how the individual speaks, and the ways in which they carry themselves during a conversation. Once the officer has an understanding of the individual's behavior, questions could be asked through the features or the individual could be called in for questioning wherein the DETECT model could be further applied. In addition, other resources, such as Skype, ooVoo, WhatsApp, KiK, etc., could similarly be used to apply the DETECT model without requiring physical interviews with an individual; although, the latter will always be more useful in detecting deception based on verbal and non-verbal cues.

With regard to the issue of public frustration and distrust of law enforcement and intelligence personnel, the main solution will be public outreach and education. If law enforcement and intelligence personnel place a priority on establishing a more open relationship with the public, it may be possible to regain trust. This will not be a fast solution, yet it will promote a cooperative relationship conducive to the detection of deception whenever necessary. Furthermore, if individuals act irrationally or in irregular ways when confronted by law enforcement personnel, then it will, as aforementioned, be difficult to clearly assess verbal or non-verbal cues. However, it will be more useful to incorrectly assume that an individual is being deceitful an initiate further investigations, rather than incorrectly assume that an individual is being truthful and allow the individual to freely leave. Law enforcement personnel, however, should realize that assuming an individual is being deceitful based on the DETECT model does not mean that the individual is guilty of a crime, and also does not provide the law enforcement with the right to freely use excessive force. The results of the DETECT model simply provide law enforcement with a basis to initiate further investigations.

The following are also strategies that should be taken into consideration in order to more appropriately detect deception, and improve the way in which security officials conduct activities:

1. **When Conducting In-Depth Interviews, Follow the Common Practices and Tactics Enlisted in Cognitive Interviews (CI):** When officials interview eyewitnesses and victims of crimes, CIs are commonly utilized to ensure that the individuals being interviewed have improved opportunities to explain themselves and provide more complete and real explanations of information. In the case of detecting deception, the common practices of this form of interviewing should be used. Firstly, officers should instruct the individuals to "think-aloud" during the interview. During this form of interviewing, law enforcement and intelligence personnel should "read each question to the

subject, and then record and/or otherwise note the processes that subject uses in arriving at an answer to the question" (Willis, 1999, 1). Accordingly, the interviewer should also ask the interviewee what they are thinking whenever they take long pauses (Willis, 1999, 1). Another strategy of CI that could be applied is known as verbal probing; here, the officer "asks the survey question [does not have to be a survey question in the case of detecting deception], and the subject answers, the interviewer then asks for other, specific information relevant to the question, or to the specific answer given" (Willis, 1999, 5). It is important to recognize that for the purposes of detecting deception, the specific details of the CI method are not entirely applicable. However, the two above-mentioned techniques will particularly allow the personnel interviewing subjects more time to identify whether the subjects are showing any of the noted verbal or non-verbal cues. **NOTE:** This may not apply to daily discussions of law enforcement/intelligence personnel who must conduct brief interviews with individuals.

2. **When Analyzing Individual Responses, Do Not Over-Analyze and/or Allow Personal Beliefs or Biases to Skew Judgment:** It is important to quickly identify the cues without spending too much time on whether or not there is a possibility that the individual is lying or telling the truth and in-turn more closely trying to purposefully identify specific cues to fulfill a biased agenda. This also expands to scenarios in which officers must interrogate several individuals with regard to the same case. Consequent to interviewing several individuals, it is apparent that there will be components of the stories that corroborate and complement one another. Nevertheless, in order for the model to work effectively, it will be important that the individuals are analyzed objectively. It may be possible for the interviewers to identify common patterns, yet the model should not be used to fulfill biased opinions with regard to patterns in individuals' stories. Therefore, the model should be applied without biases; otherwise, it will merely become a tool that can be used to substantiate and validate subjective claims.
3. **Taking Notes is Not Mandatory, But Can Be Conducive to Appropriate Detection of Deception:** There are fourteen non-verbal cues, whereas there are only six verbal cues; therefore, it may be possible to remember the six cues and mentally observe the individuals being interviewed. However, to remember each of the fourteen cues would require at least general training, yet even in these cases it may be difficult for officials to take into consideration the cues whilst also ensuring that they are asking the most appropriate questions and gaining all information that is necessary under the specific circumstances. Therefore, the use of a worksheet that would list out the cues would provide the officials with an opportunity to speak to the individuals, and then check

any cues that are noticed without having to remember the cues at the time. This is the reason why the verbal and non-verbal cue tables were incorporated in this chapter.

FUTURE RESEARCH DIRECTIONS

Officials who plan to utilize the model should take the three aforementioned suggestions into consideration. Accordingly, if this model is to be used in professional settings it may be more appropriate to establish a training course that would prepare officials to use the model on a timely basis. As is the case with any novel implementation, individuals may have difficulties in becoming comfortable with the new techniques; thus, it is of the utmost importance that the individuals are able to effectively use the model prior to applying it in the field. A training course to direct the officers on how to use the model would not require months, or many weeks. Rather the training could be broken down into four major components and taught throughout a six-week process. Each of the weeks would require devotion to the learning of the model, yet it would not overwhelm the officers by taking too much time out of their daily lives.

- **1st Week:** Officers are provided with worksheets and readings that allow them to immerse themselves in the understanding of what is deception, common deceptive practices, and how the model itself works. This week will be the introductory phase that would establish a basis for officers to understand what is expected in detecting deception. This week would be representative of a "flipped classroom" whereby students are provided materials to read and/or watch, and then attend the classes to discuss what has been learnt. The officers should feel comfortable to openly discuss the material, explain any challenges in understanding the materials, and actively engage in discussions with fellow officers to ensure that every individual in the course has progressed at the same pace.
- **2nd Week:** This week should be devoted to allowing the officers to watch videos of individuals who are telling the truth and/or lying. When the analyses for this research were conducted, the entire process was new, since no training had been undergone prior to the beginning of the project. Whilst the results have proven that the model can be used by those without training, the six-week course would be useful for those officers who wish to further learn about the processes that are involved in detecting deception. Accordingly, this week would be the prime time for officers to become accustomed to watching brief interviews with individuals and identify the non-verbal and verbal cues.

The instructors in this course, especially during this week, should allow the officers to learn their most comfortable strategies to identify the cues and note them down. For instance, when the research was conducted for this work, the verbal and non-verbal cues were listed on two separate excel sheets. As the cues were recognized, a check mark was entered into the graph, which ultimately allowed for further analyses.

- **3rd Week:** By the end of week 2, the officers should be well aware of the discipline of detecting deception and should feel more comfortable in watching interviews and recognizing the cues. Therefore, this week should be devoted to allowing the officers to conduct interviews amongst themselves within the regulations of their divisions, while also noting the cues exemplified by the interviewees. They should also be made aware, if not already, of the CI method. The officers should recognize the extent to which the model can be applied and how they can personalize their own interviewing styles to incorporate the use of the model. This week should allow the officers to experiment with the model.
- **4th Week:** Based on the results of the previous research to develop the DETECT model, there was a lack of cultural variety in the selected participants. Since each of the participants were born and raised in and around the same areas in Eastern Tennessee (e.g. Tazewell, TN, Claiborne, TN, & Harrogate, TN), there was a lack of context to establish the possible differences that may have arisen had there been a broader range of individuals with a wider variety of backgrounds. Thus, for those who have chosen to take the course, this training week would be extremely useful to allow the officials to interview individuals and determine the different ways in which certain individuals answer questions based on their background. Overall, this week would be a continuation of the practices for week 3.
- **5th Week:** This week should be a review week for the officers to once again gather around and take part in lively discussions. Furthermore, these discussions would allow the officers to discuss patterns or strategies that they have developed over the course of the past weeks. The instructors should facilitate detailed discussions to determine whether or not the individuals seem to have a strong understanding of what has been taught and what is required in the use of the model. The instructor should ask general questions and ask all the participants to discuss their answers with one another. The individuals should also be asked to complete minimum one-page essays wherein they must prove their knowledge of the model and the background of detecting deception.
- **6th Week:** The fifth week is essentially the week of the course in which the instructor determines whether or not the participants have an adequate

understanding of the model and the discipline. This week the instructor must return the graded papers with either a P for pass or an F for fail. The participants will be allowed to engage in group detection of deception activities in which they will be once again allowed to practice their skills. However, in this case, the officers will be working in groups, rather than on their own. This week will ultimately act as a cumulative review of all information that has been taught over the course of the six weeks.

CONCLUSION

In its entirety, the DETECT model is an effective resource for law enforcement and intelligence personnel to detect individual-level deception without reliance on advanced technology. The model is flexible and can be applied in a wide range of situations without requiring the practitioner to physically be in the presence of an individual. This is particularly useful in a society wherein a majority of activities revolve around technology and social media. Thus, the DETECT model can be applied on a face-to-face basis (which the author suggests is the most effective strategy), yet can also be executed through social media and online networking sites.

Furthermore, due to the issues pertaining to the trust amongst the public and law enforcement and intelligence personnel, there will be greater hurdles in appropriately applying the DETECT model. If the public purposefully act in irregular manners, due to their angst over the ways in which law enforcement and intelligence matters have been handled in recent times, then the DETECT model may result in incorrect results. However, prior research on the DETECT model only proved one case wherein an incorrect determination was made; in that case, the individual was being truthful, yet the model assessed that the individual was being deceitful. Therefore, it is herein argued that the DETECT model will still be useful in cases of odd behavior by individuals, since it will be safer to incorrectly assume that an individual is being deceitful and investigate further, rather incorrectly assume that an individual is being truthful and allow him/her to flee without further questioning.

Deception is not that which laymen can easily detect with high accuracy without training in the discipline. Accordingly, the DETECT model itself was designed for law enforcement officials, such as police officers, and intelligence personnel who must conduct individual-level interviews to determine deception. Further investigation could lead to the determination that this model would be particularly useful for the Transportation Security Administration (TSA), since these professionals encounter countless individuals on a daily basis, and they must, at times, ask questions that only require one-word answers. Through the use of DETECT, the officers would most probably have higher probability rates of detecting deception and further securing U.S.

borders at the domestic and international levels. The future of detecting deception will rely on the research that is conducted today, in the twenty-first century. There will be no major improvements that can aid in the safeguarding of intelligence systems and the upholding of the national security of the country if there is no impetus to focus on this research topic and place a priority on improving the ways in which government officials can determine if an individual is being deceptive. If a government official cannot detect deception, then the risk of falling victim to D&D, and then compromising the security of the country is raised. As more of these officials fail to recognize deceit, the overall safety standards of the country will begin to waver. Therefore, the research work that has been presented here adds to the existing body of knowledge by providing a novel avenue whereby law enforcement officers and intelligence officers may detect deception on a timely basis. Of course, there may be instances in which the model cannot be applied; yet, in a majority of the instances, the utilization of the model is plausible. Thus, the work has added a novel facet to be further explored and investigated by researchers in the field who have an avid, yet unbiased interest in the determination of the overall effectiveness of the model in a wide array of circumstances.

Finally, it is paramount to note that as technology advances, law enforcement and intelligence personnel may feel more enthusiastically about utilizing novel technological devises to detect deception, rather than relying upon models that require traditional methods of writing and examining data. However, the responsibility of law enforcement and intelligence officers is to aid in the efforts to protect the nation domestically and internationally; therefore, the most useful model should be utilized, not the one that has gained the most publicity or acknowledgment from the media. The pure goal of detecting deception for government officials is to predict, and then prevent any deceptive practices that may cause harm to the country or those living within the nation. In its entirety, DETECT is a model that has been tested through non-parametric statistical analyses and has proven to be acceptable and extremely useful in the successful identification of deception in a majority of individual-level interviews. Accordingly, it is hoped that this branch of research will become more widely known and an emphasis will be placed on the testing of this model scenarios different to those tested in previous research. Accordingly, as this research has come to a conclusion, it is imperative to note that DETECT may have a perfect place within the fields of intelligence and law enforcement; thus, the development and completion of this research is a call to fellow researchers to take an initiative to test, examine, and report about this model and aid in the improvement of this model to provide officers with an effective means of detecting deception.

REFERENCES

Biometrics.gov. (n.d.). *Biometrics*. Retrieved from http://www.biometrics.gov/mediaroom/fastfacts.aspx

Clapper, J. R. (2015). *Worldwide Threat Assessment of the US Intelligence Community*. Retrieved from http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

Colwell, K., Hiscock-Anisman, C. K., Memon, A., Taylor, L., & Prewett, J. (2007). Assessment Criteria Indicative of Deception (ACID): An integrated system of investigative interviewing and detecting deception. *Journal of Investigative Psychology and Offender Profiling*, *4*(3), 167–180. doi:10.1002/jip.73

Da Silva, C. S., & Leach, A. M. (2013). Detecting Deception in Second-Language Speakers. *Legal and Criminological Psychology*, *18*(1), 115–127. doi:10.1111/j.2044-8333.2011.02030.x

de Silva, E. (2003). Intelligence and Policy in Combating Terrorism. In R. Gunaratna (Ed.), *Terrorism in the Asia-Pacific. Threat and Response* (pp. 108–133). Singapore: Eastern Universities Press.

Eastern Michigan University. (2001). *EMU Faculty Publications*. Retrieved http://www.emich.edu/library/notablecollection/facpub/publist.php?department=Management%20and%20Law&page=10

Godson, R., & Wirtz, J. J. (2000). Strategic Denial and Deception. *Trends in Organized Crime*, *6*(6), 5–16. doi:10.100712117-000-1002-2

Google Scholar. (2014). *Kevin Colwell*. Retrieved from http://scholar.google.com/citations?user=HWwtbD8AAAAJ&hl=en

Hartwig, M., Granhag, P. A., Stromwall, L., Wolf, A. G., Vrij, A., & Roos Hjelmsater, E. (2011). Detecting Deception in Suspects: Verbal Cues as a Function of Interview Strategy. *Psychology, Crime & Law*, *17*(7), 643–656. doi:10.1080/10683160903446982

Matsumoto, D., Hwang, H. S., Skinner, L., and Frank, M. (2011). Evaluating Truthfulness and Detecting Deception. *FBI Law Enforcement Bulletin*, (80), 1-8.

Navarro, J. (2012). Detecting Deception. *FBI Law Enforcement Bulletin*, (81), 7-11.

Waltman, J. L. & Golen, S. P. (1993). Detecting Deception During Interviews. *Internal Auditor*, 50, 61-63.

Warmelink, L., Vrij, A., Mann, S., & Granhag, P. A. (2013). Spatial and Temporal Details in Intentions: A Cue to Detecting Deception. *Applied Cognitive Psychology*, *27*(1), 101–106. doi:10.1002/acp.2878

Weintraub, W. (2005). Verbal Behavior and Personality Assessment. In J. M. Post (Ed.), *Psychological Assessment of Political Leaders: With Profiles of Saddam Hussein and Bill Clinton* (pp. 215–271). Michigan: University of Michigan Press.

Whaley, B., & Busby, J. (2000). Detecting Deception: Practice, Practitioners, and Theory. *Trends in Organized Crime*, *6*(6), 73–104. doi:10.100712117-000-1007-x

Willis, G. B. (1999). *Cognitive Interviewing: A "How To" Guide*. Retrieved from http://www.uiowa.edu/~c07b209/interview.pdf

KEY TERMS AND DEFINITIONS

Cybersecurity: The strategies and measures that are taken to ensure the protection of computer systems.

Deception: The effort to ensure that an individual believes a false story that will ultimately result in a reaction that serves the benefit of the practitioner.

Denial and Deception (D&D): The blend of denial and deception to achieve one's own objectives; this can be separated into A-Type deception (causing ambiguity) and M-Type deception (misleading an adversary).

Denial: Blocking information to ensure that an individual cannot access the truth about a situation; thus, resulting in the individual's inability to appropriately react.

DETECT Model (©, Eugenie de Silva, 2014): This model is based on verbal and non-verbal cues to aid in the timely detection of deception at the individual-level. It was first designed and tested for law enforcement and intelligence personnel by Eugenie de Silva in 2014.

Intelligence Community (IC) (U.S.): The syndication of seventeen organizations and agencies that work in the U.S. to gather information and disseminate intelligence to aid in the maintenance of national security.

Non-Verbal Cues: Physical movements or non-movements exemplified by an individual.

Verbal Cues: The words or noises actually spoken or made by an individual.

This research was previously published in National Security and Counterintelligence in the Era of Cyber Espionage edited by Eugenie de Silva; pages 259-276, copyright year 2016 by Information Science Reference (an imprint of IGI Global).

Chapter 13
Sentiment Analysis of Tweets for Estimating Criticality and Security of Events

V. Subramaniyaswamy
SASTRA University, India

R. Logesh
SASTRA University, India

M. Abejith
SASTRA University, India

Sunil Umasankar
SASTRA University, India

A. Umamakeswari
SASTRA University, India

ABSTRACT

Social Media has become one of the major industries in the world. It has been noted that almost three fourth of the world's population use social media. This has instigated many researches towards social media. One such useful application is the sentimental analysis of real time social media data for security purposes. The insights that are generated can be used by law enforcement agencies and for intelligence purposes. There are many types of analyses that have been done for security purposes. Here, the authors propose a comprehensive software application which will meticulously scrape data from Twitter and analyse them using the lexicon based analysis to look for possible threats. They propose a methodology to obtain a quantitative result called criticality to assess the level of threat for a public event. The results can be used to understand people's opinions and comments with regard to specific events.

DOI: 10.4018/978-1-7998-2535-7.ch013

The proposed system combines this lexicon based sentimental analysis along with deep data collection and segregates the emotions into different levels to analyse the threat for an event.

1. INTRODUCTION

Social media websites are growing at a very fast rate throughout the world. The increase in the reach of the Internet to more people every day is also helping this. It is turning out to be one of the major industries in the world and is revolutionising several existing industries such as print media and marketing. Organisations are also benefitting from this advancement as they can now enhance their processes such as understanding customer's opinions, analysing reviews and feedbacks. However, with the increased availability of people's data online, there is an increasing concern for people's privacy and security. The advancement in social media access and increased available features has also started attracting potential hackers. This makes it possible for several crimes to occur such as selling private information, usage of such social sites to do secret transactions that are banned. Due to the massive size of the data available online, sometimes activities and potential threats can also go undetected. This motivated the development of Application Programming Interface that is freely available for people to use to create software that can track these crimes online. But owing to user's privacy these tools have limits to the amount of data that they can get. There are trackers inside these tools that ban people automatically the people that try to over use it. There are many undergoing projects in many universities that endlessly utilize everything they have to build an efficient product that helps law enforcement agencies to detect crimes in a better way.

In this work we focus on applying sentimental analysis to Twitter data to obtain tweets that can possibly lead to disruptions during an event. To use the Internet and obtain Intelligence, monitoring important sites is necessary. Useful data can be obtained for law enforcement purposes from social networking sites that can be processed for obtaining insights, detecting threats, making predictions and performing many other analyses. Such analyses will provide private organizations, authorities and law enforcement agencies to make decisions and obtain a better understanding of their people. Most analyses, including this analysis use the data that are publicly visible on the web. Users always have the option to choose their data to be publicly or privately visible. The trust and privacy gets breached when an organisation or analysis uses data that is wrongfully obtained. The proposed system is a data collection and text mining application for Intelligence and Law enforcement agencies.

A three step method is proposed for obtaining useful insights and the steps are as follows:

- Obtaining data from Social media sites like Twitter in the form of raw data and tweets by identifying important keywords and locations that are of interest, such as specific public events or places. The data is obtained by crawling periodically and using the APIs provided by these sites such as search and streaming APIs;
- A lexicon based on SentiWordNet was generated to obtain sentiment values for words;
- On the collected real time data in the knowledge base, lexicon based sentimental analysis is done to calculate the emotional sentimental value for every entity. Sentiment values are first calculated for individual words using their values in the lexicon and the sentiment for the entire sentence is obtained by evidence based combination function and sentiment normalisation as described by Jurek et al. (2015).

The tweets that are found to be negative are further analysed to measure their intensity and how they may influence the selected public event. By measuring the number of people who have negative opinion tweets about the event against the total number of people who tweeted about the event, we provide 3 levels of possible threat or disorder for the event that is about to take place. Thus, the relationship between the number of people who tweet with a negative sentiment about an event and the actual disruption or disorder that happens during an event can be obtained. Summarization of the steps is as follows:

- To collect and monitor real time data, using deep data collection by identifying public events or places of interest;
- To perform lexicon based sentimental analysis on the collected data to determine emotional values;
- To classify the obtained emotional values into possible levels of disorder that will happen during the event.

The reminder of the manuscript is organized as follows: The next section describes the existing related work of the literature. The section 3 explains the existing work in depth and section 4 depicts the proposed methodology along with the novel algorithms. Later in the section 5, the proposed method is evaluated for its performance in the real-time scenario. Finally, the article concludes with the summary of results and presents future work guidelines.

2. RELATED WORK

Social media is evolving fast as an important tool that finds usage in many ways in the domain of security and law enforcement. Organizations and agencies are increasingly turning to social media for the purposes of verification, investigations and for several other data required for security and safety measures. According to survey by LexisNexis® Risk Solutions, 73% of people in that survey, believe that social media can help solve cases more quickly and 78% expect to use it even more in the future. Sentimental analysis can be used effectively in the field of security, especially with the power of social media. Sentimental analysis is generally used in many different areas such as marketing, sales, customer feedback and retrieval of opinions from the web etc. But the application of sentimental analysis for the purpose of security analysis is relatively new. Some related work in the field of security and sentimental analysis are described below. It can be effectively used to analyse various problems in security such as the protection required for a particular public event, detecting emotional crimes etc [Jurek et al. (2015)]. There are many approached to sentimental analysis. They are generally classified into the following categories:

- Knowledge-based methods
- Statistical methods
- Hybrid approaches

Knowledge based methods rely on words for classifying the data into corresponding polarity and may use semantic networks and ontologies, while statistical methods employ techniques such as machine learning. Hybrid approaches try to combine both the techniques to perform analysis. Statistical models depending on machine learning can prove costly mainly due to their requirement of high quality training data sets. They need to be trained with data that is labelled manually, say a set of tweets and their manually labelled emotions. Obtaining labelled data sets of high accuracy in large amounts is difficult. But in methods such as lexicon based sentimental analysis, dictionaries of words are used to calculate the overall sentiment of sentences by finding the intensities of sentiments of words from lexicons. Generating a lexicon is easier than generating a labelled set of Twitter corpus.

In 2012, Glass and Colbaugh has proposed detection of cyber incidents in near real-time, emerging topics and trends, and early warning analysis for mobilization and protest events [Glass and Colbaugh (2012)]. Large collections of Dutch tweets were tested on a method proposed Spitters et al. (2014) using trigger keywords and contextual cues to automatically ranks messages based on their threat potential. Analysis of micro blog posts using a violence detection model (VDM) involving a word prior knowledge to detect violence related words was proposed by Basave et al. (2013). Such a VDM model does not require any labelled data set for training. In 2011, Colbaugh and Glass has presented a Lexicon-based sentiment analysis was illustrated by estimating regional public opinion regarding the Egyptian revolution and hotel bombing in Jakarta [Colbaugh and Glass (2011)]. A similar work was performed to analyse the relationship between sentiment about Palestinian suicide bombing attacks against Israel and the bombing event [Colbaugh and Glass (2013)]. Analysis was also done on the public sentiment about H1N1 vaccination. In Jurek et al. (2014), authors illustrate a case study examining the relation between sentiment of Twitter posts related to English Defence League and the level of disorder during the EDL related events.

Moreover, lexicon based sentimental analysis allows for easier application of the methods in another language by the simple translation of the lexicon used, into the required language. Taboada et al. (2011) propose Semantic Orientation CALculator (SO-CAL) which uses Lexicon based sentimental analysis that uses dictionaries of words along with their semantic orientations. They used Mechanical Turk to ensure consistency in their dictionaries. Ngoc and Yoo (2014) tried to calculate the rank of Facebook fan pages based on analysis on comments and user engagement by applying lexicon based sentimental analysis. They used a content based ranking that considered comment polarity and user engagement. Some works have also been done in other languages such as Arabic, Chinese. Avanco and Das Gracas Volpe Nunes (2014) have analysed product reviews from the web written in Brazilian Portuguese using the lexicon based algorithm and Abdulla et al. (2013) used both corpus based and lexicon based methods for analysis of Arabic data from the web. These are good examples for the possibility of applying the method in other languages.

3. EXISTING METHOD

From the existing literature, Jurek et al. (2015) have suggested an improved lexicon based sentimental algorithm that provides a scale of measurement, rather than just classifying text such as tweets as positive/negative. The authors proposed an improved lexicon based sentimental analysis that uses sentiment normalization and evidence based combination methods to provide such a scale of measurement. Esuli and Sebastiani (2006) used a sentiment lexicon based on SentiWordNet containing about 6300 words with their corresponding values in the range of -100 to 100. In order to determine if the sense of a word is either positive or negative, they used labelled data and conditional probability. Go et al. (2009) used the data set provided by Stanford that contains 1.6 million (800,000 positive and 800,000 negative) labelled tweets. They also proposed ways to handle negation, intensity of words with more efficiency than commonly used methods. A sentiment combining function was used with the sentiment of single words, to calculate the normalised sentiment of the message (range of −100 to 100).

Positive and negative evidence values (e_p and e_n), using an evidence function were calculated for the words and separately combined. After obtaining the combined sentiment and evidence values (F_p,F_n, E_p, E_n), they used a final Sentiment function. If it is seen to contain only positive or only negative valued words then the final value is calculated based on F_p and E_p or F_n and E_n only. But, more analysis is done if the sentence consists of both positive and negative words. If so, then the entity is determined as positive or negative, based on which words are stronger (either positive or negative). The difference between positive and negative evidence (E_p-E_n) is calculated. If this difference is found to be greater than 0.1, then positive sentiment is given. If the difference value gets below -0.1 then negative sentiment is given. Again if the difference value is found to be between these values or in case there is no evidence value available, then the decision is made based on the difference in the positive and negative sentiments. Whichever value is greater, will be the final value. The authors have also presented variations of their algorithm as L, LN, LNS, LNW, LNWS and made detailed analysis on how they perform in different scenarios.

L denotes the general lexicon based technique that includes negation and intensification. It just sums sentiment values of all positive and negative words within the given sentence and classifies them as positive, negative or neutral according to the resulting value. LN performs in the similar to L, but it uses sentiment normalisation to obtain F_p, F_n for the sentence. LNS performs LN for every sentence in a particular text or message and calculates the overall sentiment of a sentence as an average of the values obtained for all sentences within it. LNW performs as LN but in case of mixed sentiment within a message it applies the evidence-based function to classify the message as positive or negative. LNWS performs LNW for each sentence within a message. A process using F_p, F_n, E_p, E_n as described by Jurek et al. (2015) is used to classify. The final sentiment is calculated as an average of the values obtained for all the sentences. They also described that LNW performs better for short text such as tweets and LNWS is more optimal for longer messages.

The authors did a case study on the English defence league (EDL) demonstrations to analyse the relationship between negative sentiments of messages related to the events posted on Twitter and the amount of disorder during the demonstrations. They measured the negative sentiments of tweets related to four event of EDL for 6 days before every event through the RepKnight platform. They found that the Birmingham demonstration which is one of the four events obtained the highest attention of Twitter's users comparing to the other events and had most negative tweets. The results indicated that the negative sentiment of an event can be applied as an indicator to a certain extent, for the level of disorder. It could be used by law enforcement agencies as an aid to plan the deployment of resources and personnel for public events such as demonstrations. Such measurements calculated in the end will provide more benefits than simple classification of data as positive/negative, since they represent the intensity of sentiments of the person's online tweet. It can be used for many interesting applications especially in the domain of security.

3.1. Quantitative Measure

This proposed research work focuses on providing a quantitative result for the threat level of a public event by analysing the event's tweets online. By providing a criticality value for an event, agencies such as law enforcement can perform evaluations of it. With only the classification of tweets as positive / negative or finding the sentimental value of the tweets as explained in several research works above, it is difficult to estimate the severity of the event's threats in the form of users' negative emotions. Hence we try to overcome this gap by providing a criticality value that will make use of levels of threats and provide a value. That value represents the negativity of the particular event and can be used to make security decisions on conducting public events.

4. METHODOLOGY

We used a three step process to use real time data from Twitter to generate results in the form of threat levels. The architecture is shown in Figure 1. The sentiments

Figure 1. Architecture of the proposed system

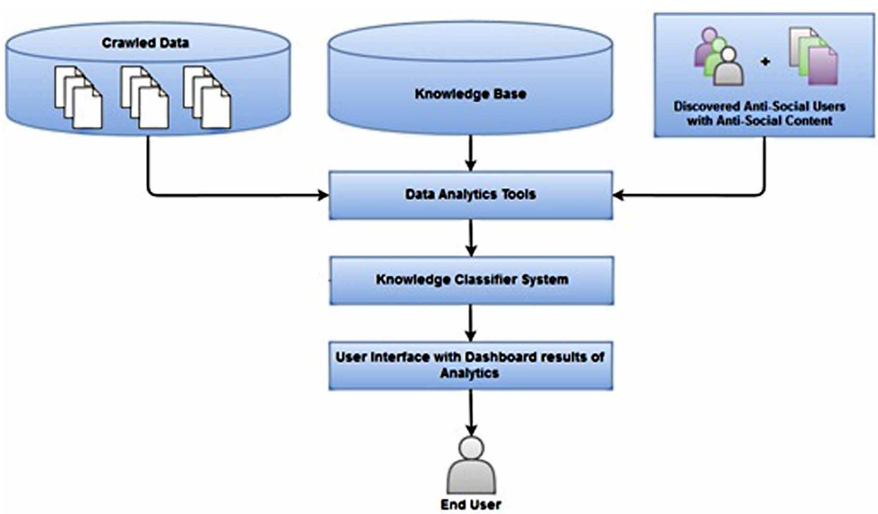
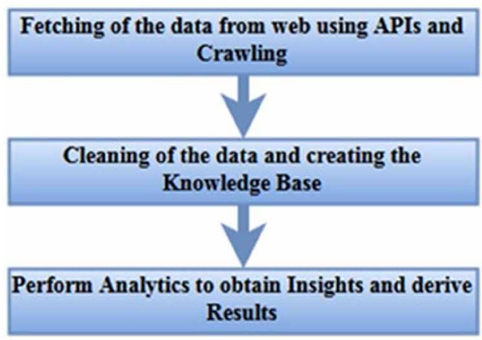


Figure 2. The process flow of the proposed system



of people who tweet in particular regions or regarding particular events can be visualized over a period of time and be watched for abnormality when they cross thresholds, as explained further. Such insights will be of use for law enforcement agencies and for intelligence purposes. As shown in Figure 2, we developed a three module system that detects possible threats. Text mining is done using deep data collection from social media such as Twitter by using parameters generated by the second module. Analysis is performed using lexicon based sentimental analysis and the results are classified based on threshold values to determine threat levels.

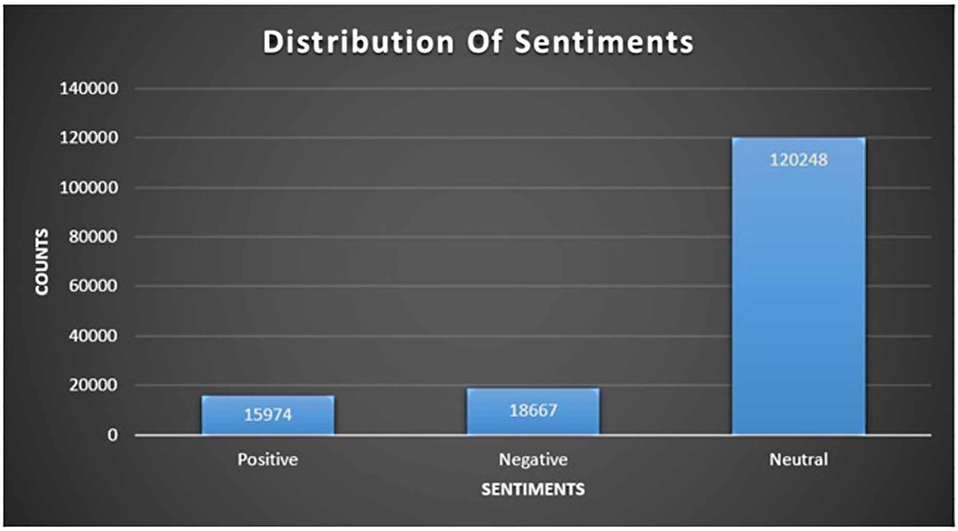
4.1. Building the Lexicon

The most important part of this proposed work was the building of a lexicon that can accurately help the software to detect possible problems in the future. The paper proposed a manual way of building a corpus for detecting emotions. But this could be time consuming and an impossible thing for the law enforcement agencies, since they have to allocate man power in detecting threats not spend time on making it accurate.

4.2. SentiWordNet

So we use an automated corpus that is ready for use. For this we made use of the SentiWordNet data set that contains a list of words with their synonyms along with their positive, negative and objective scores. This corpus was mined efficiently for getting all the unique words from it. This was first listed in a text file for further processing. Later we get the word's positive and negative values and scale them to a value between -100 to 100 just like the proposed idea by Jurek et al. (2015). Now the corpus contains about 150,000 words with their positive and negative values.

Figure 3. Distribution of sentiments in the lexicon used



Since words with zero values indicate neutral sentiment, they were removed from the corpus. This reduced the words count to approximately 33,000. The distribution of the sentiments of the words used is shown in Figure 3.

4.3. Calculation of Probability

A word can be either positive or negative depending on its nature in a sentence. But this cannot be predicted beforehand. So we took the Stanford training data set used in Go et al. (2009) that contains about 1.6 million tweets with labels as positive or negative. So technically it contains about 800,000 positive and 800,000 negative tweets. These tweets were previously classified into positive and negative tweets based on the emoticons present in them. This training data is used by many organisations for analytics of sentiments and also as an actual training data for many text analysis purposes. We used this training data to accurately determine the positive and negative probability of the words that our corpus has. These values help in increasing the accuracy of the results.

Calculating the probability of a particular word to be either positive or negative and the probability formula is:

$$P(\text{Positive} \mid w) = \frac{W_P}{W_T}$$

$$P(\text{Negative} \mid w) = \frac{W_N}{W_T}$$

For a word 'w':

W_P – number of times the word 'w' occur in positive tweets.
W_N – number of times the word 'w' occur in negative tweets.
$W_T = (W_P + W_N)$ – Total number of occurrences.

Finally, we got a corpus of lexicons with their positive and negative values along with their positive and negative probabilities.

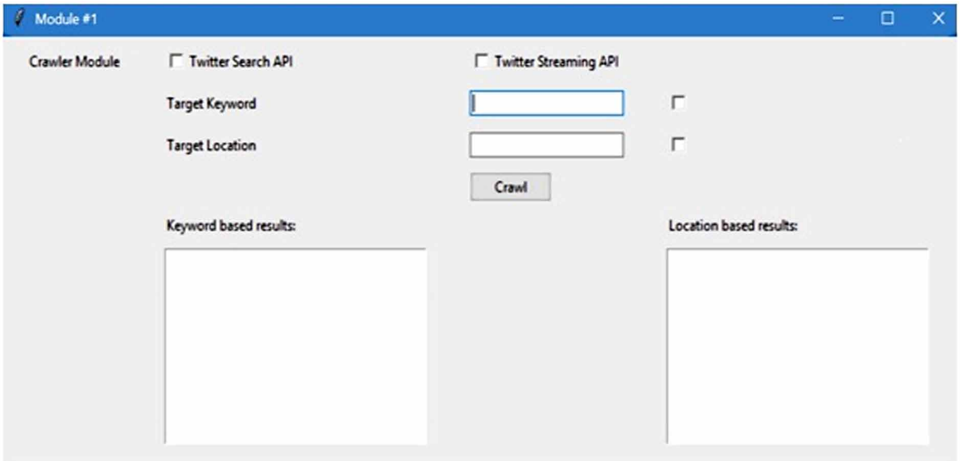
4.4. Fetching Twitter Data

This module fetches data from Twitter using Python and requires an Internet connection to fetch data from its sources. It makes use of Twitter Streaming API embedded in tweepy to fetch tweets on a real time basis. The module generates logs for the fetching that it does along with errors, if any. It also takes keywords as input which will be useful in cases where a particular keyword is to be focused. For example, an upcoming event can be monitored based on the input of keyword to fetch data. The module fetches data continuously and stores them in MongoDB for further processes such as cleaning and analysis. It also has the option of fetching and storing tweets using Twitter search API, which fetches previously completed tweets based on keywords or location.

4.5. The Interface and Storage of Tweets

An easy to understand user interface was implemented that lets us select where we want to get the tweets from. For the same event we can generate tweets from location as well as from the hash-tag or any mention of the event in tweets. This helps us collect tweets with better accuracy and store them for further processing. The MongoDB collects tweets with their id, screen name, tweet text and location as the cleaned knowledge from the unprocessed Twitter tweets data. This pre-processing is done by PyMongo API for Python. Thus, we collected tweets from specific sources using python tweepy API and stored them in MongoDB after cleaning by using PyMongo. The accessibility is given to the law enforcement agencies in the form of a simple and easy to understand user interface (shown in Figure 4).

Figure 4. User Interface of proposed sentiment analysis software application



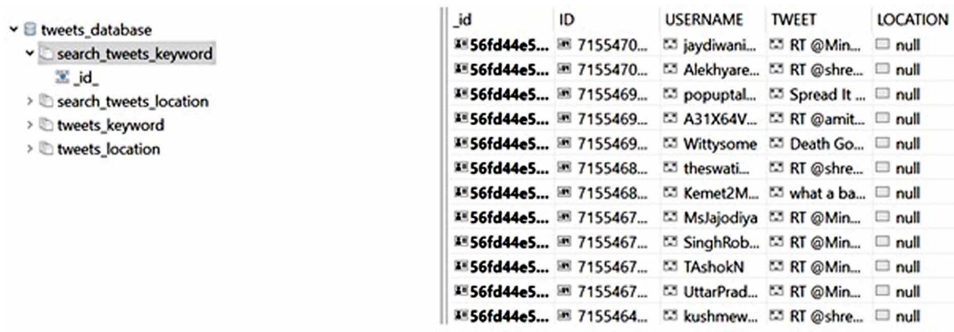
4.6. Analytics

The second step as shown in Figure 5, of our proposed work, takes the collected clean Twitter data from MongoDB and processes the text to find the emotional value of each person tweeting about the particular event we are focussing on. Firstly, we take only the tweet text from MongoDB to process. The tweet taken at a particular time goes through a list of processes before assigning it an emotional value. The tweet is separated into a list of words for lexicon based sentimental analysis. Figure 5 shows the stored tweets from Twitter in MongoDB. For this to work, we first generated a corpus of 33,000 words with their positive and negative values and the probability of occurrence of these values, as mentioned already. These values are scaled values generated from the SentiWordNet corpus available for free online for anyone who would like to work on lexicon analysis. This SentiWordNet corpus contains about 150,000 words with their synonyms, positive, negative and objective values. We planned to take just the positive and negative values and scaled it to reflect a number between -100 to 100. These are the positive and negative emotional value of each word.

4.7. Calculating Values for Fetched Tweets

Having assigned these values to words in our lexicon corpus we generate emotional values to tweets in our own MongoDB. We first assign values to each word in the tweet by referring the automated dictionary. Based on the probability of occurrence of each word in the tweet we either give it a positive or negative value. Other than these values there are words that intensify or negate a particular word. For example,

Figure 5. Tweets fetched from Twitter and stored in MongoDB as documents



_id	ID	USERNAME	TWEET	LOCATION
56fd44e5...	7155470...	jaydiwani...	RT @Min...	null
56fd44e5...	7155470...	Alekhyare...	RT @shre...	null
56fd44e5...	7155469...	popuptal...	Spread It ...	null
56fd44e5...	7155469...	A31X64V...	RT @amit...	null
56fd44e5...	7155469...	Wittysome	Death Go...	null
56fd44e5...	7155468...	theswati...	RT @shre...	null
56fd44e5...	7155468...	Kemet2M...	what a ba...	null
56fd44e5...	7155467...	MsJajodiya	RT @Min...	null
56fd44e5...	7155467...	SinghRob...	RT @Min...	null
56fd44e5...	7155467...	TAshokN	RT @Min...	null
56fd44e5...	7155467...	UttarPrad...	RT @Min...	null
56fd44e5...	7155464...	kushmew...	RT @shre...	null

the word “good” will actually be intensified by the word “very” and will be negated by the word ”not”. First, each word has a sentiment value ‘S’. The sentiment computation formulas are as follows:

$$\boldsymbol{F}_N\left(\boldsymbol{S}\right) = \begin{cases} max\left\{\dfrac{\boldsymbol{S}+100}{2}, 10\right\} if\, S < 0 \\ min\left\{\dfrac{\boldsymbol{S}-100}{2}, -10\right\} if\, S > 0 \end{cases}$$

where, $\boldsymbol{F}_N(\boldsymbol{S})$ **-** Negation Function and **S –** Sentiment of a word.

The above is the formula for calculating the correct negated value for a word that is right after a word detected for negation:

Down Toners: $S = S \times 0.5$

Weak Amplifiers: $S = S \times 1.5$

Strong Amplifiers: $S = S \times 2.0$

where, **S –** Sentiment of a word, Formulae for calculating values for words that comes after intensifiers. (Down Toners, Weak Amplifiers, and Strong Amplifiers).

4.8. Calculation of Final Sentiment

Once the emotional value of each tweet is generated we aggregate them and find the final value of the tweet. We call these the positive sentiment, negative sentiment, positive evidence and negative evidence (F_p, F_n, E_p, E_n) as used by Jurek et al. (2015).

Positive and negative sentiments are generated based on the sentiment values of each word whereas positive and negative evidence is generated based on the positive and negative probabilities. The formulae are as follows:

Calculation of F_p:

$$\boldsymbol{F_P} = \boldsymbol{min}\left\{\frac{\boldsymbol{A_p}}{2 - \boldsymbol{log}\left(3.5 \times \boldsymbol{W_p} + \boldsymbol{I_p}\right)}, 100\right\}$$

Calculation of F_N:

$$\boldsymbol{F_N} = \boldsymbol{max}\left\{\frac{\boldsymbol{A_N}}{2 - \boldsymbol{log}\left(3.5 \times \boldsymbol{W_N} + \boldsymbol{I_N}\right)}, -100\right\}$$

where, A_p is the average of positive sentiment of words, W_p is the number of positive words in the tweet, W_N is the number of negative words in the tweet:

$$\boldsymbol{E_P} = \min\left\{\frac{\boldsymbol{A_P}}{2 - \log\left(3.5 \times \boldsymbol{W_P}\right)}, 1\right\}$$

Calculation of E_N:

$$\boldsymbol{E_N} = \max\left\{\frac{\boldsymbol{A_N}}{2 - \log\left(3.5 \times \boldsymbol{W_N}\right)}, -1\right\}$$

where, A_p is the average of positive sentiment of words, W_p is the number of positive words in the tweet, W_N is the number of negative words in the tweet.

Finally, we give a single value as output with the following algorithm:

Algorithm 1

```
IF W_N==0)
        RETURN finalSentiment(F_P,E_P)
ELSE IF(W_P==0)
        RETURN finalSentiment(F_N,E_N)
ELSE
```

```
{
        IF(EP-EN> 0.1)
                RETURN finalSentiment(FP,EP)
        ELSE IF (EN-EP> 0.1)
                RETURN finalSentiment(FP,EN)
        ELSE {
                IF(FP + FN> 0)
                        RETURN finalSentiment(FN,EN)
                ELSE IF(FP+FN< 0)
                        RETURN finalSentiment(FN,EN)
                ELSE
                        RETURN 0
}}
finalSentiment(F,E)
{
        If(|F| > 25 || |E| > 0.5)
                RETURN F
        ELSE
                RETURN 0

}
```

where F is a generic sentiment value and E is a generic evidence value

The above algorithm makes use of the finalSentiment() function and carries out a series of case conditions to determine a single emotion value of a tweet. This final value is then stored in MongoDB to be used in the next phase. Figure 6 portrays the analysis of the sample tweet by our proposed sentiment analysis system.

4.9. Finding the Criticality

The final module of this proposal concentrates on calculating the range of severity of problems that might occur during an event. It basically segregates this range into three values namely mild medium and critical, as shown in Table 1.

The values 1, 2, 3 are just identifiers of the intensity of each tweet. If more tweets get the value 1 then it's a relatively non critical situation. If more tweets get the value 2 then it's slightly critical. But if the concentrations of tweets are located in the 3 region then the situation is very critical. We can use LOW, MEDIUM and HIGH instead of 1, 2, 3 but for calculation purposes its better if these values are in integer format.

Figure 6. Analysis of a sample tweet

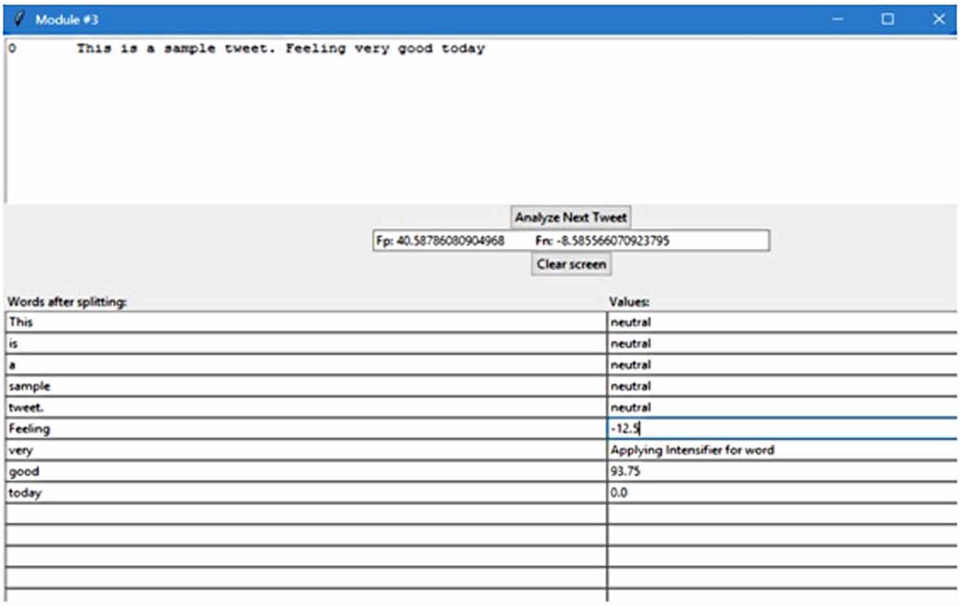


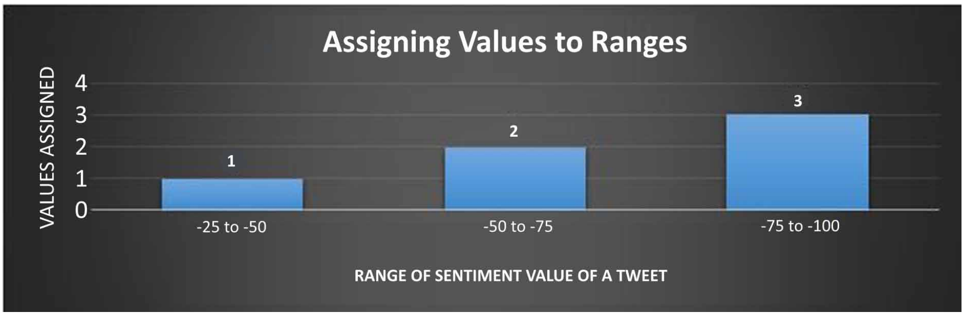
Table 1. Ranges of negative tweets sentiments and the corresponding value assigned to calculate criticality

Range of F (Final Sentiment of Tweet)	Value Assigned
-25 to -50	1
-50 to -75	2
-75 to -100	3

There is a threshold which specifies whether a particular tweet is positive or negative. Using this threshold we take into account all the tweets that go below the negative line. The range from -100 to -25 is classified into three parts as shown in Figure 7. If the tweet occurs in -25 to -50 then a value 1 is given. If the tweet occurs between -50 to -75 then a value 2 is given. If the tweet occurs between -75 to -100 then a value 3 is given. Now these values represent the number of negative tweets the particular tweet amount to. Now if the total number of negative tweets is greater than half of the total number of tweets we use the following algorithm.

The algorithm is presented below. The output from the third step is taken and a graph is plotted based on the value.

Figure 7. Assignment of value to ranges



Algorithm 2

```
tweetCriticality(F)
{
        Value is 0
        IF (F is between -25 and -50) then:
            Add 1 to Value
        ELSE IF (F is between -50 and -75) then:
            Add 2 to Value
        ELSE IF (F is between -75 and -100) then:
            Add 3 to Value
        IF (TN> TT/ 2) then:
            RETURN (TN / Value*100)
        ELSE:
            RETURN (Value/ TT *100)
}
```

Here, TN represents Number of negative tweets and TT denotes Total number of tweets.

We calculate the ratio of total number of negative tweets to that of the total number of negative tweets the values amount to. This is done by adding all the values of each negative tweet specified. This gives us a probability of the criticality of crimes. We multiply this by 100 to get the percentage of criticality expected during the event to a certain extent. Now if the total number negative of tweets is less than the total number of tweets then we use the following.

We calculate the ratio of the total number of negative tweets the values amount to with the total number of tweets. This gives us a probability of criticality occurring. Multiplying this by 100 we get the percentage of criticality of the particular event to a certain extent.

5. PERFORMANCE EVALUATION

The modules were developed using Python 3.4.2 and MongoDB for storing the tweets and related data. Tweets that are fetched by module 1 are stored in MongoDB as documents in a redefined collection. The tweets are retrieved by module 2 and the improved lexicon based algorithm is applied to calculate the sentiment of tweets. The values of F_p, F_n, E_p, and E_n are used to classify them as positive, negative and neutral. They also have an associated intensity indicating the sentiment.

5.1. Working in Hindsight

Since we can't analyse the application in real time, we decided to take a hindsight view into analysis. Recently India had played a match versus New Zealand during the group stages in 2016. In the match played in India, India lost by 40 runs against New Zealand in their home ground. Though this is a sad thing that hurts the feelings of many Indian citizens, this particular game proved to be advantageous for effectively testing our application in terms of finding the emotion shown by the Indian citizens. But since this is an Indian match even though many people were sad and angry towards the Indian Cricket Team not many like to discredit the effort they put in the match. Taking all of this into account we decided that the result would be a moderate criticality shown by the Indian citizens towards the Indian Cricket Team. The result was more than promising in the end as we achieved 50% criticality approximately.

We first searched for previous tweets with the hashtag #IndVsNz to get all the tweets about the match that took place on 15 – March, 2016. Using the search API given to us by Twitter we got about 200 tweets and placed them in the database. Then we analysed them to assign them the **F** value mentioned in our proposed work. We then calculated the criticality and displayed them in a graph for detailed support of our work. The graph is shown in Figures 8 and 9. We believe this output precisely shows the criticality of Indian Citizens that showed their emotion through Twitter. We took another match in which India actually won against Australia. It was a deciding game. That is if India lost that qualifier then they would have been eliminated. But they emerged victorious in the end.

We decided that we would like to test some event that was actually positive in the eyes of Indian citizens and came up with the idea of taking another match in which India actually won. In this match played on 27 – March, 2016 India defeated their rivals Australia by 6 wickets. It was a glorious victory and it made many fans happy.

So we decided to take tweets with hashtag #IndvsAus. We put them in database as we did for the previous analysis. Then we let our analytics part calculate the value of **F** according to the proposed work algorithms. Then we concluded by calculating the criticality of the tweets and then finally plotted a detailed graph with 200 tweets.

Figure 8. Criticality output for analysis of tweets of T20 cricket match between India and New Zealand on 15th March 2016

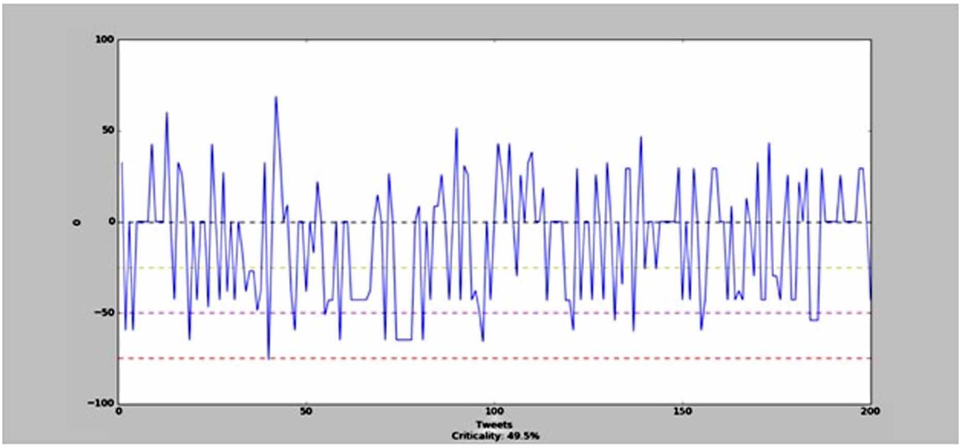
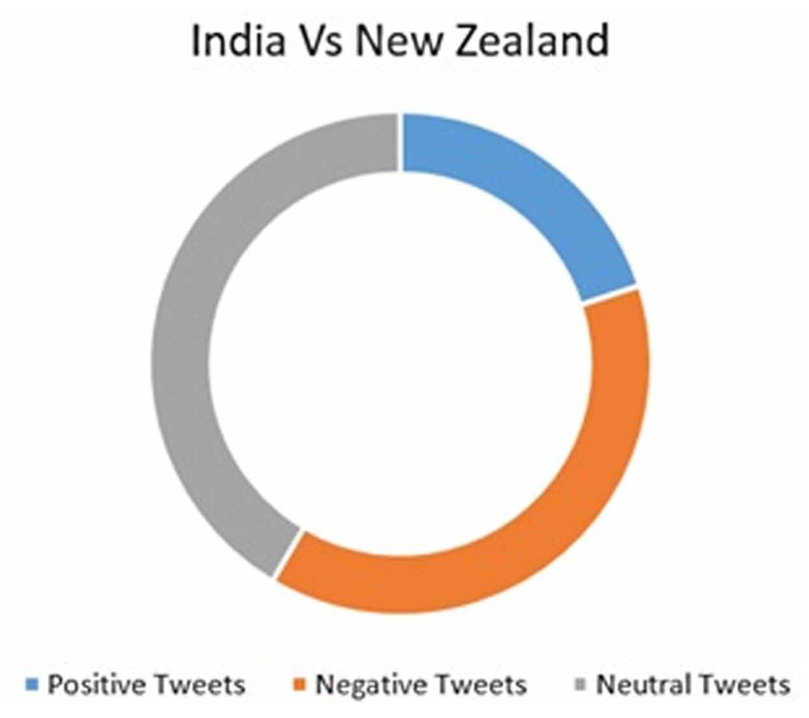


Figure 9. Pie chart showing the distribution of sentiment values of tweets for India vs New Zealand cricket match



The Graphs are shown Figures 10 and 11. We found the result of the criticality to be 2.1% which was exactly the results we were hoping for, since the users were happy with the match's results. This proved that our application can precisely find the approximate criticality when presented with various situations.

Finally, we analysed something extreme in hindsight. So we took the infamous Kolkata Bridge Collapse that happened recently and caused so much anger towards the construction company that used cheap materials to finish up the project fast. It turned out to be a really gore disaster that began to be called as the "Act of God". Over 15 people were found dead and more than 50 people were severely injured and hospitalized. For this, we used the hashtag #kolkatabridgecollapse and collected about 200 tweets. We then put them in a database for further processing. We similarly used the analytics mentioned in the proposed work to find the **F** value of the tweets. We finally got the criticality and plotted a graph for visualization. This is shown in Figures 12 and 13.

We found the criticality to be 90% approximately. This was the expected criticality because of the nature of the topic chosen to retrieve tweets.

Stanford test Twitter corpus used in Go et al. (2009) is a set of manually labelled tweets. Every tweet is already labelled as positive or negative or neutral in sentiment. We used the proposed analytics on the corpus and the criticality was found for the entire collection. The visual result as a graph plot of the tweets is shown in Figures 14 and 15 along with the resulting criticality value. Thus, three different boundary situations and the Stanford test Twitter corpus of Go et al. (2009) were taken for analysis of criticality and the efficiency was found to be quite precise to what we

Figure 10. Criticality output for analysis of tweets of T20 cricket match between India and Australia on 27th March 2016

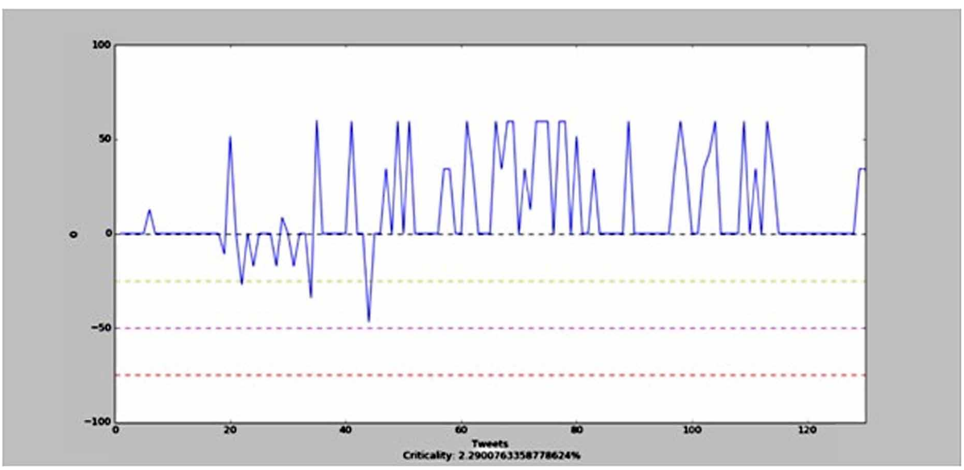


Figure 11. Pie chart showing the distribution of sentiment values of tweets for India Australia cricket match

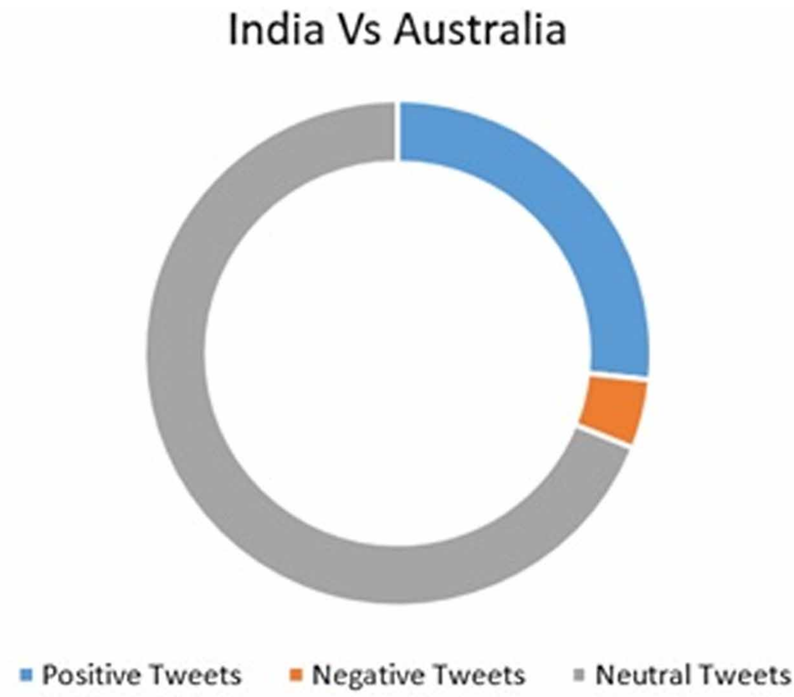


Figure 12. Criticality output for analysis of tweets during the unfortunate Kolkata bridge collapse accident on 31st March 2016

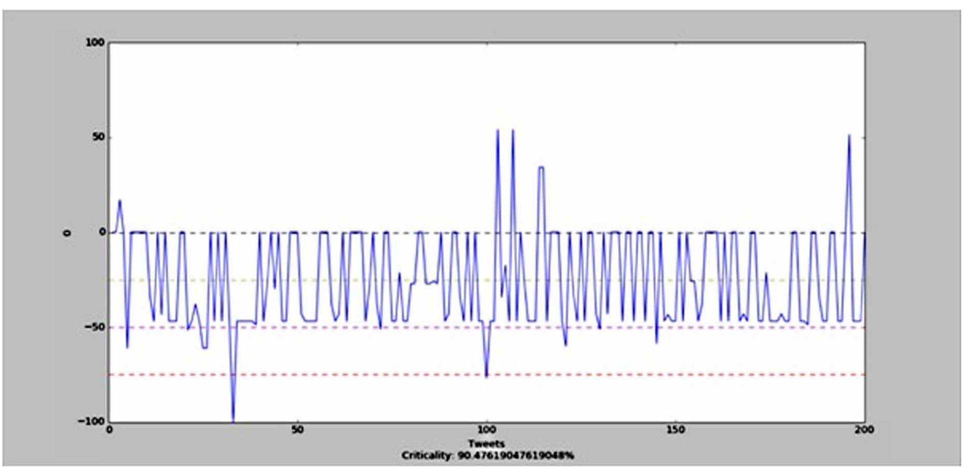
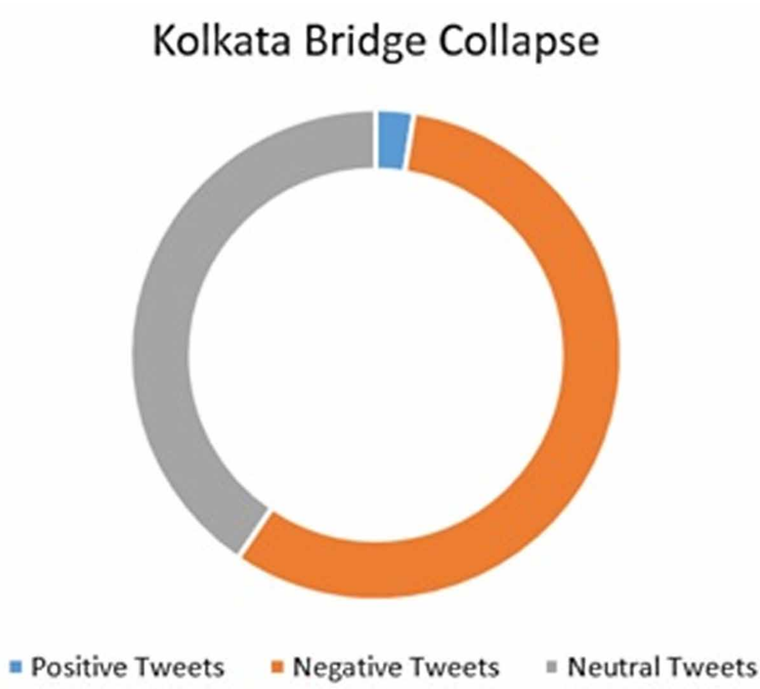


Figure 13. Pie chart showing the distribution of sentiment values of tweets for Kolkata bridge collapse incident



predicted. This proves the functioning of the application. Figure 16 depicts the number of positive words and their intensity in relation with all the test cases that we experimented with using the application. The x axis contains different type of test data that we collected. As shown below, the positivity of Kolkata data is very low in comparison with its negativity since its criticality is very high.

Figure 17 shows how many neutral words are there in each of the test data used to test the application. Even though it's not directly related to the results, it still is a useful remark for future analysis as it shows how many neutral tweets are actually there in real time data. Figure 18 relates the test cases with their number of negative tweets and their intensities. As shown we can see that for Kolkata the negativity is high in relation with the positivity.

The relation between different test cases in accordance with theirpositive and negative tweets was clearly established in Figure 19 to get a picture of the data we dealt with as a whole. Thus, the results of different test cases in regard to their criticality and final level of sentiment is tabulated in Table 2. It shows that the event's sentimental nature (positive or negative) can be quantified by the measure of criticality and also be inferred as positive or negative.

Figure 14. Analysis result for Stanford Twitter test corpus

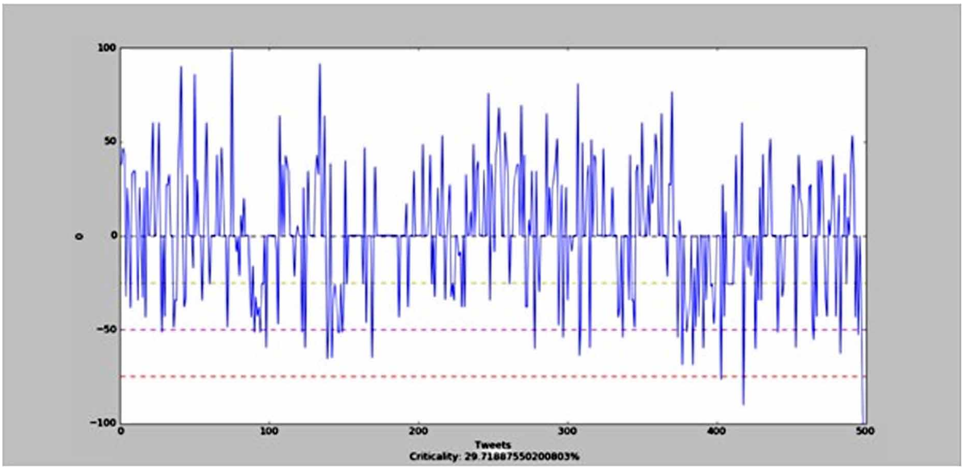


Figure 15. Pie chart showing the distribution of sentiment values of tweets for India vs New Zealand cricket match

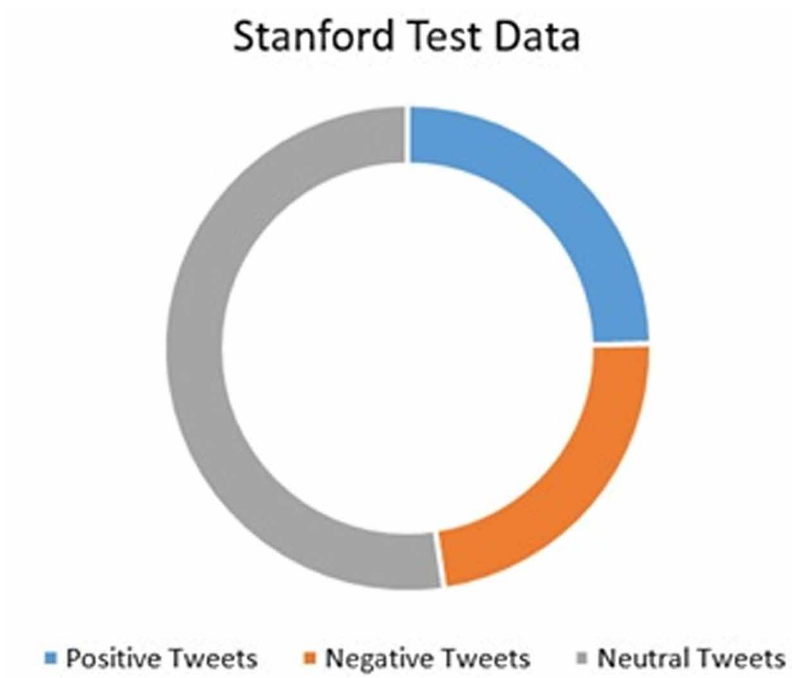


Figure 16. Correlation between number of positive tweets with their sentiment values and the test scenarios

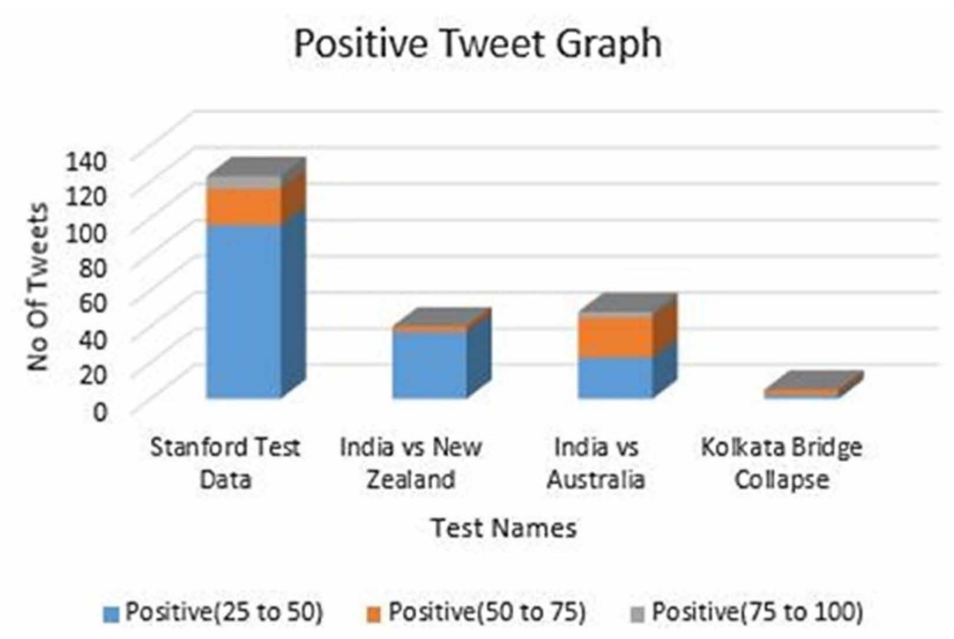


Figure 17. Correlation between number of neutral tweets and the test scenarios

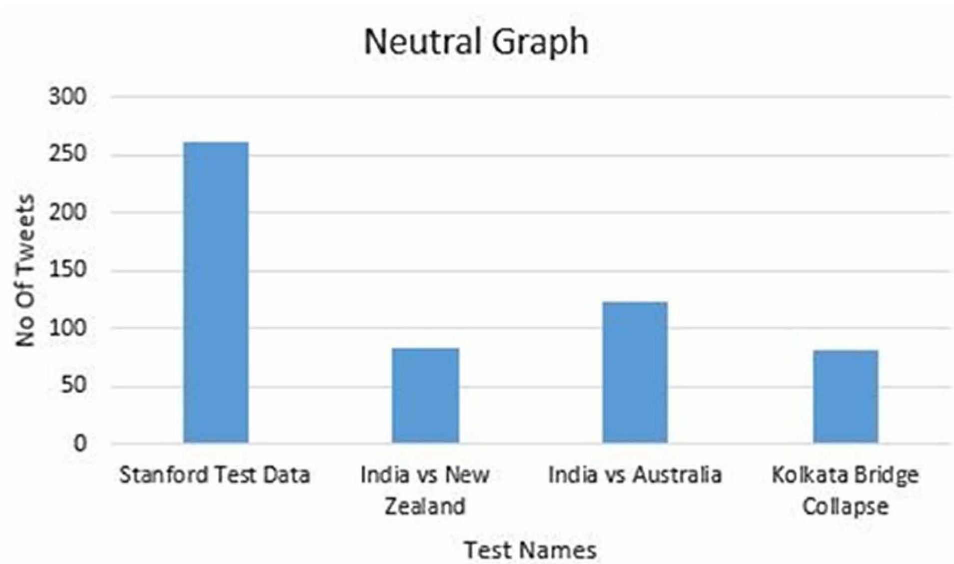


Figure 18. Correlation between number of negative tweets with their sentiment values and the test scenarios

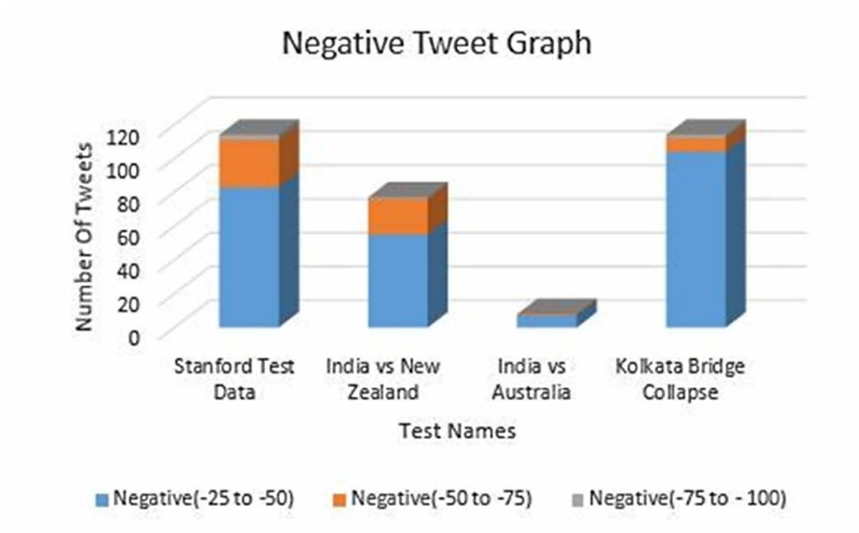
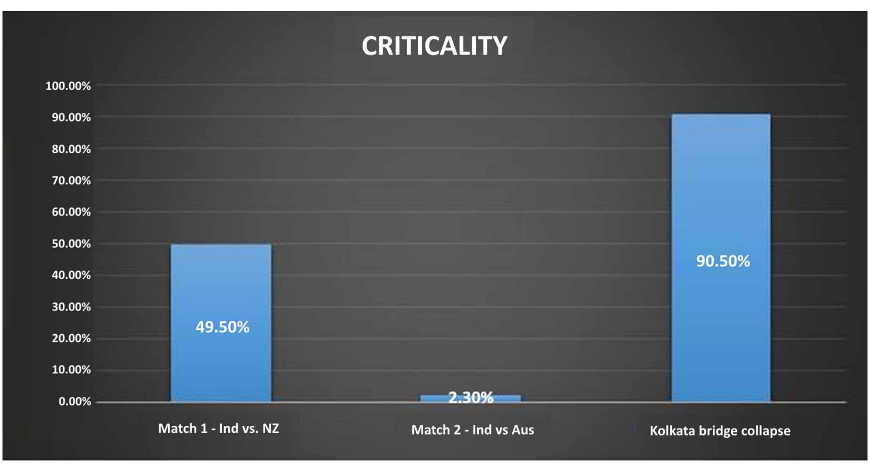


Table 2. Criticality results for the three events taken for experimentation

S. No	Event	Expected Result	Criticality	Obtained Inference
1	Match 1 – Ind vs NZ	Negative	49.5%	Negative
2	Match 2 – Ind vs Aus	Positive	2.3%	Positive
3	Kolkata bridge collapse	Negative	90.5%	Negative

Figure 19. Obtained criticality values of for all the test cases



6. CONCLUSION

The proposed work makes use of a lexicon based analysis to find the emotional values of each tweet. To the proposed system, we have included the ability to predict possible problems that can occur in the future using the criticality value generated, so that the law enforcement agencies can take appropriate action and be prepared for them. The percentage of criticality calculated can be used efficiently by any security agencies to predict possible riots that can happen during an public event and in that regard, either they can assign a better police force or just cancel the event if the criticality is high. This work as a whole is done with the main purpose of modulating the specific tasks of analysing the events in public domain and any part of the system as a module can be reused in the future, based on the trending issues. The generation of the list of words and their values in the language like Tamil manually or automatically, and then database of English words should be switched with the newly generated database. If we are able to generate a corpus with words from another language then this whole work can be done to calculate the criticality in that particular language. The present system makes predictions on an event based search, specifically based on the location based tweets generated. The generated results of the system have accurate prediction on the sentimental values of the crowd at a particular location. The same system can be used with any language, with simple modification with the words corpus database in that language. As a future work, the developed system can be extended to the mobile version. The developed system can be further enhanced to detect criticality on multi-language tweets such as tweets combining multiple languages English and Hindi.

ACKNOWLEDGMENT

The authors are grateful to Science and Engineering Research Board (SERB), Department of Science & Technology, New Delhi, for the financial support (No. YSS/2014/000718/ES). Authors also thank SASTRA University, Thanjavur, for providing the infrastructural facilities to carry out this research work.

REFERENCES

Abdulla, N. A., Ahmed, N. A., Shehab, M. A., & Al-Ayyoub, M. (2013). Arabic sentiment analysis: Lexicon-based and corpus-based. Proceedings of AEECT (pp. 1-6). IEEE.

Avanco, L. V., & Das Gracas Volpe Nunes, M. (2014). Lexicon-Based Sentiment Analysis for Reviews of Products in Brazilian Portuguese. Proceedings of BRACIS (pp. 277-281). IEEE. doi:10.1109/BRACIS.2014.57

Basave, A. E. C., He, Y., Liu, K., & Zhao, J. (2013). A Weakly Supervised Bayesian Model for Violence Detection in Social Media. Proceedings of IJCNLP (pp. 109-117). Asian Federation of Natural Language Processing / ACL.

Colbaugh, R., & Glass, K. (2011). Agile Sentiment Analysis of Social Media Content for Security Informatics Applications. Proceedings of EISIC (pp. 327-331). IEEE Computer Society. doi:10.1109/EISIC.2011.65

Colbaugh, R., & Glass, K. (2013). Analyzing Social Media Content for Security Informatics. Proceedings of EISIC (pp. 45-51). IEEE. doi:10.1109/EISIC.2013.14

Esuli, A., & Sebastiani, F. (2006). *SENTIWORDNET: A Publicly Available Lexical Resource for Opinion Mining*. LREC.

Glass, K. & Colbaugh, R. (2012). Web Analytics for Security Informatics. CoRR: abs/1212.6810

Go, A., Bhayani, R. & Huang, L. (2009). Twitter Sentiment Classification using Distant Supervision.

Jurek, A., Bi, Y., & Mulvenna, M. D. (2014). Twitter Sentiment Analysis for Security-Related Information Gathering. Proceedings of JISIC (pp. 48-55). IEEE. doi:10.1109/JISIC.2014.17

Jurek, A., Mulvenna, M. D., & Bi, Y. (2015). Improved lexicon-based sentiment analysis for social media analytics. *Security Informatics*, *4*(1), 9. doi:10.118613388-015-0024-x

Ngoc, P. T., & Yoo, M. (2014). The lexicon-based sentiment analysis for fan page ranking in Facebook. Proceedings of ICOIN (pp. 444-448). IEEE.

SentiWordNet. (n. d.). Retrieved from http://sentiwordnet.isti.cnr.it

Spitters, M., Eendebak, P. T., Worm, D. T. H., & Bouma, H. (2014). Threat Detection in Tweets with Trigger Patterns and Contextual Cues. Proceedings of JISIC (pp. 216-219). IEEE. doi:10.1109/JISIC.2014.39

Taboada, M., Brooke, J., Tofiloski, M., Voll, K. D., & Stede, M. (2011). Lexicon-Based Methods for Sentiment Analysis. *Computational Linguistics*, *37*(2), 267–307. doi:10.1162/COLI_a_00049

This research was previously published in the Journal of Organizational and End User Computing (JOEUC), 29(4); edited by Steven Walczak and Sang-Bing Tsai; pages 51-71, copyright year 2017 by IGI Publishing (an imprint of IGI Global).

Chapter 14
Using the Internet to Plan for Terrorist Attack

David Romyn
Griffith University, Australia

Mark Kebbell
Griffith University, Australia

ABSTRACT

In this chapter, we discuss how terrorists can use the Internet as a source of information to plan for terrorist attacks. Online anonymity services such as virtual private network (VPN) are discussed, along with advantages and disadvantages of using these services. We also discuss online bomb-making instructions and highlight ways in which these can be used to the advantage of law enforcement. Finally, the use of the Internet as a reconnaissance tool for target selection is discussed, with descriptions of current and past research in this field to identify key information that is available to terrorists, and how this information can be manipulated to reduce the likelihood or severity of a terrorist attack.

INTRODUCTION

The Internet has been used in a variety of ways by terrorists, including the provision of information to others, financing terrorist organisations, communication between terrorists, the recruitment of new potential terrorists, and as an information gathering tool (Conway, 2006; Keene, 2011; United Nations Office on Drugs and Crime [UNODC], 2012). It has also been argued by some that the Internet provides a mechanism by which individuals, who would otherwise not have conducted a

DOI: 10.4018/978-1-7998-2535-7.ch014

terrorist attack, can self-radicalise and access the information they require to carry out an attack (Benson, 2014).

In this chapter, we will discuss aspects of how the Internet can be used by terrorists to prepare for terrorist attacks. We will also discuss how the Internet can be used by law enforcement to increase the chance of detecting terrorism before it happens, or to reduce the effectiveness of attacks when they occur. Specifically, we will discuss the use of online anonymity services such as virtual private network (VPN) and the onion router (TOR). We will also discuss the use of the Internet for instructions on how to make explosive devices. Prior research based on a 'red-team' design to investigate terrorist target selection and the use of the Internet as a reconnaissance tool will also be described. Finally, ways that these factors can be manipulated to reduce the likelihood and effectiveness of terrorist attacks will be explored. We conclude that while the Internet is a valuable source of information for those planning a terrorist attack, the accuracy and availability of this information can be manipulated to reduce the likelihood and effectiveness of an attack.

TRACING TERRORIST ACTIVITY ONLINE

While some authors (e.g., Conway, 2006; Keene, 2011; Thomas, 2003) discuss ways in which the Internet can facilitate aspects of planning and conducting a terrorist attack, other authors (e.g., Benson, 2014; Kenney, 2010; Torres-Soriano, 2012) argue that the Internet poses a risk to terrorists that use it, and a method by which law enforcement can identify and track terrorists. Both of these conclusions are partly correct.

Benson (2014) notes that while the Internet can give the perception of anonymity to those who use it, it is still possible for law enforcement to trace where information has come from and where it has gone. While this is true of the ability to monitor and trace general Internet traffic, this assertion may not be true in all cases if someone takes steps to remain anonymous online and hide their identity. An investigation of the use of online anonymity practices amongst those involved with online piracy, found a portion (17.8%) of those involved with the practice, used services such a VPN to hide their identity online (Larsson, Svensson, de Kaminski, Rönkkö, & Olsson, 2012). Antoniades, Markatos, and Dovrolis (2010) note that there are over 100,000 Internet users who are using TOR on a daily basis to hide their identity. Those involved with terrorism, who are also motivated to hide their identity online, could use these same methods to make tracking them more difficult.

The use of a VPN is a reasonably robust method to ensure online anonymity. All traffic sent between a user and a VPN is encrypted, so that the content of this traffic is hidden from the Internet service provider (ISP) or any other agency that may be collecting metadata (Larsson et al., 2012). The use of a VPN also makes it difficult to identify which individuals have accessed particular information online, as the identifying information will be referred to the VPN itself, rather than the person who was using that VPN. It has also been found that as the efforts of authorities to track particular individuals increase, so does the use of VPN to hide people's identity.

Larsson and Svensson (2010) investigated the use of online anonymity services, such as VPN, to hide the identity of those involved in file sharing in Sweden. Specifically, the authors surveyed a very large sample (N=1047) of computer users two months prior to the implementation of a policy aimed at stopping online piracy. They then surveyed a sample (N=1042) of computer users seven months following the implementation of the policy. The survey also gauged how frequently participants were engaged in online file sharing. Overall, the study found that among those who were not heavily involved in file sharing, there was no significant increase in use of VPN following the implementation of the new policy. However, there was a significant increase in the use of VPN among those in the sample that had been identified as being frequently involved in file sharing following the implementation of the policy (Larsson & Svensson, 2010). This study demonstrates that the use of anonymity services such as VPNs increases among those motivated to hide their identity, as measures to track those people online are increased. However, the use of a VPN is still not a perfect solution for anonymity.

The provider of the VPN service still has full access to all of the information regarding their users' actions on the service; so users are placing a great deal of trust in the service that they use (Larsson et al., 2012). It is also possible for law enforcement agencies to subpoena the information held by VPN services that fall within their jurisdiction (Benson, 2014). It is also possible for an ISP to block its customers from accessing a particular service such as a VPN (Edman & Yener, 2009; Rescorla, 2008). Because of this, it may be possible in some jurisdictions for governments to require a locally-based ISP to block customers' access to a VPN, if it is found that the service is being used to facilitate terrorism-related activities (Edman & Yener, 2009). Another possible solution, where user access to the VPN itself cannot be controlled, is for governments to block the actual VPN service from being able to access key services. In that instance, while users would still be able to access the VPN, any traffic identified as being from that VPN would be blocked from accessing those services. A further way of reducing the use of VPN to hide a terrorist's identity online, is to give the impression to the wider community that it is a less-secure method than it actually is.

There has been much discussion in recent years regarding the ability of the U.S. National Security Agency (NSA) to use a 'back door' to break through encryption services (Schneier, 2007; Soghoian, 2010). Without discussing which encrypted traffic the NSA is or is not able to access, the belief that governments are able to view encrypted information may lead some away from using services such as VPN when using the Internet (Torres-Soriano, 2012). For this reason, it would be useful to give the impression to those engaged in terrorist activities that VPN are not a reliable method of ensuring anonymity. Doing this may encourage some terrorists to avoid the use of the Internet altogether. While this would mean that they are also unable to be monitored using the Internet, as we shall see later, it also means that they would be removing themselves from a useful medium to facilitate terrorist attacks.

Another commonly used method of maintaining online anonymity is TOR. TOR is a method of online browsing that randomly routes a user's traffic through multiple points, or 'nodes', before it reaches its online destination (Antoniades et al., 2010; Dingledine, Mathewson, & Syverson, 2004). This routing makes it impossible for an outside observer to identify the origin of the traffic. Unlike VPN services, TOR does not function well for moving large volumes of data, and is more suited to Internet web-browsing than for piracy (Antoniades et al., 2010; "The Tor Project", n.d.). However, an advantage with TOR is that it is freely available to anyone and does not require a high level of skill to use. Most people are able to access TOR simply by installing a particular type of browser on their computers ("The Tor Project", n.d.). TOR also has some advantages over VPNs to a would-be terrorist, in that it does not require all of a user's traffic to pass through a single service provider that could pass that information on to the authorities. However, there are also some weaknesses with TOR that have been exploited by government agencies.

Murdoch and Danezis (2005) note that while it is impossible to observe traffic and identify a particular source, it is possible to identify which traffic has come from the same source and attempt to use the content of that traffic to identify the source itself. This form of traffic monitoring allows for an observer to build a profile of a particular user, and to sift through the content of their traffic for identifying information. While using TOR itself does not require much technical skill, maintaining an online presence without providing identifying information can be difficult (Murdoch & Danezis, 2005; "The Tor Project", n.d.). Another weakness that has been identified is the use of malicious exit nodes (Chakravarty, Portokalidis, Polychronakis, & Keromytis, 2011). When traffic passes through TOR, it must exit TOR through what is known as an exit node, which is a random router that can be set up by anyone who wishes to be a part of TOR. Antoniades et al. (2010) estimate that in 2009, there were over 600 of these exit nodes located in 48 different countries. It is possible for whoever is controlling the exit node to insert malicious code into the traffic and identify the origin (Chakravarty et al., 2011). This fact has been exploited by government agencies to identify individuals using TOR.

Although the identity of the original user is hidden in TOR, an observer knows the identity of the exit node that the traffic is coming from. While the selection of exit nodes is essentially random within TOR, Jansen, Tschorsch, Johnson, and

Scheuermann (2014) describe a method, known as a sniper attack, which can be used to exploit exit nodes and identify an individual using TOR. A sniper attack involves a government agency identifying, overloading and shutting down specific exit nodes being used by an individual. This action then forces the individual's traffic to route through a different exit node. By overloading the exit node that that an individual is using, the user's traffic can eventually be routed through an exit node that is being monitored by the government agency (Jansen et al., 2014). At this point, the original user can be identified.

In summary, it should not be assumed that the Internet provides a completely safe environment for terrorists to organise terrorist attacks, or that the Internet provides a sound method by which law enforcement can trace the online presence of those involved in terrorist activities. While it is possible to trace an individual's activity online, it is also possible for an individual to use services like VPN or TOR to hide their identity from those who are monitoring their activity online.

However, depending on jurisdiction, there are still measures that can be used to trace the identity of people using a VPN. It is also possible to either block access to the VPN service itself, or to block the VPN service from being able to access particular information. Likewise, TOR does provide a level of anonymity to a user, but it is possible to still profile a user or exploit weaknesses in TOR to identify an individual. Finally, if those who are utilising VPN or TOR to hide their identity, are given the impression that this is not a reliable method of ensuring anonymity, they may avoid using these sorts of services, or from using the Internet altogether.

USING THE INTERNET TO PREPARE FOR TERRORIST ATTACKS

Regarding the planning of attacks, the Internet has been described as being an invaluable tool for the gathering of information such as how to create weapons for an attack, and to identify and conduct reconnaissance on likely targets for an attack (Barnes, 2012; Brunst, 2010). Romyn and Kebbell (2013) conducted a 'red-team' experiment to investigate the order and importance of particular tasks when planning a terrorist attack. A red-team is where participants play the role of an enemy – in this case a terrorist. In the experiment, soldiers and civilians were given the roles of trained and untrained terrorists respectively, and participants were asked to list the order and importance of specific tasks related to planning a terrorist attack. These tasks included: identifying a target, searching for information online, conducting reconnaissance on the target, acquiring weapons, and testing weapons.

The results of this experiment showed that regardless of whether participants were military trained or civilians, they tended to identify targets before working towards acquiring weapons (Romyn & Kebbell, 2013). The results also indicated that the acquisition of weapons and the identification of a target were considered significantly more important than other tasks, such as acquiring other equipment or finding a location to prepare for an attack. Because of the importance of acquiring weapons and identifying targets, we will discuss each in turn.

Using the Internet to Construct Weapons

The most common method of terrorist attack in Europe and Australia is using an explosive device (Mullins, 2011; Nesser, 2008). In the United States, the most common method of terrorist attack is using a firearm, with explosives the second most frequent method (Spaaij, 2010). Spaaij (2010) suggests the difference for the method of attacks within the U.S. compared to other countries is due to the lack of firearm restrictions in the United States. Barnes (2012) notes the ease with which one can use the Internet to access technical information, such as how to build an explosive device. Some of this technical information provides instruction not only on how to build the device, but also how to acquire the necessary parts.

Explosives can generally be categorised into one of two broad categories: high explosives, such as dynamite and Trinitrotoluene (TNT), which undergo an explosive reaction when initiated; and low explosives, such as black powder or compressed gas, which burn rapidly instead of exploding. High explosives have a detonation force and burn rate that is many times greater than that of low explosives[1], and comparably sized devices based on high explosives create a far larger impact than those based on low explosives. Fertiliser based explosives, such as ammonium nitrate fuel oil (ANFO), are generally considered to be high explosives, and have been used in a number of attacks and attempts in the past.

While ANFO is categorised as a high explosive, it has a burn rate about half of that of other high explosives – though it is still far greater than low explosives. However, high explosives are far more difficult to create and initiate than low explosives (Benson, 2014). While ANFO is one of the simplest high explosives to make, as it requires access to specific forms of fertiliser and fuel to create, it is also one of the most difficult to actually detonate. Given ANFO has a slower burn rate than other high explosives, far more of it is required to construct an effective explosive device. For this reason, ANFO-based explosive devices are usually too large to be easily carried, and require a vehicle to be moved around, limiting their use.

Devices based on low explosives are far easier to construct and initiate, but are far less effective than comparably sized devices based on high explosives. These devices can be constructed by placing any readily available incendiary material, such as black powder, into a compressed space. When initiated, the material undergoes a very rapid burn and expansion, which causes the explosive effect. While an advantage of low explosive devices is that they are easier to initiate than high explosive devices, in turn this means that they are also easier to initiate prematurely, and if not constructed carefully, can be more dangerous to the person using it than to any would-be targets. Therefore, construction of explosive devices (i.e., based on either high or low explosives) require access to sound technical information and a degree of skill on the part of the person constructing the device.

Kenney (2010) suggests that much of the information available online would pose more of a risk to a would-be terrorist than to the general public. Many of the instructions for explosive devices that are available online would result in devices with a high likelihood of premature detonation, or a high likelihood of failing to detonate at all (Kenney, 2010). It is often difficult for someone who is searching online to build an explosive device, to gauge the quality of that information (Benson, 2014). Also, while some guides include information on how to acquire the parts needed to construct an explosive device, there are some common parts such as blasting caps (i.e., required to detonate high explosives) that are extremely difficult to acquire or construct (Barnes, 2012; Benson, 2014). This has meant that terrorists have to rely on less effective explosive devices, such as those based on chemical mixes, compressed flammable gas, or compressed gunpowder.

There have been a number of cases, such as the attempted public transport bombings in London on July 21, 2005, the attempted car bombings in London and Glasgow in 2007, and the car bombing of Times Square in New York in 2010; where the attacks failed because the explosive devices failed to detonate (Segell, 2006; West & Stewart, 2010).

The attempted terrorist attack carried out in London on July 21, 2005 was an attempt to mimic the attack carried out two weeks prior on July 7, 2005, where 52 civilians had been killed in a number of coordinated attacks on public transport around London (Segell, 2006). Similar to the July 7 attacks, the July 21 attacks consisted of four different bomb attacks carried out on public transport targets around London. Segell (2006) reports that the July 21 attacks relied on devices that were similar, but not identical to those used in the July 7 attacks. The fact that all of the devices used in the July 21 attack failed to detonate demonstrates that either the skill of those constructing the devices and/or the instructions they were relying on were inadequate.

Another similar example is the attempted attack on Times Square in New York City. On May 1, 2010, Faisal Shahzad, a U.S. citizen of Pakistani descent, parked a car loaded with two separate explosive devices and some fuel cans in the middle of Times Square in New York City (West & Stewart, 2010). West and Stewart (2010) describe the two devices as 113 kilograms of fertiliser and three 75-litre propane tanks. If Shahzad had managed to initiate the fertiliser or propane within the car, the resulting explosion would have caused considerable casualties and damage to the surrounding area. However, despite having received training overseas and being able to access instructions on the Internet on how to construct these devices, these devices failed to detonate and there were no casualties from this attack. It is unclear whether the device failed because the fertiliser had not been mixed properly, or because the initiating device was not large enough, or whether the initiating device simply failed to function; but it was this failure that led to the failure of the attack and the perpetrator was arrested soon after (West & Stewart, 2010).

There has been one recent incident (i.e., Boston Marathon bombing in 2013) where terrorists have successfully used an explosive device that was believed to have been based on an Internet-based design (Benson, 2014). However, it has since been suggested that the perpetrators of that attack had also received training overseas rather than relying solely on plans that they had viewed online, and that this may explain why their device worked correctly (Benson, 2014). It is also noted that the devices used in the Boston bombing were based on low explosives such as gunpowder rather than high explosives, indicating the difficulty with building explosive devices based on high explosives. If a comparably sized device based on high explosives was detonated in the Boston attack instead, there would have been many times more casualties as a result.

An example of the type of information (i.e., instructions for various devices) available online to terrorists can be found in 'Inspire', Al-Qaeda's English-language online magazine. A specific example is a device referred to as an 'ember bomb', which is designed to ignite and spread embers in a forest environment and start a forest fire. This device was tested by the California Department of Forestry and Fire Protection (CAL FIRE) (California Department of Forestry and Fire Protection, 2012). The ember bomb relies on a timer and electric initiator, made from a broken light bulb and match-heads, to ignite a liquid fuel mix. Staff at CAL FIRE constructed the device according to the instructions provided in the magazine. However, the initiator for the device failed to ignite the fuel. The fuel was then lit using a match, to observe the effect the fuel would have once ignited. Rather than spreading embers, the fuel created a small fire, which burned for less than 12 minutes over an area of approximately 8 inches. The CAL FIRE staff concluded that the ember bomb was impractical, compared with starting a fire using a cigarette lighter, and would probably leave valuable physical evidence behind that would be useful for identifying the perpetrator.

Another bomb-making example available from Inspire magazine, involves rigging gas bottles with a mix of flammable gases to serve as a car bomb. This device relied on using the same broken light bulb and match-heads initiator that was suggested for the ember bomb. The likelihood that the bulb and match-heads would actually function and ignite the gas cylinder is low, given that the design relies on an unprotected and fragile filament to remain intact and produce enough heat to ignite the match heads. There is also a risk that even if the initiator for that device was made effectively, the device could still detonate prematurely due to extraneous current in the circuit. For these reasons, the would-be terrorists may well blow themselves up simply from static electricity while detonating the bomb.

A separate issue with accessing specific terrorism-related information online, is that it provides a method for law enforcement to identify those planning an attack (Torres-Soriano, 2012). Given the content on these sites is designed specifically to facilitate a terrorist attack, the monitoring of IP addresses of people who access these sites could assist in identifying those who are planning an attack. This method has been used to identify individuals involved in terrorist activities in the past (UNODC, 2012). However, as previously discussed, this method would not identify possible terrorists if they are using a VPN, unless the VPN's user data can be compromised (Larsson et al., 2012). With TOR users, it may be possible to identify those accessing terrorism literatures using a sniper attack (Jansen et al., 2014). Torres-Soriano (2012) also notes that many terrorists are aware of the ability of law enforcement to monitor activity on particular websites, and are avoiding these sources of information for this reason. One particular incident, where MI6 was able to replace part of a bomb instruction in Inspire magazine with instructions for making cupcakes, led to many in jihadi terrorist groups to advocate avoiding that magazine as a source of information (Torres-Soriano, 2012).

The difficulty in constructing high explosive devices and the fear that the websites providing this sort of information may be monitored, may be the reason why some terrorists have recently been leaning towards the use of attacks based on less conventional weapons. An example of this, is the attacks in France in December 2014, where cars were driven into crowded markets in different locations, injuring dozens of people ("France attack: Van", 2014). Another example is the use of knives rather than firearms or explosives, such as the attack in Kunming, China, where 29 people were killed with knives (Gracie, 2014); or a recent attack in Melbourne, Australia where two police officers were stabbed with a knife, and where others have been accused of plotting attacks based on the use of knives or swords ("Melbourne shooting: Man", 2014). Similarly the killing of a soldier, Lee Rigby, in London, United Kingdom was committed with a machete. This may indicate that some terrorists are leaning towards simpler but less-effective methods to carry out attacks. While this does create a difficulty, in that it is easier to monitor firearms and explosives than it is to monitor cars and knives, these simpler methods also have a much smaller impact than those based on explosives.

In summary, while there is a lot of technical information available to would-be terrorists, the quality of this information is often poor (Benson, 2014; Kenney, 2010). There can also be a risk to terrorists who are accessing this sort of information, particularly if they are not using an online anonymity service, as it may be used to identify those who are planning a terrorist attack (Benson, 2014; Torres-Soriano, 2012). By monitoring who is accessing particular types of information, law enforcement may be able to identify those who are planning a terrorist attack. Because of the difficulty in creating high explosive devices, some terrorists have moved towards devices based on low explosives, or to unconventional methods such as cars and knives. While these methods are more difficult to trace and prevent, they also pose far greater risk to the perpetrators, and are far less effective.

Target Selection Preferences

Romyn and Kebbell (2013) investigated how terrorists select targets by providing several groups of participants with a list of generic locations, and asking them to rank those locations in order of preference for a bomb attack and explain why they selected those targets. The locations used in this research, in descending order of preference, were: an underground train station, a football grand final, a military parade, an airport, a religious gathering, an electrical substation, and a military base. It was found that an underground train station was the most preferred target. The reasons provided by participants for selecting this location were that it was considered to be very crowded and likely to cause high number of casualties, and that it was more likely that the attack would be successful because security personnel would not be able to identify them. A military base was the least preferred target. Participants who avoided this target did so because they believed it would not cause enough casualties or that the target was not an easy one to attack.

A later experiment (Romyn & Kebbell, 2015) also placed participants in the role of would-be terrorists, and asked them to select from a list of prospective targets, which they would prefer to attack. As with the previous experiment, participants were required to rank all the locations in the list from most to least preferred, then to explain why they selected their most and least preferred targets. This later experiment differed from Romyn and Kebbell (2013), in that the participants were provided with specific locations in a specific city that most participants were not familiar with. To inform their decisions, participants were provided a photo and brief description of each location, and with links to publicly available online information.

The links provided for participants included the specific website for that location, Google Maps, street-view images, government information pages, and security information. Participants were also able to use Google to search independently for any further information on the target locations. The Internet browser history was recorded for each participant, which provided insight into which of the links they had viewed, as well as which other information they had sought to inform their decision. It was found that almost all participants relied heavily on Google maps and street-view images to learn more about the target locations. Many participants were also found to have independently searched for information regarding the security of locations, and the number of people who visit each of the locations. It was also found that there was a significant moderate correlation between the number of websites for each location that a participant looked at, and the participant's preference for that location as a target. It was also found that participants tended to revisit information for locations that they preferred to attack. As well as providing insight into which information terrorists may view online to learn about potential targets, this experiment identified which targets were significantly more or less preferred, and what attributes of those targets informed participants' choices.

The most preferred target was a public pedestrian shopping mall in the middle of the city. Participants selected this location because it was easily accessible, had relatively low security, and a high volume of traffic. Participants selected this location over a nearby railway station, generally because there was a perception of less security in the mall than at the railway station. The target considered to be the least preferred by participants was the international airport. Participants who selected this location as their least preferred location were nearly unanimous in their reason why. The airport was the location that was perceived to have the greatest level of security.

One thing that needs to be noted regarding aspects of target vulnerability is that these assessments are very subjective, and are based heavily on how the individual perceives the location. This was demonstrated by participant responses in the research by Romyn and Kebbell (2015), where many of the participants who selected the university as their most preferred target stated that they believed the location was quite crowded; while those who selected that same target as their least preferred stated that they did so because they believed the target was not crowded. While a significant majority of people selected the pedestrian mall as their most preferred target (i.e., over 70 percent of those stated that they would attack that location because they perceived it to be an easy target), of the few who selected the pedestrian mall as their least preferred target, nearly half said that their decision was because it would not be an easy target to attack (Romyn & Kebbell, 2015). This means that one does not necessarily need to alter the features of a location to make it less vulnerable to an attack. By altering the perception of key features, such as altering online information describing how crowded the location is or the level of security present, a location can be made to appear less attractive as a target location.

While the research by Romyn and Kebbell (2013), and Romyn and Kebbell (2015) does indicate which features of a location are likely to make a terrorist more or less inclined to want to target it for an attack, it is still nearly impossible to predict which location will actually be attacked (Mueller, 2010). This is because there are arguably a near-infinite number of possible locations that a terrorist could attack, and the likelihood of any particular location coming under an attack is incredibly small. Altering the features of one location so as to make it less vulnerable to a terrorist attack would only serve to shift the attention of a would-be terrorist to a different location (Mueller, 2010).

However, there are still key public locations, such as centrally located public-transport hubs and vital infrastructure, where the impact of an attack would be amplified, when compared to other locations. Addressing vulnerability issues at these key locations may increase the likelihood of an attack occurring somewhere else, the analogy used in crime prevention is that reducing vulnerability in one area merely increases it in another – i.e., like air moving in a squeezed balloon. However, research indicates that this is not necessarily the case (for a review see Crawford, 2007). In some instances, crime prevention initiatives reduce crime not only where they are applied but this also extends to include areas where the crime prevention initiatives are not in effect. In addition, some offenders seem to give up when they find offending too difficult and not worthwhile.

Target Reconnaissance Using the Internet

Another widely cited way that terrorists could use the Internet to help facilitate an attack is through the use of Internet-based reconnaissance (Keene, 2011). Conway (2006) refers to an Al-Qaeda manual that was captured prior to 2003, which states "Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty percent of information about the enemy" (p. 290). There have since been numerous incidents overseas where people involved in planning terrorist attacks were found to possess information they had sourced online regarding specific targets and locations (Brunst, 2010; Conway, 2006; Thomas, 2003).

Some examples include an online Al-Qaeda manual that contains structural plans for a dam in the United States (Thomas, 2003); Muhammad Naeem Noor Khan, who was arrested in Pakistan in 2004 with floor plans for public buildings in the United States (Conway, 2006); and insurgents in Iraq found with Google Maps images of British military bases, which were in enough detail to identify where the accommodation, amenities and vehicle storages were located within each base (Brunst, 2010). In Australia, convicted terrorist Faheed Khalid Lodhi was found to have utilised the Internet to access electricity grid maps (Conway, 2006; Urbas & Choo, 2008). The Internet has since been utilised in some form in most cases of terrorism in Australia (Mullins, 2011). Finally, those interested in planning an assassination of a public figure can often easily find information on the upcoming locations of their target through online sources.

To investigate how the Internet can be used to plan a terrorist attack, the authors conducted an experiment to observe differences between tourists and terrorists in Internet usage in terms of gathering information on a particular location. The aim of the experiment was to observe how people use the Internet to find information about specific locations, and how this usage may differ depending on the reason for looking for that information. To investigate this, participants were randomly allocated to either a 'tourist' or 'terrorist' group, and asked to look for information on an international airport in a distant city. Participants were required to explain how they would travel to and from the airport, and where they would leave their bag or bomb (i.e., depending on the group they were assigned to). The actual Internet browsing for each participant was captured by video and analysed to identify patterns within the groups, and differences between the groups.

Both groups indicated that they were generally satisfied with the level of information they were able to access via the Internet to inform their decisions. There were no significant differences between the groups regarding how many websites they looked at, or in the number or length of Internet searches conducted. However, some valuable insights were made regarding the amount and type of information that a would-be terrorist have access to. Websites such as Google Maps, as well as websites specific to the airport, provided detailed maps of buildings and surrounding areas. These maps include details regarding the location of security within the airport, and allowed terrorist participants to identify the best place to leave an explosive device.

Further Internet searches conducted by participants, provided terrorist participants with information on: whether or not CCTV was used in a particular location; the number and type of security personnel present; and which modes of transport were more or less likely to include security that would positively identify passengers. For example, one of the terrorist participants explained his choice of transport by stating "… my name is not on any records, and I have a higher chance of getting away with it", while another stated "… you can purchase a ticket on the day from the driver of the bus, this means that you would not have to provide any information therefore there will be no record of your name". Overall, while tourists identified modes of transport that were fast or cheap, terrorists identified modes where they were not required to provide identification in order to ride, which did not include cameras on-board (so that they could blend in with the crowd).

Participants in both the tourist and terrorist groups were compared on their Internet browsing habits. Specifically, the research investigated the number of unique websites participants looked at, and the time spent searching for information. The number of Google searches conducted did not significantly differ between participants in the tourist or terrorist groups. The results from this experiment suggest that it may be difficult to identify someone conducting terrorism-related reconnaissance among all of the other Internet traffic, simply by the pattern in which individuals look for information.

However, the research has also highlighted the types of information that can be freely accessed, and how this information can be used to inform terrorist's decisions when planning an attack. Using the Internet alone, it is possible to find out the layout of a location, what sort of security exists at a particular location, the number of people who visit a location, transport to and from a location, and many other very relevant pieces of information. Because of this, care must be taken to ensure information that may be useful to those planning a terrorist attack is limited wherever possible. Finally, while the findings of this research suggest that it is not possible to identify terrorist suspects involved in online reconnaissance by monitoring all Internet traffic, monitoring the browsing habits of those already suspected of being involved in terrorism has been used many times in the past to identify which locations are likely to be targets for an attack (Mullins, 2011; Urbas & Choo, 2008).

SOLUTIONS AND RECOMMENDATIONS

The Internet does provide a large amount of information that is useful to someone planning a terrorist attack, including information on key locations, and instructions on how to make and use weapons for an attack. By monitoring individuals who are accessing terrorist-specific information, such as bomb-building instructions, it may be possible to identify those involved in terrorism activities. While it may be possible to track the activities of individuals online, it is also a relatively simple process to ensure anonymity online using services such as VPN or TOR (Dingledine et al., 2004; Larsson et al., 2012). For those who are using a VPN to hide their activities online, authorities may be able to legally require the VPN services to allow them access to their records (Benson, 2014). It may also be possible to block an individual's access to the VPN service, or in the case of VPN and individuals that exist in a different jurisdiction, it may be possible to block that VPN's access to key online information. TOR users can possibly be identified by building a profile of their activities online, or by using a sniper attack (Jansen et al., 2014; Murdoch & Danezis, 2005). Finally, by giving the impression that VPN and TOR are not entirely anonymous sources and this being a reality, authorities may be able to reduce the use of such services by terrorists.

Some terrorists, when planning an attack, have certainly used online information both to learn more about specific locations, and how to construct explosive devices and other weapons. However, acquiring the materials to construct an explosive device and assembling one that will actually function as intended, is not a simple process (Benson, 2014). Much of the information available online is considered to be of poor quality, and is more likely to fail or cause injury to the terrorist than to harm others (Kenney, 2010). Given how difficult it is for non-experts to tell the difference between good and bad information on how to build explosives, law enforcement could further reduce the usefulness of this information by including misinformation regarding how to construct explosive devices. This reduces the likelihood that a device would function, and that terrorists would base a device on one of these instructions. Providing misinformation regarding how to make bombs would also reduce the credibility of this source of information generally among terrorists, which in turn means that terrorists would need to rely on more reliable but less effective methods (Torres-Soriano, 2012).

Given the numerous recent examples of failed terrorist attacks, such as the Times Square attack, it may be useful to focus more public attention on these failures. By highlighting the likelihood of failure, those considering involvement in terrorism may be dissuaded. Also, playing down the possible severity of the attacks, while highlighting their failures, would serve to reduce public fear regarding such attacks. In the end, given that the aim of these attacks is to induce fear in a wider audience, this would reduce the effectiveness of these actions.

Regarding the selection of targets, the Internet does provide a wealth of extremely useful information for those planning a terrorist attack. This information can be used to inform decisions regarding which target should or should not be attacked. In particular, Romyn and Kebbell (2015) found that locations that were considered to be very crowded and with relatively low security were more attractive as terrorist targets. Conversely, locations that were seen to have very high security were perceived as being significantly less attractive as possible terrorist targets. Security aspects such as the presence of security personnel on the ground, the location of nearby police stations, or the presence or absence of CCTV can influence the decisions of those planning an attack.

With this in mind, it may be useful to either increase security, or at least give the impression of increased security on key locations so as to deter a would-be attacker. Likewise, the information regarding the number of people who visit a location strongly influences the decision to select it as a target. To reduce how attractive a target appears to those planning an attack, it would be best to omit this data from websites wherever possible.

These suggestions all work towards influencing aspects of rational choice theory to make terrorist attacks less likely (Clarke & Newman, 2006). In the context of crime, rational choice theory asserts that would-be criminals weigh up the possible costs and benefits of committing a crime prior to actually committing it. This theory is based on an individual's perception of the costs and benefits of an act, and individual's perceptions can be changed. The actions suggested in this chapter all seek to change the perceptions of those involved in terrorism:

- Giving the impression that Internet anonymity services are not effective,
- Providing false information regarding how to make explosive devices (and other potential weapons),

- Making locations appear less attractive to a would-be terrorist, and
- Playing down the impact of terrorist attacks while highlighting their failures.

Specifically, by increasing the perceived cost of an action, while reducing the perceived benefit, some may be turned away from following that course of action.

FUTURE RESEARCH DIRECTIONS

Whilst in its infancy, the use of a red-team design for research investigating how terrorists plan attacks has provided valuable insight into aspects of terrorism, particularly in highlighting how attacks can be planned and conducted, and has the potential to inform how security may be enhanced to reduce the likelihood of a terrorist attack. However, other sources of information regarding how attacks are planned and conducted are also crucial in identifying key aspects of the planning process of terrorist attacks. For example, interviews with those arrested for terrorism offences would certainly provide very valid insight into common aspects of the planning process. This information could also be used to further inform future red-team research designs.

Another example is to investigate the Internet usage habits of past terrorists in various settings around the world, to identify key points that could be used to identify those currently involved. Using information from primary sources such as terrorist interviews and terrorist Internet usage, future red-team designs could be focused on specific aspects of the terrorism attack planning. The results from this research can further highlight aspects of the planning process that can be influenced to reduce the likelihood of an attack occurring, or to reduce the impact of an attack if one is to occur.

CONCLUSION

To conclude, the Internet can be used to facilitate terrorist attacks through obtaining and developing weapons, selecting targets, and supplying reconnaissance. While some argue that terrorists are at a disadvantage using the Internet because of their likelihood to be identified and monitored, it is possible for those involved to either hide their identity entirely, or to make it much more difficult to be identified. The availability of technical and reconnaissance information, and the ability to increase anonymity while using the Internet, will continue to pose a persistent challenge for disrupting terrorism.

Nevertheless, there are many ways (some that we have identified in this chapter) to disrupt and weaken terrorists. Focusing on (1) terrorist's ability to use anonymity services, (2) the reliability of online bomb-making instructions, and (3) altering specific online information about key locations will increase the likelihood of detection while decreasing the likelihood and severity of an attack occurring. While terrorism has been a persistent problem, and is one that is not likely to disappear in the near future, steps can be made to increase the difficulty in conducting attacks, while reducing the effectiveness of those attacks when they occur.

REFERENCES

Antoniades, D., Markatos, E. P., & Dovrolis, C. (2010). MOR: Monitoring and measurements through the onion router. In A. Krishnamurthy & B. Plattner (Eds.), *Passive and active measurement* (pp. 131–140). Berlin: Springer-Verlag. doi:10.1007/978-3-642-12334-4_14

Barnes, B. (2012). Confronting the one-man wolf pack: Adapting law enforcement and prosecution responses to the threat of lone wolf terrorism. *Boston University Law Review. Boston University. School of Law*, *92*, 1613–1662.

Benson, D. C. (2014). Why the Internet is not increasing terrorism. *Security Studies*, *23*(2), 293–328. doi:10.1080/09636412.2014.905353

Brunst, P. W. (2010). Terrorism and the Internet: New threats posed by cyberterrorism and terrorist use of the Internet. In M. Wade & A. Maljević (Eds.), *A war on terror?: The European stance on a new threat, changing laws and human rights implications* (pp. 51–78). New York, NY: Springer. doi:10.1007/978-0-387-89291-7_3

California Department of Forestry and Fire Protection (CAL FIRE). (2012). *A practical test of the 'Ember Bomb' as described in Inspire, Issue 9*. California State Threat Assessment Center.

Chakravarty, S., Portokalidis, G., Polychronakis, M., & Keromytis, A. D. (2011). Detecting traffic snooping in Tor using decoys. In *Proceedings of the 14th International Conference on Recent Advances in Intrusion Detection*. Berlin: Springer. 10.1007/978-3-642-23644-0_12

Clarke, R. V., & Newman, G. R. (2006). *Outsmarting the terrorists*. Westport, CA: Greenwood Publishing Group.

Conway, M. (2006). Terrorism and the Internet: New media - new threat? *Parliamentary Affairs*, *59*(2), 283–298. doi:10.1093/pa/gsl009

Crawford, A. (2007). Crime prevention and community safety. In M. Maguire, R. Morgan, & R. Reiner (Eds.), *The oxford handbook of criminology* (4th ed.; pp. 866–909). Oxford, UK: Oxford University Press.

Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The second-generation onion router*. Washington, DC: Naval Research Lab.

Edman, M., & Yener, B. (2009). On anonymity in an electronic society: A survey of anonymous communication systems. *ACM Computing Surveys*, *42*(1), 1–35. doi:10.1145/1592451.1592456

France attack: Van driven into shoppers in Nantes. (2014, December 23). *BBC News*. Retrieved from http://www.bbc.com/news/world-europe-30583390

Gracie, C. (2014, July 16). The knife attack that changed Kunming. *BBC News*. Retrieved from http://www.bbc.com/news/world-asia-28305109

Jansen, R., Tschorsch, F., Johnson, A., & Scheuermann, B. (2014). *The sniper attack: Anonymously deanonymizing and disabling the Tor Network*. Arlington, VA: Office of Naval Research.

Keene, S. D. (2011). Terrorism and the Internet: A double-edged sword. *Journal of Money Laundering Control*, *14*(4), 359–370. doi:10.1108/13685201111173839

Kenney, M. (2010). Beyond the Internet: Mētis, techne, and the limitations of online artifacts for Islamist terrorists. *Terrorism and Political Violence*, *22*(2), 177–197. doi:10.1080/09546550903554760

Larsson, S., & Svensson, M. (2010). Compliance or obscurity? Online anonymity as a consequence of fighting unauthorised file-sharing. *Policy and Internet*, *2*(4), 77–105. doi:10.2202/1944-2866.1044

Larsson, S., Svensson, M., de Kaminski, M., Rönkkö, K., & Olsson, J. A. (2012). Laws, norms, piracy and online anonymity: Practices of de-identification in the global file sharing community. *Journal of Research in Interactive Marketing*, *6*(4), 260–280. doi:10.1108/17505931211282391

Melbourne shooting: Man being investigated over terrorism shot dead after stabbing police officers outside Endeavour Hills police station. (2014, September 24). *ABC News*. Retrieved from http://www.abc.net.au/news/2014-09-23/one-person-shot-dead-two-stabbed-endeavour-hills/5764408

Mueller, J. (2010). Assessing measures designed to protect the homeland. *Policy Studies Journal: the Journal of the Policy Studies Organization*, *38*(1), 1–21. doi:10.1111/j.1541-0072.2009.00341.x

Mullins, S. (2011). Islamist terrorism in Australia: An empirical examination of the 'Home grown' threat. *Terrorism and Political Violence*, *23*(2), 254–285. doi:10.1080/09546553.2010.535717

Murdoch, S. J., & Danezis, G. (2005). *Low-cost traffic analysis of TOR*. Paper presented at the 2005 IEEE Symposium on Security and Privacy, Oakland, CA. 10.1109/SP.2005.12

Nesser, P. (2008). Chronology of jihadism in Western Europe 1994–2007: Planned, prepared, and executed terrorist attacks. *Studies in Conflict and Terrorism*, *31*(10), 924–946. doi:10.1080/10576100802339185

Rescorla, E. (2008). *Notes on P2P blocking and evasion*. IETF P@P Infrastructure Workshop (P2Pi). Retrieved from http://64.170.98.42/area/rai/trac/raw-attachment/wiki/PeerToPeerInfrastructure/27 rescorla-p2pi.pdf

Romyn, D., & Kebbell, M. R. (2013). Terrorists' planning of attacks: A simulated 'red-team' investigation into decision-making. *Psychology, Crime & Law*, *20*(5), 480–496. doi:10.1080/1068316X.2013.793767

Romyn, D., & Kebbell, M. R. (2015). *Use of Internet to inform terrorist target selection*. Australia: Griffith University.

Schneier, B. (2007). Did NSA put a secret backdoor in new encryption standard? *Wired*. Retrieved from http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115

Segell, G. M. (2006). Terrorism on London public transport. *Defense and Security Analysis*, *22*(1), 45–49. doi:10.1080/14751790600577132

Soghoian, C. (2010). Caught in the cloud: Privacy, encryption and government back doors in the Web 2.0 era. *Journal on Telecommunications & High Technology Law*, *8*, 359–423.

Spaaij, R. (2010). The enigma of lone wolf terrorism: An assessment. *Studies in Conflict and Terrorism*, *33*(9), 854–870. doi:10.1080/1057610X.2010.501426

Thomas, T. L. (2003). Al Qaeda and the Internet: The dangers of 'cyberplanning'. *Parameters*, *33*(1), 112–123.

Tor Project. (n.d.). Retrieved from https://www.torproject.org/index.html.en

Torres-Soriano, M. R. (2012). The vulnerabilities of online terrorism. *Studies in Conflict and Terrorism*, *35*(4), 263–277. doi:10.1080/1057610X.2012.656345

United Nations Office on Drugs and Crime (UNODC). (2012). *The use of the internet for terrorist purposes*. Retrieved from http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

Urbas, G., & Choo, K. R. (2008). *Resource materials on technology-enabled crime (Technical and Background Paper no.28)*. Canberra: Australian Institute of Criminology.

West, B., & Stewart, S. (2010). Uncomfortable truths and the Times Square attack. *Stratfor*. Retrieved from https://www.stratfor.com/weekly/20100505_uncomfortable_truths_times_square_attack

ENDNOTE

1. High explosives burn rate is between 4,000 and 8,000 meters per second, while low explosives burn rate is around 500 meters per second.

This research was previously published in Combating Violent Extremism and Radicalization in the Digital Era edited by Majeed Khader, Loo Seng Neo, Gabriel Ong, Eunice Tan Mingyi, and Jeffery Chin; pages 91-105, copyright year 2016 by Information Science Reference (an imprint of IGI Global).

Chapter 15
JPSC KP:
Joint Public Safety Cell App

Abu Baker
KP Information Technology Board, Pakistan

ABSTRACT

Advancement in technology has facilitated humans in various ways. However, the phenomenon has negative strain, too, in the form of weaponry and transport and communication technologies that have accelerated the momentum and broadened the spectrum of terrorist activities. Kidnappings, bomb blasts, vandalisms, target killings, physical harassments, etc. are a few of the various bad practices a racket or terrorist organization resorts to, to satisfy its thirst for blood and money. Some even resort to making extortion demands and threat calls to raise their finances and spread terror, respectively. These activities have become difficult to trace with the use of burner phones, outstation phone calls, and calls from unregistered service identity module (SIMs). Given this scenario, the proposed Joint Public Safety Cell app is intended to assist the general public in efficient registration of a complaint, and keeping updates of security forcers' action on their complaint. Details of JPSC app have been discussed in the chapter.

INTRODUCTION

Human vulnerability to terror has never appeased over the centuries. With the advancement in science and technology, terrorist activities and their perpetrators have rather gained momentum. On one hand, progress in science and technology has made living easier. On the other hand, the very advances in science and technology have been responsible for introduction of newer and undetectable criminal maneuvers

DOI: 10.4018/978-1-7998-2535-7.ch015

and terrorist activities. Guns, carbines, rifles, rocket launchers, explosives, all-terrain vehicles have traditionally been favorite tools of groups with anti-humanity mindset (Popular Mechanics, 2018). Advances in mobile technology have worked like fuel to fire. These have catalyzed smart planning, coordination and execution of terrorist activities world-wide.

Terrorist activities are carried out with a sinister aim to spread terror and cause subsequent social anomaly, something which these pernicious organizations and groups have achieved with quite a felicity, especially in Pakistan. These include contract killing, kidnapping for ransom, extortion demands and threat calls. Use of burner phones (Satzman, 2016), unregistered SIMs, and outstation calls are the some of the mobile phone-facilitated tactics terrorists use to get away with their gory games, uncaught. To make the matters worse, the same technology is also being used to achieve forced financing of these groups in the form of extortion demands and threat calls, as like any organization, their survival depends on money.

Keeping in view the above facts, JPSC KP App has been designed and developed to clamp down on extortionist and terrorists. Working two-way, the app is intended to help the Pakistan army and police departments in containing the terrorist groups and their eerie activities. The main aim of developing this system is to provide meaningful assistance to the people who fall victim to extortionists and terrorists. This android app with web based application is an online platform, easily available to everyone. When a person wants to complain he/she has to provide some basic information such as name, address, phone number and CNIC number, call type, content of threats, terrorist contact numbers, organization and brief description. The application also facilitates its user to record a call or a video, and upload video, audio and image files.

Through this app the personal information stores on a centralized server which consists of database. Here the individual information cannot be accessed by a third party except Pakistan army and police department. With the help of provided information the security organizations, Pakistan army and police, can track the terrorist and terrorist groups. It is meant to help thwart incidence of kidnapping, extortion, threat calls and protection money (Ahmadni, 2017).

BACKGROUND

On May 24, 2018, a resident of South Waziristan, Abdullah, lost his life at refusal to pay extortion money to Riaz, another resident of South Waziristan. Local administration is probing the case and has arrested Riaz after confirmation of the pattern of Abdullah's murder (PT, 2018).

On May 26, 2018, another extortion-related story surfaced in Karachi involving alleged involvement of a station house officer (SHO) and two constables in extortion racket. The three officials were subsequently suspended by Deputy Inspector General (DIG), Karachi. An inquiry is being conducted into the matter. A case has also been registered against the accused under Sections 385, 34 and 386 of the Pakistan Penal Code (PPC) and 7-ATA (PT, 2018).

According to police officials, around 70 per cent people, threatened by militants, pay up extortion money without informing any law-enforcement agency. The 30 per cent who show courage to contact law enforcers and take them into confidence, usually do so at second or third extortion demand after having paid up the money once (Ahmad R., 2017). Reports suggest extorting money through threats over phone is one of the major sources of militants or terrorists for inflow of funds.

Similarly threat calls that may not have a connection with extortion demands and may well be called criminal intimidation are another regular mechanism of terrorizing influential members of general public. Such murder and rape threats are routinely directed at lawyers, journalists, social reformers, human rights activists, and conscientious politicians (Something rare in the case of the latter!).

In Sami Shah's words, "The life of an 'advocate' is at risk the moment he takes up a case," (Perspectives, 2018). Similarly, back in 2015, Kiran Nazish complained of women journalists being at greater risk of harassment than men journalists. However, the former hesitate to voice their difficulties out of shame. Therefore, if their male colleagues face similar threats, they receive large coverage. However, whatever one's profession, gender, family background, one is likely to face threats one's speech and actions directly challenge the vested interests of an individual or whole racket involved in underhand activities.

With the advancement in computer and mobile technologies, scientists around the world have come up digital solutions to undermine extortions and terror threats. These include SGSecure app, developed for Singaporeans (Government of Singapore, 2018), SAIP (Système d'alerte et d'information des populations) app downloadable on both: iOS and android, for the people of France (Toor A. 2015), and Safeture, a travel security app for Europeans (Mcintosh L., 2018). Following the suit of technologists abroad, the government of Khyberpakhtunkhwah in conjunction with Pakistan army and KP police has developed a Joint Public Safety Cell app in order to contain growing incidence of extortions and threat calls, favorite ways of pulling funds and terrorizing the masses, respectively. Its use is easy and efficient. It can be installed in any android mobile or smart phone. The app dispenses with all cumbersome red tapes of registering the First Information Report (FIR) and facilitates coordination between both Pakistan army and police department in analyze and investigating a terrorist activity at the complaint of app user.

MOTIVATION

Internet has made this world a global village. With internet, one can get information about everything anywhere in the world sitting in their room. As we know that android is the market leader of mobile phones, there are hundreds and thousands of applications that users can download from Play Store. These range from games to all kinds of big and small applications that could serve as virtual assistants in business, office work, entertainment, education, and so on. However, barely a handful of security based applications are available for people to guide and assist them in terror situations. Through this app, we have tried to propose and develop an android mobile application for terrorist target peoples so that to synchronize the data or the records and give better information about the terrorist and terrorist groups in a better way of life saving. This application will be very much user friendly and will provide rich information.

APPLICATION SCOPE

The project aims to offer numerous facilities in a limited capacity to the user. It provides help to admin and security organizations, Pakistan army and police, to manage and analyze the terrorist activities in a better way. The fundamental motivation behind this project is to interconnect the terrorist target people and Pakistan security organizations in one combined system. This system is utilized to store information over a unified server which comprise of database where the user's data cannot be accessed by a third party, except Pakistan security organizations, army and police departments. This application has different modules which include Report an Incident, Chatting, News and Alerts.

PROBLEM STATEMENT

Currently, a manual system is being by the security forces to ensure public safety. However, like a white elephant the system is difficult to maintain and manage. For general public too it is a headache to first approach a police station or complaint cell, register their complaint in the form of a First Information Report (FIR), and later make frequent visits or calls to the place for updates on their status of their registered complaint. The manual system also involves a lot of paper work and its maintenance for record, rendering investigations all the more cumbersome and slower to carry out. Besides, the records are not secure, nor are stored efficiently. It is always a task to find a file for checking status of investigations vis-à-vis certain complaint/FIR, slowing down investigations, security arrangements, and justice.

The Joint Public Safety Cell (JPSC) app is meant to facilitate the registered user in online registration of a complaint, saving them the labor of travel to a police station or complaint cell for filing First Information Report (FIR). The lifesaving app also provides 24/7 online facility of checking updates on the progress of one's complaint/FIR. The application is easy to download in any android mobile phone or smartphone.

JPSC KP APP SIGNIFICANCE

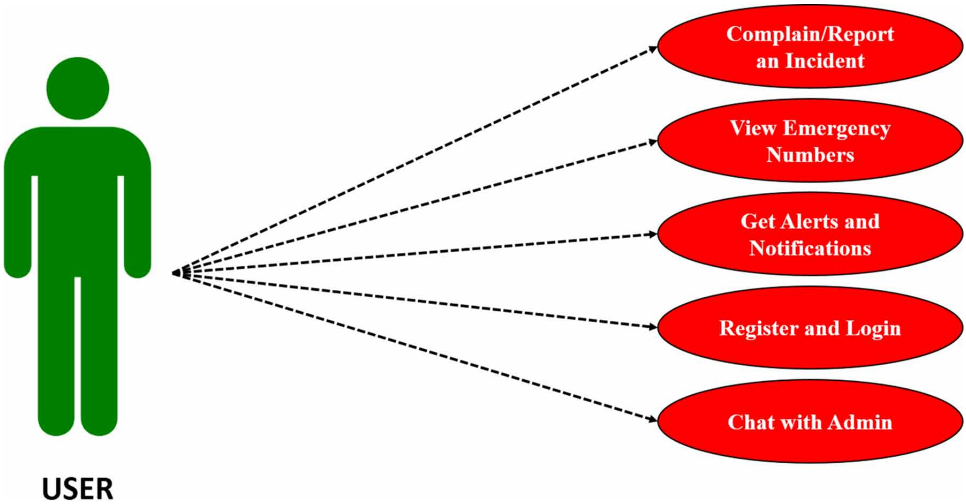
- **Performance:** This system provides quick and up-to-date information about complaint or terrorist incident report. It economizes on user's time and energy for registration of an FIR and checking updates for progress of investigation(s) into the registered complaint, in turn, accelerating the very process of justice and public safety.
- **Usability:** JPSC KP is an easy-to-use app. Its application is absolutely user-friendly and simple.
- **Reliability:** This application boast of accuracy and precision in terms of performance.
- **Error Tolerance and Security:** Errors inside the software are handled internally through the tool used in the development of the software with the interface coding logic Errors are handled in such a way that the user is not interrupted. Security requirements are particularly significant in the defense system and many database systems. Security requirements impose restrictions on the use of certain commands, and controls access to data. Therefore, access to some features of the app has been locked with a password in order to maintain a log of activities in the system (Outhwaite, 2013).

ENTITIES IDENTIFICATION

Following entities are identified in android JPSC KP application:

- Complain about an Incident
- Alerts
- Chat
- Emergency Contacts

Figure 1. Use-case Diagram



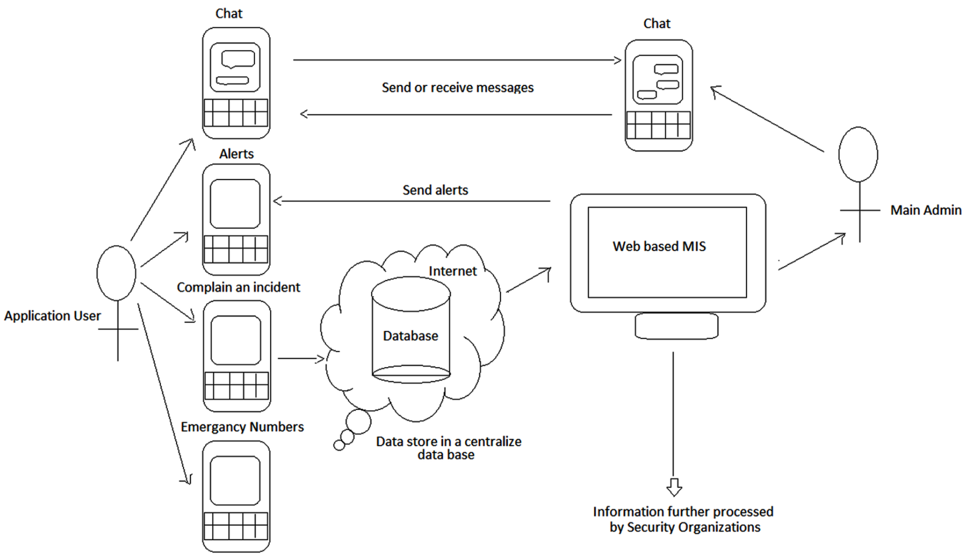
USE-CASE DIAGRAM

Figure 1 specifies that the application user can do all these tasks.

APPLICATION FLOW

All data can be stored in a centralized location on cloud in a centralized data base. After download, the app user registers a complaint about threat calls or extortion attempts, providing all necessary information to the database using JPSC KP ANDROID application. The web based Management Information System (MIS) is used for analyzing and management of all data. The main admin is responsible for overall operations. The data is further processed and investigated by security organizations of Pakistan like Pakistan army and police. The main admin coordinates with the complainant after the latter's registration, which is the next step after filing a complaint. The complainant receives updates on progress of work vis-à-vis their complaint through Short Message System (SMS) alerts. They can also have one-on-one chat with the admin by sending and receiving messages from main admin. They can also view emergency contacts of the Cell to seek urgent help against imminent danger from terrorist. The details of work flow of JPSC KP app shown in Figure 2.

Figure 2. Application Flow of JPSC KP App



MODULES OF JPSC KP APP

Discussion of each and every module of JPSC KP application has been presented in detail in this section. JPSC KP is an android based mobile online app which comprises the following modules.

1. Start Pop-Up

This screen only appears for 5 seconds during which certain background tasks are performed. The application accesses unidentified mobile subscriber identity modules (SIMs) and (IMIs) numbers and registers them in data base. The data is accessed when the user uses the app for the first time. After five seconds the next Home screen appears.

The graphical representation of Start Pop-Up screen is shown in Figure 3.

2. Home Screen of JPSC KP APP

Home screen is the main screen of the application. It presents different options to the app user including filing a complaint, checking alerts, chatting with admin, and accessing emergency numbers. The graphical representation of home screen of JPSC app is shown in Figure 4 below:

Figure 3. Start Pop-Up Screen of JPSC KP APP

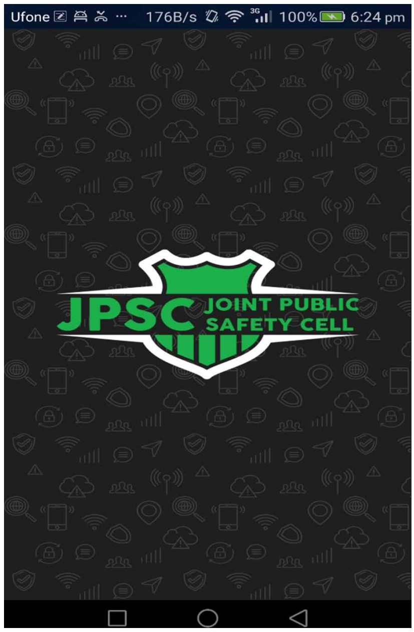
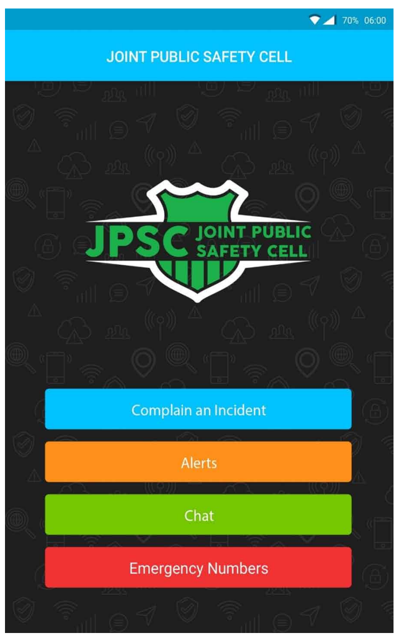


Figure 4. Home Screen of JPSC KP APP



3. Complain an Incident

This is the next screen headed: Report a File. It allows the user to enter necessary details of an incident they want to complain about.

The user is required to give particular such as name, CNIC#, mobile number, address it, type or nature of incident, threat content, the numbers from which threat calls or extortion demands have been made, name of terrorist organization (or individual), and the number of calls received. After submission of this basic information, Joint Public Safety Cell, Pakistan army and Khyberpakhtukhwah police come into action. The graphical representation of complaint filing through JPSC app is shown in Figure 5.

4. Alerts

On this screen the users can find the new events and important alerts from the admin of the apps. The graphical representation of alerts of progress of work on JPSC app user's complaint is shown in Figure 6.

5. Chats

From this screen, the users can send messages to and receive updates from admin (Kilbride & Ray, 2017). The graphical representation of Chat with admin of JPSC app is shown in Figure 7.

6. Registration

This screen allows the JPSC app user to register themselves for chatting with admin. The graphical representation of Registration for Chat on JPSC app is shown in Figure 8.

7. Login

On this screen the users can login themselves for chatting with admin. The graphical representation of Login for Chat on JPSC app is shown in Figure 9.

8. Emergency Numbers

This screen provides the JPSC app user with information on all emergency contacts of the Cell is shown in Figure 10.

Figure 5. Complain an Incident Screen

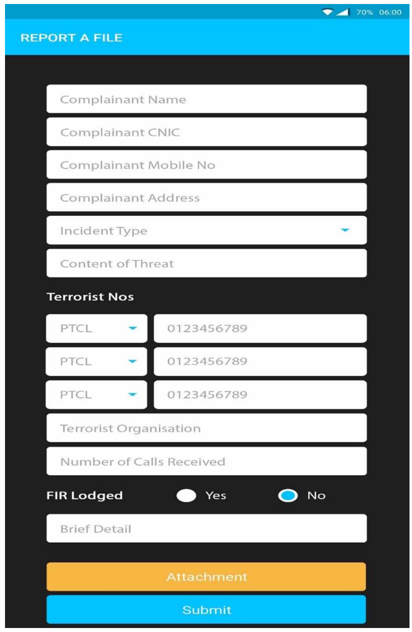


Figure 6. Alerts Screen

Figure 7. Chat Screen

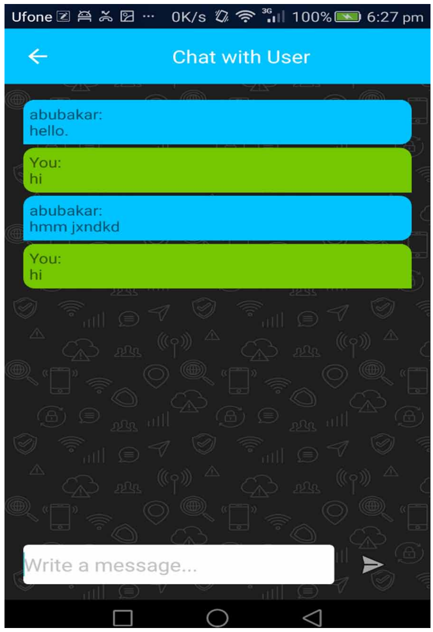


Figure 8. Registration Screen

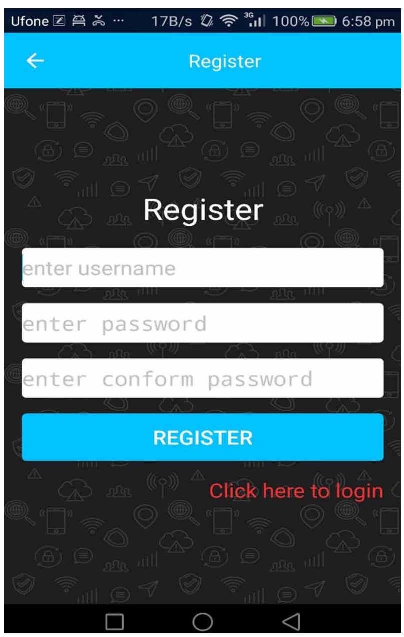


Figure 9. Login Screen

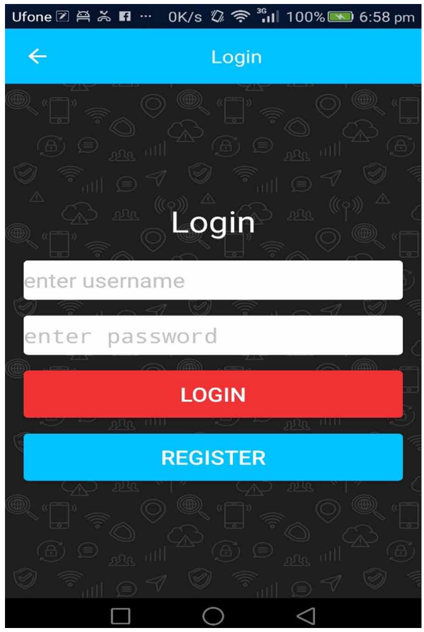


Figure 10. Emergency Numbers Screen

- Helpline number 1425
- By sending text message on 0333-3331425
- Through Whatsapp on 0333-3331425
- Email to jpsc@ publicservicekp.org
- Send letter on PO Box GPO 8 Peshawar

The graphical representation of Emergency Numbers of JPSC app is shown in Figure 10.

SOFTWARE REQUIREMENT

The term requirement means a detailed definition of how a system works. A Software Requirement Specification (SRS) basically defines the requirements. If the requirements are well defined, the design of software flows logically and smoothly. If the requirements are met poorly, the resulting design is awkward and the coding is more difficult.

The software requirement is the phase where the current system is analyzed from various aspects. The manual data that the system has is analyzed after going through all the data of the current system (Capterra, 2017).

1. Functional Requirements.

The functional requirements of the system are as follows:

- Filing a complain.
- User Login.
- Registration of user.
- Changing personal contact details by application user.
- Receiving a notification of important event or updates on progress of work on the user's complaint by concerned security agencies (Kilbride & Ray, 2017).

2. Non-Functional Requirements.

Nonfunctional requirements specify how the system should behave. It is a constraint upon the systems behavior. These are the remaining requirements not covered by the functional requirements. They specify criteria that judge the operation of a system rather than specific behavior. They may include constraints on the services or functions offered by the system such as timing constraints, constraints on the development process and standards etc.

TOOLS AND TECHNIQUES

Here is the list of tools and equipment which have been used to develop the proposed system:

- Android Studio
- Visual Studio
- JavaScript (scripting)
- Microsoft word
- Microsoft power point
- MS Project
- Adobe Photoshop

HARDWARE ENVIRONMENT

The hardware Environment in which the system was developed includes:

1. **Operating System:** Windows operating system and android operating system.
2. **CPU:** Intel Core 2 Duo 2GHz, AMD Athlon 64 X2 2GHz.
3. **Memory:** 4 GB RAM.
4. **Windows and Android Studio** is the environment in which the system is developed.

APPLICATION LIMITATIONS

Following are the JPSC KP App limitations:

- **Internet Connection Failure:** JPSC KP app is an online mobile application. Availability of internet connection and signals is a must for its smooth functioning. In case of internet connection failure, the application stops working.
- **Platform Dependent:** JPSC KP app is platform dependent and only runs on android devices. Other mobile operating systems like IO'S and Window phones do not support this application.
- **Centralized Database:** All data of this application are stored at centralized location in a server in a single database. If that system gets corrupted then all the data will be lost.

FUTURE DIRECTIONS

This app is only used for controlling extortion and threats call. In future, its gambit may be expanded to include other complaints in different departments like courts, police, army, post office and agriculture.

If any country requires our software for use to benefit its people, then it is available free of cost, because our aim of making this software is to provide an easy and efficient way to help the terror-stricken people where they be.

CONCLUSION

This JPSC KP system application is a useful mobile application, developed purely to serve the masses sick of extortion demands and threat calls from terrorist groups. It has been designed to save the app user the trouble of travelling to a police station of their jurisdiction, and under various red-tapes with headachy plethora of paperwork to register an FIR. It also saves them the headache of visiting the police station for updates on progress of work on their complaint. The app coordinates communication between the app user and the joint cell of Pakistan army and KP police to curb incidence of extortion and threat calls from terrorist groups. Users could be registered. Online complaint and updates on progress of necessary subsequent action save lots of time, and is expected to block finances of terrorist organizations. Since the entire system is computerized, the record of registered users can be maintained for longer duration of time. This system is user-friendly. Anyone can access it anytime through mobile. This application can be modified in future in order to make it more efficient and effective.

REFERENCES

Ahmad, R. (n.d.). Most people pay up extortion: police. *The Express Tribune*. Retrieved on June 9, 2018 from https://tribune.com.pk/story/1323123/people-pay-extortion-police/

Ahmadni, A. (2017). *Joint public safety cell to keep KP safe from extortion*. Retrieved on June 11, 2017 from https://www.pakistantoday.com.pk/2017/05/25/joint-public-safety-cell-to-keep-kp-safe-from-extortion/

Kilbride, K., & Ray, T. (2017). *Intuitive and Beautiful Project Planning*. Retrieved on July 23, 2017 from http://www.teamgantt.com/

Nazish, K. (2015). Threats to Pakistan's Women Journalists. *The New York Times*. Retrieved on June 9, 2018 from https://kristof.blogs.nytimes.com/2015/10/23/threats-to-pakistans-women-journalists/

Outhwaite, A. (2013). *4 steps to design & prototype a better business model*. Retrieved on June 10, 2017 from http://pollinators.org.au/2013/10/18/4-steps-better-business-model/

Popular Mechanics. (2018). *Military News - Latest Military Technology and Advancements*. Retrieved on June 9, 2018 from https://www.popularmechanics.com/military/

Shah, S. (2018). Who will protect the lawyers? *Daily Times: Perspectives*. Retrieved on June 9, 2018 from https://dailytimes.com.pk/203347/will-protect-lawyers/

Toor, A. (2015). *France launches terror alert app ahead of Euro 2016 tournament*. Retrieved on June 9, 2018 from https://www.theverge.com/2016/6/8/11881732/france-terrorism-alert-euro-2016-app

ADDITIONAL READING

Capterra, (2017). Requirements Management Software. Retrieved on June 10, 2017 from http://www.capterra.com/requirements-management-software/

Desouza, K. C., & Bhagwatwar, A. (2012). Citizen apps to solve complex urban problems. *Journal of Urban Technology*, *19*(3), 107–136. doi:10.1080/10630732.2012.673056

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491–497. doi:10.1016/j.jare.2014.02.006 PMID:25685517

Government of Singapore. (2018). SGSecure: Home. Retrieved on June 9, 2018 from https://www.sgsecure.sg/

Hickman, M. J. (2006). *Citizen complaints about police use of force*. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

Lentin, A., & Humphry, J. (2017). Antiracism apps: Framing understandings and approaches to antiracism education and intervention. *Information Communication and Society*, *20*(10), 1539–1553. doi:10.1080/1369118X.2016.1240824

Obiodu, V., & Obiodu, E. (2012). An empirical review of the top 500 medical apps in a European Android market. *Journal of Mobile Technology in Medicine*, *1*(4), 22–37. doi:10.7309/jmtm.74

Pakistan Today. (2018). Man gunned down in South Waziristan for 'refusing to pay extortion money'. Retrieved on June 9, 2018 from https://www.pakistantoday.com.pk/2018/05/24/man-gunned-down-in-south-waziristan-for-refusing-to-pay-extortion-money/

Roundupreviews. (2017). Measuring Project Risk. Retrieved on July 24, 2017 from http://roundupreviews.com/us/measuring%20project%20risk

Saltzman, M. (2016). Why you might want to own a 'burner phone'. Retrieved on June 9, 2018 from https://www.usatoday.com/story/tech/columnist/saltzman/2016/09/17/whats-a-burner-phone/90382874/

Seo, S. H., Gupta, A., Sallam, A. M., Bertino, E., & Yim, K. (2014). Detecting mobile malware threats to homeland security through static analysis. *Journal of Network and Computer Applications*, *38*, 43–53. doi:10.1016/j.jnca.2013.05.008

Smith, S. K., Steadman, G. W., Minton, T. D., & Townsend, M. (1999). Criminal victimization and perceptions of community safety in 12 cities, 1998. NCJ, 173940.

Whipple, J., Arensman, W., & Boler, M. S. (2009, October). A public safety application of GPS-enabled smartphones and the android operating system. In Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on (pp. 2059-2061). IEEE.

KEY TERMS AND DEFINITIONS

App User: End user, which runs this application on a mobile phone, with personal interest.

Extortion: Is a criminal offense of obtaining money, property, or services from an individual.

Extortionists: Is the illegal use of one's official position or powers to obtain property, funds, or patronage.

FIR: First information report, report a crime to police.

Human Right App: Those applications which are used for protection of human rights.

Incident Complaint: A complaint to security organization from terrorist activities.

JPSC: Joint Public Safety Cell is the combined effort between Pakistan Army and Khyber Pakhtoon Khwa (KP) Police departments to controls threats call and extortions.

JPSC KP: It is an android application Joint Public Safety Cell to control threats and extortion in Khyber Pakhtoon Khwa, Pakistan.

Kidnapping: The unlawful act of capturing and carrying away a person against their will and holding them in false imprisonment.

Protection Money: Money paid to secure protection.

Report Khyberpakhtunkhwa (KP) Police: A crime FIR lodged with KPK police.

Threat Call: A warning call from terrorists.

Threat Call Report: A threat call FIR lodged to police department.

This research was previously published in Mobile Devices and Smart Gadgets in Human Rights edited by Sajid Umair and Muhammad Yousaf Shah; pages 27-45, copyright year 2019 by Information Science Reference (an imprint of IGI Global).

Chapter 16
Resources in Parks and Police Management Applying Decision Utility to Solve Problems With Limited Resources

Ceyhun Ozgur
Valparaiso University, USA

ABSTRACT

This is the first research article that attempts to relate public service to managing an organization and explains systems with realistic yet simplistic examples. This article is the first of its kind to relate public service to managing organizations that relate public service such as parks and police. It measures and implements maximin value functions. A maximin value function applies when the criteria are totally non-substitutable: a decrease in a critical criterion cannot be compensated for by an increase in another criterion. This article illustrates situations where a maximin value function is an appropriate model, develops a method to measure a decision maker's maximin value function, and demonstrates how a maximin value function can be used in applications such as park and police systems. The measurement technique is easy to understand and most decision makers can complete the process in a short period of time. For quantitative scheduling techniques found in journals, their wider use in applications has been declining due to a variety of obstacles. This article will first list a number of these obstacles and then suggest ways to overcome them. Parks and Police departments are government agencies that both have limited and competing resources. In these circumstances, it is an ideal situation to share the resources as much as possible. In this article, examples are shown of where the limited resources

DOI: 10.4018/978-1-7998-2535-7.ch016

may occur in both agencies, and how the manager may overcome these problems by sharing the resources. Examples of affective and just sharing of resources are given for both parks and police departments. In Parks Management, affective trade-offs are shown among trim mowing, tractor mowing, garbage collection and ball-field dragging. In Police departments affective trade-offs are shown among foot patrol, car patrol, detective analysis and office work.

INTRODUCTION

Let us begin with a situation encountered in 1972 by a researcher in devising a computerized quantitative production scheduling system for a tire production plant. The schedule produced by the system was constrained by the machines available, the sequencing of the machines for each type of job, the flow of materials, the demand of make to order jobs, the demand of make to stock jobs, the job due dates, and the personnel available. The corporate MIS department commissioned the system which was designed to be updated on their update computer more than once a week. After the system was completed, the MIS department said the system was a success because it demonstrated to the company that the computer could be used to schedule production which was the entire purpose of the project. After much thought, there were many reasons for the non-implementation. (1) Job control: the production schedulers did not want the MIS department to take control. Basically, they did not want someone else doing even part of their job. (2) Efficient schedule: the production schedulers felt that a computer program could never produce a schedule as efficient as their own and the company had the potential to lose money. (3) Short term priority changes: the computer schedule could not respond to short term changes in the priorities such as marketing or corporate headquarters requesting that a particular customer receive top priority today. (4) Tradeoffs: Production schedulers did not agree with the suggested schedule and more importantly did not know how the computer schedule that made the myriad of tradeoffs necessary to produce a schedule. For example, a production schedule must tradeoff decreasing total setup time versus increasing the chance that some due dates will not be met. In addition, if all due dates cannot be met, the computer schedule internally chooses which jobs are late and the production schedulers may not agree with the tradeoffs used to make that choice. (5) Preference and knowledge input: the computer schedule did not reflect the preferences and knowledge of the production schedulers or any other department such as marketing. (6) Using the computer schedule as a tool: most production schedulers don't understand or even want to understand how the quantitative scheduling algorithm determines the computer schedule. Therefore, any real or perceived problem with the computer schedule is cited as proof that the quantitative scheduling algorithm should be scrapped as it is clearly inferior to a schedule produced by a production scheduler. In other words, a production scheduler is not trained to use the computer schedule as tools to help them do their job but instead view it as a competitor. (7) Incomplete information: the data used to produce the computer schedule did not completely mirror the real world situation and by necessity left out some information including political nuances. Thus, any computer schedule will usually be seen by someone as having serious shortcomings

PRIORITY CLASS SCHEDULING

Most of the problems listed above are present in all applications of quantitative scheduling techniques but there has been very little work in literature to try and solve these problems. One study by (Brown and Ozgur, 1997) suggested using priority class scheduling to reduce due date conflicts between marketing and the production schedulers by replacing due dates with production periods and priority classes. The priority classes are used by the production scheduler as constraints on what can be scheduled in a production period. If any job in priority class i is started in the production period, then all jobs in priority class i-1 must be completed within the production period. This is the only constraint on the production scheduler and allows the scheduler to concentrate on optimizing manufacturing efficiency within the production period. The constraint is so simple that its consequences are easily understood by those who assign jobs to priority classes but at the same time allows manufacturing some flexibility in scheduling. Indeed, the production scheduler can schedule a priority three job to be completed early in the production period as long as all priority one and priority two jobs are completed within the production period. In addition, if only some priority three jobs can be completed in the production period, the selection of which jobs to produce is made entirely on the basis of production efficiency. This gives some flexibility to manufacturing to optimize production efficiency. Indeed, the production scheduler only considers the priority classes when scheduling and does not even need to know the due dates of the jobs. This means that marketing alone without any help from the production schedulers could determine the priority class for each job and let the production schedulers concentrate on increasing production efficiency. Theoretically, priority class scheduling would greatly reduce the conflict between marketing and manufacturing. However, getting the production schedulers to agree to even try priority class scheduling would be very difficult because of some of the problems listed above. The production schedulers would perceive a loss of job control because they would feel that marketing would be dictating their jobs to them. With marketing in control of the "due dates," manufacturing would think that getting an efficient schedule would be impossible and the company would lose money. Short term physical changes could cause the violation of the priority class scheduling rules. For example, suppose a priority class 3 job was lumped together with a priority class 1 job early in the production period to reduce setup time and cost. If later in the production period a machine broke down and caused a priority class 2 job to not be run, then at the end of the production period, a priority class 3 job was completed while a priority class 2 job was not completed. This is a clear violation of the idea of priority classes. The production schedulers would be blamed for the violation and marketing would be furious.

SCHEDULING PARKS MAINTENANCE

Although many quantitative scheduling techniques are designed for production scheduling, other types of scheduling problems have been studied but they have some of the same obstacles listed above for production scheduling. For example, consider the problem of scheduling jobs in a governmental agency where the amount of work to be done almost always exceeds the resources available. In this case, the scheduling problem is deciding how much of each job to do and not do given the amount of resources on hand. Anderson and Brown (1978) devised the Parks Maintenance Management System (PMMS), a quantitative parks maintenance scheduling system that avoided some but not all of the obstacles listed above. Using the resources available (mainly personnel and machines), parks maintenance must determine how much of each job to do to keep the parks in as good condition as possible. For example, in the summer, a parks maintenance district must tradeoff how the number of times jobs like tractor mowing (mowing large open areas), trim mowing (mowing small areas around trees, sidewalks, buildings, etc.), litter removal, and ball field dragging are done in each park. The main problem is to determine the correct balance between the jobs given the resources available. This is clearly a case where a balance is necessary because doing a lot of litter removal and ball field dragging while doing no mowing would not be acceptable to the tax payers. For each parks district and scheduling period, the PMMS used as data a list of the parks, estimates of the time for a parks maintenance crew to complete each job in each park, the personnel and equipment available, and what personnel and equipment that constituted a parks maintenance crew for each job. In addition, the model was driven by a maximin value function collected from the parks maintenance management that showed what they considered the best balance of the jobs at various levels of resources. For example, they might feel that for a low level of resources, relatively more mowing should be done while for a higher level of resources, the amount of litter removal and ball field dragging relative to mowing should be increased. A computer schedule was run every two weeks and gave a district maintenance supervisor an amount of each job the district could accomplish in the next two weeks with the resources predicted to be available. This computer schedule represented the best balance between the jobs as it maximized the maximin value function given the resource constraints. A very simple example will be used to illustrate PMMS. Suppose a parks manager (PM) is trying to decide how many times the jobs trim mowing, tractor mowing, litter removal, and ball field dragging should be completed this summer for the parks in his district. First, the PM's perfect complements preference structure is determined by having him complete a table. Table 1 contains a completed table where initially the Desirable Quantity column as well as columns 1, 2, 3, 4, and 6 are empty except for the Totals and UTILITY rows. The PM is asked to give how many times each job should be done to keep the parks in good condition (these amounts should represent the upper end of the PM's range of interest). The PM's response is shown in the Desirable Quantity column of Table 1. Next the PM is asked to complete column 1 with percentages of the corresponding desirable quantity that sum to 80. The response of 10 for trim mowing corresponds to 10 percent of the desirable quantity of 20 or 2 trim mowings. These percentages reflect the PM's tradeoffs between the four attributes and contain what he considers the best balance between them given the percentages can only sum to 80. The attribute values corresponding to the percentages in column 1 are 2 trim mowings, 10 tractor mowings, 2 litter removals, and 0 ball field draggings over the summer. These attribute values are then entered in column 1 of Table 2. In a similar manner, the PM then fills in columns 2, 3, 4, and 6 so the percentages for each column sum to the amount listed in the Totals row. Finally, the attribute values corresponding to the percentages are entered in the appropriate columns in Table 2. This collects data on what the PM thinks is the best balance between the attributes over a range from doing nothing (column 0) to the desirable quantities (column 5) and beyond (column 6).

Table 1. Constrained Choice Table for Parks Maintenance Example

	DESIRABLE	**PERCENT OF DESIRABLE QUANTITY**						
ATTRIBUTES	**QUANTITY**	**0**	**1**	**2**	**3**	**4**	**5**	**6**
1.Trim Mowing	20 Mowings	0	10	40	50	80	100	100
2.Tractor Mowing	20 Mowings	0	50	70	90	100	100	100
3.Litter Removal	10 Removals	0	20	50	80	90	100	120
4.Ballfield Dragging	100 Draggings	0	0	0	20	50	100	160
	Totals	0	80	160	240	320	400	480
	UTILITY	**0**	**20**	**40**	**60**	**80**	**100**	**120**

Table 2. Attribute Value Table for Parks Maintenance Example

	LABOR	**ATTRIBUTE VALUES**								
ATTRIBUTE	**HOURS**	**0**	**1**	**2**			**3**	**4**	**5**	**6**
1.Trim Mowing	50	0	2	8	8.8	9.6	10	16	20	20
2.Tractor Mowing	40	0	10	14	15.6	17.2	18	20	20	20
3.Litter Removal	150	0	2	5	6.2	7.4	8	9	10	12
4.Ballfield Dragging	10	0	0	0	8	16	20	50	100	160
TOTAL LABOR HOURS		0	800	1710	**2074**	**2438**	2620	3450	4300	5200
UTILITY		**0**	**20**	**40**	48	56	**60**	**80**	**100**	**120**

Since each column in Table 2 is a point in the attribute value space, a linear line between these points approximate what the PM considers the best balance over the entire attribute value space. To keep it simple, suppose the only limiting resource needed to accomplish the jobs is labor measured in hours. The PM estimates that one trim mowing requires 50 labor hours, one tractor mowing requires 40 labor hours, one litter removal requires 150 labor hours, and one ball field dragging requires 10 labor hours. These estimates are entered in the LABOR HOURS column of Table 2. The labor hours needed to accomplish the attribute values in columns 0, 1, 2, 3, 4, 5, and 6 are computed and entered in the TOTAL LABOR HOURS row. Suppose the PM has 2074 labor hours available this summer. Then the amounts of each attribute that provides the best balance while using no more than 2074 labor hours can be found by linear interpolation in Table 2. From Table 2, the best balance is 8.8 trim mowings, 15.6 tractor mowings, 6.2 liter removals, and 8 ball field dragging for a utility of 48. Note that a non-integer amount such as 8.8 trim mowings is acceptable because that means every park would be trim mowed 8 times and get 80 percent of the way through the ninth trim mowing.

The PM can easily understand how the quantitative scheduling algorithm determines the schedule. In addition, "what if" questions can now be answered. Suppose city council asked the Parks Department what it could accomplish if the labor hours were increased from 2074 to 2438. Using linear interpolation, Table 2 shows that 2438 labor hours would increase the trim mowing from 8.8 to 9.6, increase tractor mowing from 15.6 to 17.2, increase litter removal from 6.2 to 7.4, and increase ball field dragging from 8 to 16. PMMS also collected data on how much of each job was accomplished in the preceding two week period. Although this actual job performance data was compared to what the computer schedule predicted could be done, it was not used in a punitive fashion but rather as a starting point for discussion of what changes would enable the parks department to do a better job of serving the public. The objective was to instill pride in the parks maintenance personnel and to motivate them into making continual improvements. By design and by enlightened management, PMMS avoided many of the obstacles listed above. PMMS avoided the job control obstacle as parks maintenance management viewed the computer schedule as simply a starting point and was free to change it as conditions warranted. In addition, the computer schedule only gave the amounts of each job that could be accomplished and did not tell a manager what personnel should be assigned to which crew or, like priority class scheduling, when the jobs should be done within the period. The managers were free to devise their own work schedule within the computer schedule framework so they were motivated to design an efficient schedule and could not blame any inefficiencies on the computer schedule. The managers were also free to respond to both short term physical changes and priority changes as they saw fit. The preference and knowledge input obstacle and the tradeoffs obstacle were, for the most part, avoided by using the maximin value function supplied by the parks maintenance management to drive the determination of the computer schedule. For the obstacle regarding using the computer schedule as a tool, every effort was made to enable parks management to accomplish this but was limited by the fact that the computer schedule was only produced once every two weeks and the parks maintenance managers could not use it to ask "what if" questions. In addition, although there was some minimal training on how the quantitative scheduling algorithm worked, hindsight says that more effort should have been directed into training. Finally, as with all applications of quantitative scheduling techniques, the incomplete information obstacle was present. As it was applied to parks management, another example was given by the author in a separate journal article regarding the scheduling of police work by using maximin value function, an article written by Ozgur and Brown (2012).

MAXIMIZING EFFICIENCY AND BALANCING WORK LOAD FOR POLICE STATION

Although many quantitative scheduling techniques are designed for production scheduling, other types of scheduling problems have been studied but have some of the same obstacles listed above for production scheduling. For example, consider the problem of scheduling police officers in a police department where the amount of work to be done almost always exceeds the resources available in a given time period such as summer months. In this case, the scheduling problem is deciding how much of each type of job to do and still protect the public and ensure public safety given the amount of resources on hand for the entire summer months. For each police scheduling period, the police chief used as data a list of the police officers, estimates of the time for a police officer or police car to complete each job in the city, and what additional personnel and equipment was available and needed by the police department for each police activity. In addition, the model was driven by a maximin value function collected from the police department that showed what the police chief considered the best balance of the jobs at various levels of resources. For example, they might feel that for a low level of resources, relatively more patrol, either foot or car patrol should be done while for a higher level of resources, the amount of detective analysis and office work should be preferred over foot patrol or car patrol. A computer schedule was run every two weeks and gave the police chief or the police supervisor an amount of each job the city could accomplish in the next two weeks with the resources predicted to be available. This computer schedule represented the best balance between the jobs as it maximized the maximin value function given the resource constraints (Brown, J.R., & Ozgur, C., 2011). A very simple example will be used to illustrate police scheduling. Suppose the police chief or the police supervisor is trying to decide how many times the detective analysis or the office work will be done in lieu of foot patrol or car patrol. The decision should be how much foot or car patrol should be completed in lieu of office work or detective analysis in a period in his district. First, the police chief's perfect complements preference structure is determined by having him or her complete a table. Table 3 contains a completed table where initially the Desirable Quantity columns, as well as columns 1, 2, 3, 4, and 6 are empty except for the Totals and UTILITY rows. The police chief is asked to give how many times each job should be done to keep the city, and its streets or roads safe in good condition (these amounts should represent the upper end of the police chief's range of interest). The police chief's response is shown in the Desirable Quantity column of Table 3. Next the police chief is asked to complete column 1 with percentages of the corresponding desirable quantity that sum to 80. The response of 10 for foot patrol corresponds to 10 percent of the desirable quantity of 20, or 2 foot patrols. These percentages reflect the police chief's tradeoffs between the four attributes and contain what he/she considers the best balance between them given the percentages can only sum to 80. The attribute values corresponding to the percentages in column 1 are 2 foot patrols, 10 car patrols, 2 detective analyses, and 0 office works over the entire summer. These attribute values are then entered in column 1 of Table 4. In a similar manner, the police chief then fills in columns 2, 3, 4, and 6 so the percentages for each column sum to the amount listed in the Totals row. Finally, the attribute values corresponding to the percentages are entered in the appropriate columns in Table 4. This collects data on what the police chief thinks is the best balance between the attributes over a range from doing nothing (column 0) to the desirable quantities (column 5) and beyond (column 6).

Table 3. Constrained Choice Table for City Police Departments

	DESIRABLE	PERCENT OF DESIRABLE QUANTITY						
ATTRIBUTES	**QUANTITY**	**0**	**1**	**2**	**3**	**4**	**5**	**6**
1.Foot Patrol	20 Officers	0	10	40	50	80	100	100
2.Car Patrol	20 Cars	0	50	70	90	100	100	100
3.Detective Analysis	10 Detectives	0	20	50	80	90	100	120
4.Office Work	10 Officers	0	0	0	20	50	100	160
	Totals	0	80	160	240	320	400	480
	UTILITY	**0**	**20**	**40**	**60**	**80**	**100**	**120**

Table 4. Attribute Value Table for City Police Departments

	LABOR	ATTRIBUTE VALUES								
ATTRIBUTE	**HOURS**	**0**	**1**	**2**			**3**	**4**	**5**	**6**
1.Foot Patrol	80	0	2	8	8.53	9.04	10	16	20	20
2.Car Patrol	40	0	10	14	15.05	16.08	18	20	20	20
3.Detective analysis	100	0	2	5	5.79	6.56	8	9	10	12
4.Office Work	40	0	0	0	5.27	10.39	20	50	100	160
TOTAL LABOR HOURS		0	760	1700	**2074**	**2438**	3120	4980	7400	10000
UTILITY		**0**	**20**	**40**	46	50	**60**	**80**	**100**	**120**

Since each column in Table 4 is a point in the attribute value space, a linear line between these points approximate what the police chief considers the best balance over the entire attribute value space. To keep it simple, the only limiting resource needed to accomplish the jobs is labor measured in hours. The police chief estimates that one foot patrol requires 80 labor hours, one car patrol requires 40 labor hours, one detective analysis requires 100 hours, and one office work requires 40 labor hours. These estimates are entered in the LABOR HOURS column of Table 4. The labor hours needed to accomplish the attribute values in columns 0, 1, 2, 3, 4, 5, and 6 are computed and entered in the TOTAL LABOR HOURS row. Suppose the police chief has 2074 labor hours available this summer. Then the amount of each attribute that provides the best balance while using no more than 2074 labor hours can be found by linear interpolation in Table 4. From Table 4, the best balance is 8.53 foot patrol, 15.05 car patrol, 5.79 detective analysis, and 5.27 office work for a utility of 46. Note that a non-integer amount such as 8.53 foot patrol is acceptable because that means every officer would foot patrol 8 times and 1 officer would get only 53% percent of the way through the ninth patrol walk.

This system has many advantages. The police chief preferences are inputted to the model and are used to determine the best amounts of each attribute to accomplish given the resources available. The police chief can easily understand how the quantitative scheduling algorithm determines the schedule. In addition, "what if" questions can be answered in the quantitative algorithm. Suppose the city asked the Police Department what it could accomplish if the labor hours were increased from 2074 to 2438. Using linear interpolation, Table 4 shows that 2438 labor hours would increase the detective analysis from 5.79 to 6.56, increase office work from 5.27 to 10.39, increase foot patrol from 8.53 to 9.04, and increase car patrol from approximately 15 to 16. The police chief also collected data on how much of each job was accomplished in the preceding two week period. Although this actual job performance data could be compared to what the computer schedule predicted could be done, it was not used in a punitive fashion but rather as a starting point for discussion of what changes would enable the police department to do a better job of serving the public. The objective was to instill pride in the police department personnel and to motivate them into making continual improvements. By design and enlightened management, the police chief avoided many of the obstacles listed above. The police chief avoided the job control obstacle as the police department viewed the computer schedule as simply a starting point and was free to change it as conditions warranted. In addition, the computer schedule only gave the amounts of each job that could be accomplished and did not tell the chief what personnel should be assigned to which job or, like priority class scheduling, when the jobs should be done within the period. The chief was free to devise his/her own work schedule within the computer schedule framework so he/she was motivated to design an efficient schedule and could not blame any inefficiencies on the computer schedule. The chief was also free to respond to both short term physical changes and priority changes as he/she saw fit.

The preference and knowledge input obstacle and the tradeoffs obstacle were for the most part avoided by using the maximin value function supplied by the police department to drive the determination of the computer schedule (Brown & Ozgur, 2009). For the obstacle of using the computer schedule as a tool, every effort was made to enable the police department to use the computer schedule as a tool. This was limited by the fact that the computer schedule was only produced frequently and the police department chief could not use it to ask any "what if" questions. In addition, although there was some minimal training on how the quantitative scheduling algorithm worked, hindsight says that more effort should have been directed into training. Finally, as with all applications of quantitative scheduling techniques, the incomplete information obstacle was present. Another model that was used successfully in scheduling is for sequence-dependent set-up products. (Ozgur & Brown, 1995)

OVERCOMING OBSTACLES

Using the discussion above, some strategies and ideas on how to overcome obstacles to the application of quantitative scheduling techniques can now be stated. Probably the most important idea is to make the quantitative scheduling technique accessible to the managers as an integral tool in their day-to-day work. This requires three important changes in the way quantitative scheduling techniques are designed and implemented. Managers must understand how the scheduling algorithm works so they know not only its strengths but its weaknesses. Much more time must be spent in educating the managers so they view the scheduling algorithm as an important tool that they can use. Managers must have constant access to the scheduling algorithm so they can run “what if” analyses. This access was not possible in the 1972 tire production system because only mainframe computers were available. However, today the power of laptop computers and the internet make this access possible, but the designers and programmers of the scheduling system must make this access the top priority in the design and implementation of the computerized quantitative scheduling system. Ways to measure a manager’s value function and integrate that value function into their model must be invented. If this is done, the manager will feel a sense of ownership of the model and will not be afraid to use its results.

ACKNOWLEDGMENT

Special thanks to Kelsie Bolerjack, Dong Zhang, Taylor Colliau, Zachariah Hughes, and Grace Rogers for their assistance with this paper.

REFERNCES

Anderson, R. D., & Brown, J. R. (1978). Better parks maintenance. *Park Maintenance*, *31*(10), 10–12.

Brown, J. R. (1979). The Knapsack sharing problem. *Operations Research*, *27*(2), 341–355. doi:10.1287/opre.27.2.341

Brown, J. R. (1979). The sharing problem. *Operations Research*, *27*(2), 324–340. doi:10.1287/opre.27.2.324

Brown, J. R. (1984). The Linear sharing problem. *Operations Research*, *32*(5), 1087–1106. doi:10.1287/opre.32.5.1087

Brown, J. R. (1991). Solving knapsack sharing problems with general tradeoff functions. *Mathematical Programming*, *51*(1), 55–73. doi:10.1007/BF01586926

Brown, J. R. (1994). Bounded knapsack sharing. *Mathematical Programming*, *67*(1), 343–382. doi:10.1007/BF01582227

Brown, J. R., Harvey, M., & Ozgur, C. (2006). Rational arithmetic functions to evaluate the one –sided two sample Kolmogorov- Smirnov cumulative sampling distribution In *Proceedings of the 2006 Annual Decision Sciences Institute Meeting* (pp. 24261-24266).

Brown, J. R., Harvey, M., & Ozgur, C. (2010). Systematic study of error in approximations to the one-sided one sample K–S sampling distribution. In *Proceedings of the Annual National Meeting of the 2010 Decision Sciences Institute Meeting* (pp. 1081-1086).

Brown, J. R., Harvey, M., & Ozgur, C. (2010). Rational Arithmetic functions to evaluate the two –sided two samples Kolmogorov- Smirnov cumulative sampling distribution. In *Proceedings of the MWDSI 2010 Annual meeting* (pp. 1051-1056).

Brown, J. R., & Israeli, A. (2004). Modeling a decision maker's preferences, Part 2: A tool for pricing decisions in the hospitality industry. *Tourism Economics*, *10*(1), 5–22. doi:10.5367/000000004773166565

Brown, J. R., & Israeli, A. (2013). Solving linear design problems using a linear-fractional value function. *Decision Support Systems*, *55*(1), 110–116. doi:10.1016/j.dss.2012.12.037

Brown, J. R., Israeli, A., & Mehrez, A. (2002). Modelling a Decision Maker's Preferences with Different Assumptions about the Preference Structure: Theory Development and Initial Applications for Tourism and Hospitality Management. *Tourism Economics*, *8*(1), 39–57. doi:10.5367/000000002101297981

Brown, J. R., & Ozgur, C. (1997). Priority class scheduling: Production scheduling for Multi-objective environments. *International Journal of Production Planning and Control*, *8*(8), 762–770. doi:10.1080/095372897234650

Brown, J. R., & Ozgur, C. (2009). Measuring and Implementing Maximin Value Functions. In *Proceedings of the* 2009 *Annual Meeting of the Midwest Decision Sciences Institute (pp. 55-60).*

Brown, J. R., & Ozgur, C. (2011). Utilizing maximin value functions. *International Journal of Operations and Quantitative Management*, *16*(4), 17–28.

Khouja, M., Rajagopalan, H., & Zhou, J. (2013). Analysis of the effectiveness of manufacturer-sponsored retailer gift cards in supply chains. *European Journal of Operational Research*, *230*(2), 333–347. doi:10.1016/j.ejor.2013.04.012

LSA Associates Inc. (2010). East bay regional parks district wildfire hazard reduction and resource management plan environmental impact response to comments document. Retrieved from http://www.ebparks.org/Assets/filesEBRPD_WHRRMP_Final_RTCr.pdf

Mehrez, A., Brown, J. R., & Khouja, M. (1992). Aggregate efficiency measures and simpson's paradox. *Contemporary Accounting Research*, *9*(1), 329–342. doi:10.1111/j.1911-3846.1992.tb00884.x

Ozgur, C., & Bai, L. (2010). Hierarchical composition heuristic for asymmetric sequence dependent single machine scheduling problems. *Operations Management Research*, *3*(1), 98–106. doi:10.100712063-010-0031-5

Ozgur, C., & Brown, J. R. (1995). A Two-Stage traveling salesman procedure for the single machine sequence dependent scheduling problem. *OMEGA*. *International Journal of Management Sciences*, *23*(2), 205–219.

Ozgur, C., & Brown, J. R. (2012). Applying decision utility to solve business problems with limited resources. *International Journal of Manufacturing Excellence*, *3*(1), 13–19.

Policeone. (n.d.). Police officers scheduling video a new, integrative, and proven police chaplaincy model. Retrieved from https://www.policeone.com/videos/originals/249675519-A-New-Integrative-and-Proven-Police-Chaplaincy-Model/

Siebert, J., & Keeney, R. L. (2015). Creating more and better alternatives for decisions using objectives. *Operations Research*, *63*(5), 1144–1158. doi:10.1287/opre.2015.1411

Parkpatrol. (2015Volunteer Trail Safety Patrol East Bay Regional Park District. Retrieved from http:// parkpatrol.org

This research was previously published in the International Journal of Information Systems in the Service Sector (IJISSS), 10(2); edited by John Wang; pages 69-78, copyright year 2018 by IGI Publishing (an imprint of IGI Global).

Section 3
Training Tools

Chapter 17
Design Principles for Online Role Play Simulations to Address Groupthink Tendency in Professional Training:
An Exploration

Lawrence Leung
Hong Kong Police College, Hong Kong

Nancy Law
University of Hong Kong, Hong Kong

ABSTRACT

Decision making for professionals in crisis situations can be highly stressful and mission critical. It is a kind of naturalistic decision making (NDM), characterized by highly fluid situations under great stress and uncertainty and involving interprofessional teams. A major challenge to the effective handling of crisis situations is the tendency for the personnel involved to ignore alternatives and make irrational decisions, a phenomenon referred to as Groupthink. This chapter reports on a case study of the application of a set of design principles for an online role play simulation (RPS) in addressing Groupthink in crisis management professional training. The training effectiveness on participants' Groupthink tendency was investigated using Bale's interaction process analysis (IPA). The design principles underpinning the RPS training system is discussed in light of the findings.

DOI: 10.4018/978-1-7998-2535-7.ch017

INTRODUCTION

In general, a crisis is a major event, which can bring damaging effects to individuals, groups, organisations and even society. Crisis management is a process for an organisation to deal with such critical events. However, there is no official or agreed definition for crisis among researchers. According to Oxford English Dictionary, crisis is a state of change, uncertainty, which can either become better or worse. Hermann (1963) states that there are three conditions for the occurrence of crisis: there exists a severe danger to the organisation's survival, there is a very short period of time to act, and the situation will become worse if the further development of the situation is not correctly anticipated. A fundamental characteristic of crisis is its ill-structuredness. Billings, Milburn, and Schaalman (1980) also point out that crisis can be disruptive, and no one can be fully prepared for a crisis because of its unpredictability. Coombs (2007) summarises four key characteristics of crisis from previous research. First, crises are low-probability events and are thus hard for decision-makers to even have the motivation to plan for them. Therefore, management will normally start planning only when the organisation has been hit by a severe crisis. Second, crises can induce severe damage or loss. The extent of the damage may go far beyond an organisation or even a country, such as in case of natural disasters like earthquakes and tsunamis. Third, the cause-effect relationships of crises are generally not easily identifiable. Because of this ambiguity, it is not easy to pinpoint even if the cause of the crisis is due to negligence. Fourth, crisis management requires quick and effective decision-making. If the organisation cannot respond with a quick and effective decision-making process, the crisis may rapidly intensify, resulting in significant damage and loss.

Crisis management poses great challenges for professionals who have to handle crisis situations due to their inherent uncertainty, as both problems and consequences are not well understood, at least at the time of occurrence. If crisis decision-makers are not well prepared both mentally and organisationally, the consequences could be chaos management rather than crisis management (Boin,'t Hart, Stern and Sundelius, 2005). Since each crisis has its own specific context and conditions, there is no single or predefined solution even for the same kind of problem. Therefore, decision-makers have to be mentally prepared through previous experience or training. Under such circumstance, previous crisis experience can offer lessons for learning, but not as solutions to be modelled (Flin, 1996). In other words, crisis personnel should learn something from previous crisis experience, but observations alone have little value in handling crisis. There is a difference between procedural operations in crisis management training and strategic level crisis decision-making. For example, it is essential for a fire-fighter to practise and learn how to extinguish a fire through step-by-step instructions, which are usually well-defined and relatively routine. This kind of skills can be acquired through practicing the procedures. On the other hand, crisis management at a more strategic level cannot simply follow a routine process or predefined schema, such as in following the crisis management process adopted during the fatal fire at the London King's Cross underground railway station in 1987. That operation involved multiple government units such as police, fire and paramedic personnel, and the aspects to be handled in the crisis was complex and dynamic (Boin, 't Hart, Stern and Sundelius, 2005). This kind of crisis requires strategic level management for effective handling.

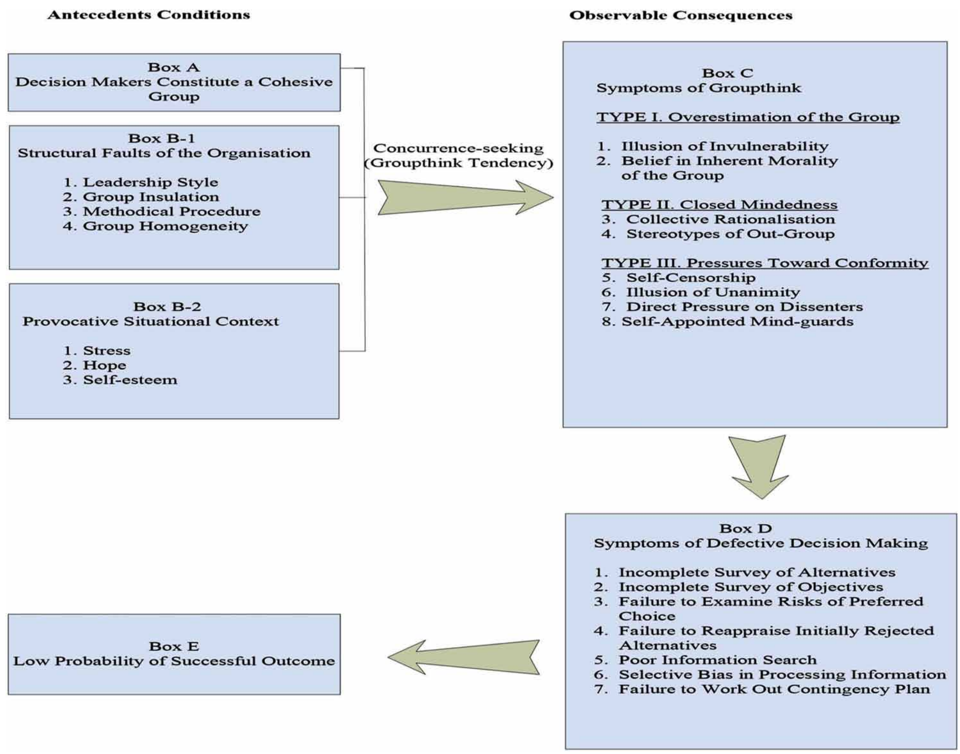
Due to the complexity and time constraints, as well as the non-routine nature of the problems, strategic level crisis management requires thinking out of the box and flexible decision-making (Borodzicz, 2005). Unlike procedural instructions, strategic level crisis management training should help learners to understand that there is more than one solution to resolving a crisis, and to encourage creative thinking in the decision-making process. The objective of crisis management training is to develop learners' ability to solve problems that require different adaptations to rapidly changing situations.

Sniezek, Wilkins, and Wadlington (2001) summarise the following challenges in crisis management training. First, crises do not occur frequently or regularly such that learning from direct experience in a specific crisis situation is not possible. Second, it is impossible for learners to test the causal relationships in crisis processes, as these are non-deterministic and complex. Third, the conditions in real crises are not favourable for training or observation. Fourth, as each crisis has its own unique features, the skills of crisis management cannot be generalised to all kinds of crises. Fifth, there is a need for crisis management personnel to continuously update their knowledge and skills continuously due to the dynamic nature of crisis environments, changes in regulations and technologies for managing crises.

GROUPTHINK

Groupthink is a term coined by Janis in 1972 from his book *Victim of Groupthink*. Groupthink is what happens when a group fails to make effective decisions due to group pressures that lead to a deterioration of "mental efficiency, reality testing, and moral judgment" (p. 9). Under the influence of groupthink, constructive ideas and alternatives offered by one group may be ignored by members of another group, and irrational actions may be taken because of stereotypic perceptions of each other across groups. Group cohesiveness refers to the attractiveness a group has for its members. A group could be any collection of people, friends or even a government. In summary, groupthink occurs when there is pressure for conformity towards consensus. Cohesiveness and conformity affect a group's ability to analyse and

Figure 1.



make judgments, resulting in poor decision-making. Victims of groupthink hence lose their ability to engage in creative and independent thinking. Janis's groupthink model (illustrated in Figure 1) is adopted to guide this study.

Janis's groupthink model is based on his analyses of historical decision-making activities in government policy-making committees or groups and supported by the associated content analysis of several political-military fiascos. The latter includes: Nazi Germany's decision to invade the Soviet Union (1941), US's failure to be prepared for the Japanese attack on Pearl Harbour (1941), the immature decision to launch the Bay of Pigs invasion in Cuba (1961), the stalemate in the North Korean War (1950), the escalation of the Vietnam War (1975) and the Watergate Cover-up scandal (1972). In general, the term groupthink describes a problematic decision that occurs when a group makes faulty decisions due to group pressure, without going through discussion, testing and exercising discrete judgment. Janis further explains that victims of groupthink neglect the seeking of alternatives, taking irrational actions to attack people of other groups. In addition, the hierarchical nature, rank cautiousness of law enforcement agencies and the existence of social cohesiveness in crisis management teams can also increase the possibility of groupthink (Rosander, Stiwne and ranstorm, 1998). In addition, the high stress levels due to uncertainty, ill-defined goals and high stakes of the decisions can increase the rigidity of decision-making, and reduce the motivation to find alternatives, leading to poor decision-making. Other factors that can induce groupthink include over-evaluation, isolation, and homogeneity among members.

Training through role play simulations (RPS) is a possible method to foster critical decision-making skills and reduce decision error or groupthink (Boin et. al., 2005). In order to make the training more realistic, the simulations should induce psychological processes to be similar to those that are experienced during an actual crisis (Salas, Bowers and Rhodenizer, 1998). Acute stress is a state that happens in situations of potential harm, time pressure, and arousal. Therefore, it is especially important that crisis management training can provide learners with a high degree of psychological fidelity in experiencing stress in decision-making. In RPS, learners can practise crisis management in a realistic environment that is safe to make mistakes, and to learn from those mistakes.

ROLE PLAY SIMULATIONS

The conventional way of transferring crisis management knowledge is through lectures that provide general knowledge of the necessary skills. Knowledge, either implicit or explicit, is emphasised as the skills learned can be applied to real crises. However, traditional crisis management training in the form of classroom lectures and presentations mainly focuses on individual tasks such as getting a situation update report from site officers using an agreed protocol. The communication mode is mostly one-way and top-down from trainer to trainees. Moreover, the conventional training is more focused on the responsibilities of the team members, rather than on the team aspects in the process. Role Play Simulation (RPS) is a useful technique for fostering virtual learning processes. It takes inspiration from “situated constructivism” approaches, which state that an educational experience has to be realistic for learners to observe and reflect critically (Winn, 1997).

Effective decision-making is essential for crisis decision-makers handling critical incidents, as serious consequences, including high casualty may be involved. In addition, crisis incidents are always dynamic and scenario-based. As such, the effectiveness of crisis management training through lecturing alone is very limited. Instead of individually focused, role plays offer experiential learning opportunities that are team- and scenario-based, allowing participants to evaluate their own competencies based on explicit behaviour in authentic contexts. Hence, RPS has become an integral component in assessment and training of crisis management in many law enforcement agencies, particularly for the resolution of high-risk problems without using violence (Schneid and Collins, 2001).

Online Role Play Simulations

Online role play simulation, a special form of Computer Supported Collaborative Learning (CSCL) facilitated by a set of technologies in an online environment designed to support and structure group interactions for the purpose of information exchange, problem solving and decision-making. Through the development of various scenarios, the crisis decision process can be realised and monitored. Online RPS supports activities such as idea creation, message exchange, project planning, document preparation, joint planning and decision-making, which are usually provided by Group Support Systems (Poole and DeSanctis, 1989).

Various forms of Online RPS have become increasingly popular in education and training. Online RPS is different from earlier forms of computer-based RPS in that the former mediate interactions among learners via computers rather than offerings interactions between an individual learner and a computer simulation model (Wills and McDougall, 2008). The support provided by online RPS platforms range from simple text discussions to video games, e-simulations, social media and multi-user virtual environments such as Second Life, and the possibilities are widening all the time (Wills, Leigh and Ip, 2011). McLaughlan and Kirkpatrick (2005) also observe that the scope of online RPS can be widened to include inter-location and international interactions, as well as augmentation with web-based information, multimedia and computer-based information management.

Although physical embodiment and immediacy are lost in the translation of face-to-face RPS to online formats, Wills, Leigh and Ip (2011) claim that online RPS retains the pedagogical power of face-to-face RPS. In addition, the possibilities of online interactions for asynchronicity and anonymity offer distinct advantages for learning (Freeman and Capper, 1999). Face-to-face RPS cannot be sustained for long periods and demands spontaneous action, with little time for planning or analysis before action, and less opportunity for reflection. In contrast, online RPS can stretch over several weeks, providing more opportunity for research, data gathering, reflections on the implications and consequences of actions taken, consolidation and internalisation.

Anonymity can break down hierarchies that dominate typical meetings and equalise the participation of all group members. Freeman and Capper (1999) argue that online RPS, because of the anonymity of the interactions, is particularly well-suited to those with learning disadvantages in face-to-face role plays, such as shyness, timidity and lack of self-confidence. Anonymity can also be helpful to learners whose mother language is not the language used in the role play as it can reduce self-consciousness of the language problem, thereby promoting creativity and imagination.

Based on the Project EnROLE, an Australian project on adoption of role-based e-Learning in university education, Wills et al. (2009) identified the following as key features to be attended to in the design of online RPS:

1. **Learning Objective:** To increase the understanding of human interactions and dynamics in real world situations;
2. **Role Assignment:** Learners play the role of some else, so that he or she can learn in a situated environment from others' perspectives;
3. **Task Authenticity:** Learners undertake authentic tasks as in real life contexts during role play;
4. **Task Design Requirement:** To focus learners' attention on role interactions, so as to foster collaboration, debate or negotiation;
5. **Interactions Among Roles:** Mainly carried out an online in the RPS environment;
6. **Learning Outcomes Targeted:** Are assessable and can encourage reflection from learners.

Conventional face-to-face role play approaches have serious limitations in crisis management training, such as maintaining realism and involvement of large amounts of resources in the form of manpower and props for scenario setting. Moreover, only a small number of officers can be trained in such settings. Advanced online technologies can reduce these limitations. There are three major technology components in an online RPS:

1. An immersive multimedia interface,
2. A crisis simulator, and
3. A critiquing system (Sniezek, Wilkins, Wadlington and Baumann, 2001).

In online RPS, the term "simulation" often refers to a number of technical implementations used to mimic social, political, economic, and/or psychological processes. Here, learners participate in the simulation rather than directing it (Portney and Cohen, 2006).

In contrast to other simulations such as stock market simulations or role play games, which allow participants or learners to set parameters, start a simulation, and see what happens as events unfold over time, participants of online RPS have no parameters to set and only the facilitator can start a simulation. Although online role-play decisions may be flexible, the flexibility is not in the hands of learners. Learners participate in the simulation and make one or more decisions that influence an outcome (Borodzicz, 2005). Online RPS may allow simulation administrators the flexibility to modify the simulations systematically and analyse how different interactions might influence decisions and their learning outcomes (Portney and Cohen, 2006).

In crisis management training, online RPS allows trainers or teachers to create synthetic or artificial crisis situations to teach participants about the appropriate decisions they should make and their underlying processes without any pre-set consequences. It requires participants to play roles in order to deliver simulation materials and to facilitate decision-making skills under stress through computer-mediated interactions.

GROUPTHINK FOCUSED DESIGN PRINCIPLES FOR ONLINE RPS SYSTEMS

The Naturalistic Decision-making (NDM) approach examines how people make decisions in natural settings, which can be difficult to reproduce in experimental laboratory studies. It supports explorations of collaboration and cooperation between people, between people and systems, as well as situations involving diagnosis, planning, supervision and control processes (Klein et al. 1993). Four principles have been formulated based on the literature review in our design of the online Role Play Simulation platform to address the problems of Groupthink. These principles also ensure that the online Role Play Simulation platform can support holistic observations of the participants' interactions according to the Groupthink model and analyse the Groupthink tendency of participants during training. The following is a description of the design principles we have adopted in this study.

The first principle requires that the platform setting must be able to simulate real-world situations in terms of the working environment and communication protocols for the training context. According to Klein (1993), the importance of naturalistic settings is frequently ignored in decision-making research. Real world settings are particularly important and essential for studying Groupthink, given the typically stressful and high stakes situations and the uncertain dynamic environments involved (Janis 1982).

The second principle stipulates that participants must be assigned specific roles and that the assignment must be made anonymously. Anonymity ensures that all participants can enact the roles assigned and practise the corresponding communication protocols in decision-making without interference from pre-existing roles and relationships among participants in their actual workplace. It is essential that participants can play the role of someone else and think from others' perspectives (Wills et al. 2009).

The third principle concerns the design of the communication platform in the RPS online system. There should be no rules or platform limitations that restrict communication. Further, all communications need to be recorded for the Groupthink tendency analysis using IPA (to be described in a later section). According to Dickens (2003), when groups become too close, the quality of decision-making may suffer from the lack of intense discussion. Cornelius, Gordon, and Harris (2011) suggest that the anonymity of online RPS can also encourage open discussion and argument. In fact, open discussion and argument can reduce the tendency of Groupthink (Janis 1982). Hence, this unrestricted environment can promote creative thinking, encourage collaboration, argument and information exchange during decision-making. The recorded transactions are very useful during debriefing to provide elaborations of the Groupthink tendency, and allow discussions on the remedies for problematic issues of Groupthink.

The fourth principle requires the platform to allow facilitators to change or adjust scenario settings according to the development of the episode. This would allow the training the flexibility to engage participants in more or less challenging tasks in a situated environment. Participants may thus be able to experience during training evolving and increasingly treacherous scenarios as in real world situations.

THE DESIGN FEATURES OF THE ONLINE RPS USED IN THE STUDY

Crisis management simulation should also produce the same emotional experiences and responses as in a real crisis scenario, such as frustration, stress, time pressure and uncertainty (Borodzicz, 2005). In order to set up a realistic crisis scene, the design of the online RPS and crisis scenario should be treated as high-threat, high-surprise event and has to be solved within a limited time frame. In addition, Gredler (1992) suggests that there are four essential elements in building a RPS: role assignment, background information, stimulus to learner's responses and reaction to learner's actions. Gredler further suggests that simulations should also facilitate both learner's reflective reaction and the generation of new thinking.

Janis's (1982) suggestion for the avoidance of groupthink provides the basic concepts for the design of the online RPS platform to be developed in this study. Janis suggests that acceptance of criticism can reduce the tendency of groupthink, as this provides a social climate within which learners are able to discuss and express their opinions freely without any penalty or restriction. In order to achieve this, the platform should be able to eliminate the physical organisational hierarchy during the training. The environment should also allow learners to enact their assigned roles using all available channels of communication provided on the platform. In

Table 1. RPS design concepts and skill development objectives to tackle groupthink

Skills to Avoid Groupthink (Janis, 1982)	Behavioral Indicators	Supportive RPS Design Features
Acceptance of criticism	• No restriction on discussions • No rules or restrictions for decision-making / discussion • No penalty for criticism	• Physical organisational hierarchy should not exist, but learners have to act according to the roles assigned • Communication tool/channel is available to all learners
Impartial leadership	• Each member should have the same right of speech • Leaders should not have any stating preferences, expectation or specific solutions that he or she would like to see accepted	• Anonymity • Access to external information is available
Seek peer feedback on plans/ decisions	• Double checking of plans or decisions by other team members • Welcome devil's advocate	• Peer review and argumentation • Group decision
Seek expert input	• Willing to seek external sources of information • Awareness of expertise relevant to the situation	• Access to external information is available • Upon request, expert is available to give advice anonymously.
Prepare for contingency	• Prepare for the worst case scenario	• Preparation of a contingency plan as a required written group assignment
Openness before consensus	• Hold review meetings for any critical consensus • Encourage argument/expression of conflicting views on critical issues	• No restriction on topics for discussion • Equal communication right for all • Facilitator gives credit for open sharing of ideas

addition, learners should be able to access external information or references. The key design concepts and features of the online RPS to implement Janis's suggestion in the avoidance of groupthink is summarised in Table 1.

In the design of the online RPS system, the appropriate selection and design of technology is critical to ensure that the learning environment and tasks provide the necessary learning experience. Otherwise the training effectivness would be jeopardized. From the previous work by Miranda (1994), Bostrom and Anson (1992), groupthink tendency may be reduced by applying appropriate technologies. The reduction of groupthink is achieved by decreasing the occurrence of certain antecedent conditions (such as cohesiveness among team members and group homogeneity) and procedural conditions of groupthink (such as few alternatives examined and discouragement of dissent). The design features adopted in the online RPS used in this study to tackle groupthink tendency (summarized in Table 2) has taken the above into consideration.

Table 2. Design features of the online RPS mapped to conditions for groupthink reduction

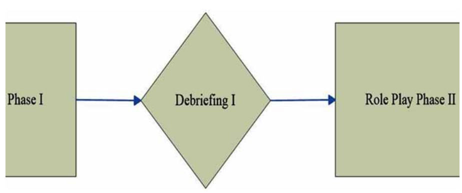
Design Feature of the Online RPS	Conditions for Reduction of Groupthink Tendency (Miranda, 1994; Bostrom and Anson, 1992; Nunamaker et al., 1991)
Anonymity on the computer network	*Antecedent conditions* Directive leadership Group homogeneity *Procedural conditions* Discouragement of dissent Few alternatives examined
Simultaneous input / Group communication and Synchronous communication	*Antecedent conditions* Directive leadership Group homogeneity Nature of task *Procedural conditions* Discouragement of dissent Few alternatives examined
Process structuring / Scenario builder (role play platform design)	*Antecedent conditions* High cohesiveness Group homogeneity Nature of task *Procedural conditions* Discouragement of dissent Few alternatives examined
Extended information processing capacity / Web hosted resources	*Antecedent conditions* Nature of task *Procedural conditions* Few alternatives examined
Access to external information / Internet search and Anonymous expert connection (Intranet)	*Procedural conditions* Perception of invulnerability Lack of expert advice
Written input / Asynchronous or synchronous communication	*Antecedent conditions* High cohesiveness Directive leadership *Procedural conditions* Few alternatives examined
Electronic recording	*Antecedent conditions* Nature of task
Public screen	*Antecedent conditions* High cohesiveness Group homogeneity Nature of task Directive leadership

RESEARCH DESIGN AND DATA COLLECTION

In this study, 16 trainees from the Hong Kong Police College participated in an online RPS exercise as part of a 4-week crisis management training programme. In this exercise, trainees were randomly assigned to 4 different teams named Alpha (α), Beta (β), Gamma (γ) and Delta (δ) with specific functional roles in a crisis scenario. The teams were assigned to different rooms within the exercise vicinity without face-to-face contact. The facilitator (i.e. the exercise controller) located at the control room could communicate with the trainees in all the groups through a computer networked RPS platform called SIMS (Scenario-based Interactive RPS System). Participants did not know the scenario of the role play before the start of the exercise. SIMS provides all the simulated communication tools for professional training in decision-making, including chat-box, e-mail, beat radio, telephone and video conferencing. Trainees can use the tools provided to carry out all communications, decision-making and Command and Control operations during the role play simulation. In addition, the Controller can also send out instant multimedia information (such as TV news, video clips) according to scenario development and to enhance realism of the crisis situation. All role play interactions and communications are logged by the system for data analysis and debriefing.

The whole exercise was divided into two phases with two debriefings as illustrated in Figure 2. Trainees took part in two role plays in Phases I and II respectively. Each phase had the same duration of 2 hours. Before the commencement of Phase I, the participants had to complete a 40-question Groupthink Index (Glaser, 1993) questionnaire before the exercise commenced. Debriefing I was conducted after the completion of Phase I. In this 30-minutes session, the facilitator gave a short introduction on groupthink to participants. The participants then took a break before commencing Phase II. Debriefing II was the post-exercise discussion. The facilitator discussed with participants their experience throughout the entire exercise. At the end of the exercise, participants completed the Groupthink Index questionnaire again to find out if there have been any changes in participants' groupthink tendency.

Figure 2.



ANALYSIS OF RESULTS

Two instruments were used in this study to measure groupthink: Glaser's Groupthink Index (GTI) and Bales' Interaction Process Analysis (IPA).

Glaser's Groupthink Index

Groupthink Index (GTI) (Glaser, 1993) is a commercial instrument often used in management training to measure the groupthink tendency of an individual or a team. The 40-item questionnaire comprises eight sets of five items, each designed to measure one of the eight groupthink symptoms. Each item uses a 5-point Likert-scale with responses ranging from "almost never" to "almost always". Each groupthink symptom sub-category consisted of 5 questions, giving a maximum score of 25 for each groupthink symptom. According to the GTI scale, a score for "very insignificant" groupthink is less than 93, a score for "insignificant" groupthink is 94-111, a score for "moderate" groupthink is 112-129, a score for "significant" groupthink is 130-147, and a score equal to or over 148 indicates "very significant" groupthink. Glaser further suggests that for each symptom subcategory, a score for "very insignificant" groupthink is less than 8, a score for "insignificant" is 9-13, a score for "moderate" is 14-15, a score for "significant" is 16-17, and a score for "very significant" is 18-25. Hence GTI yields an overall groupthink index and sub-scale scores for each of the 8 groupthink symptoms. Table 3 presents the overall GTI scores of each team before and after the online RPS exercise, and the percentage improvement achieved.

The Groupthink Indices of the four teams were found to have been reduced from Significant to Moderate level after the exercise, but to different extents. The reduction in groupthink tendency indicates that online RPS may have contributed to the change. However, this can not be substantiated unless one can establish the link

Table 3. Pre- and post- GTI scores and percentage improvement achieved of the four teams

Team	Team Average (Glaser's Groupthink Index)		% of Improvement
	Pre-Role Play Simulation	Post-Role Play Simulation	
Alpha (α)	147	125	15.0
Beta (β)	139	127	8.6
Gamma (γ)	141	116	17.7
Delta (δ)	142	113	20.4

between online RPS behavior and change in groupthink tendency. The IPA analysis reported in the next section is to investigate this relationship.

Bales' Interaction Process Analysis (IPA)

Interaction Process Analysis (IPA) is a generic method developed in 1950 by Robert F. Bales to analyse interactions in small groups. Bales' IPA is the first and most frequently used tool to study small group dynamics through analyzing interactions. It is a structured coding system to identify and examine task and socio-emotional communication activities in groups, based on the social psychological belief that group interactions are driven either by social or task needs (Bales, 1950). Bales' IPA consists of 12 specific behavioural categories nested within 4 overarching process categories as shown in Table 4. Three categories describe positive socio-emotional activities (Codes 1-3), three categories describe negative socio-emotional activities (Codes 10-12). Three describe active task activities (Codes 4-6), and three describe passive task activities (Codes 7-9). A total of 871 transactions recorded by the system. About 0.8% of the total transactions had input error or were incomplete statements with no logical meaning and was not transcribed. A total of 864 transactions (307 in Phase I and 557 in Phase II) were transcribed and analysed.

In Phase I, the percentages of task-based and social-emotional interactions were 78% and 22% respectively. The corresponding percentages for Phase II were 86% and 14%. From Table 5 and Table 6, the IPA category (code) with the highest mean is "Asks for information" in Phase I and "Gives information" in Phase II. On the other hand, the lowest mean is "Shows antagonism" for both phases. Moreover, the most frequent interaction categories were task-based. This indicates that exchange of information, suggestions and opinions were the predominant activities and not social-emotional interactions. In fact, this implies that the groups' crisis decision-making had gone through the processes of information gathering, discussion and teamwork, as expected from the literature (McGrath 1984). This distribution of IPA codes is significantly different from the study by Bales (1950), which was a face-to-face free form role play, but is similar to the studies by Hiltz (1978) on problem solving via computer conferencing.

The interactions among the four teams observed during the two phases (I & II) of the online RPS exercises are illustrated in Figure 3a-d. It should be noted that the percentages in these figures are computed with the total number of interactions during the corresponding phase as the denominator.

Table 4. Bales' 12 interaction categories (Adapted from Bales, 1950, p.9)

Code	Behavior Category	Type of Interaction
1	Shows solidarity – Raises other's status, gives help, encourages others, reinforces (rewards) contribution, greets others in a friendly manner, and uses positive social gesture.	Social Emotional: Positive Emotions
2	Shows tension release – Jokes, laughs, shows satisfaction, relives or attempts to remove tension, express enthusiasm, enjoyment, satisfaction.	
3	Agrees – Shows passive acceptance, acknowledges understanding, compiles, co-operates with others, and expresses interest and comprehension.	
4	Gives suggestion – Makes firm suggestion, provides direction or resolution, implying autonomy for others, attempts to control direction or decision.	Task: Giving (Neutral emotions)
5	Gives opinion: Offers opinion, evaluation, analysis. Expresses a feeling or wish. Seeks to analyse, explore, and enquire. Provides insight and reasoning.	
6	Gives information: Provides background or further information, repeats, clarifies, confirms. Brings relevant matters into the forum, acts and assists group focus.	
7	Asks for information: Asks for further information, repetition or confirmation. Acts used to request relevant information and understand the topic.	Task: Asking (Neutral emotions)
8	Asks for opinion: Asks for opinion, evaluation, analysis, or expression of feeling on the matter.	
9	Asks for suggestion: Asks for suggestion, direction, and possible ways of action. Requests for firm contribution, solution or closure to problem.	
10	Disagree: Shows passive rejection, formality, withhold help, does not support view or opinion, fails to concur with view, and rejects a point, issue or suggestion.	Social Emotional: Negative Emotions
11	Shows tension: Shows concern, apprehension, dissatisfaction or frustration. Persons interacting are tense, on edge. Acts that express sarcasm or are condemning.	
12	Shows antagonism: Acts used to deflate other status, defends or asserts self, purposely blocks another or makes a verbal attack.	

Figure 3. A-D

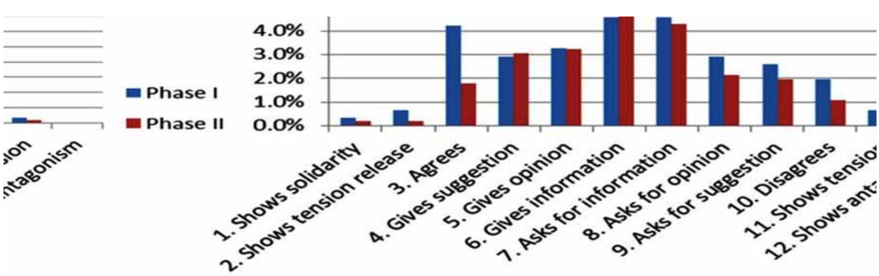


Table 5. Bales' IPA categories – sorted by mean (Phase I)

IPA Category (Code)	Mean	Std. Dev.
Asks for information (7)	15.5	3.9
Gives information (6)	11.8	3.9
Gives suggestion (4)	8.8	2.6
Asks for suggestion (9)	8.8	2.2
Agrees (3)	8.3	3.3
Gives opinion (5)	7.5	3.9
Asks for opinion (8)	7.3	1.5
Disagree (10)	3.3	1.9
Shows tension release (2)	2.5	1.7
Shows solidarity (1)	2.3	1.5
Shows tension (11)	1.0	0.8
Shows antagonism (12)	0.0	0.0

Table 6. Bales' IPA categories – sorted by mean (Phase II)

IPA Category (Code)	Mean	Std. Dev.
Gives information (6)	33.3	16.0
Asks for information (7)	21.8	4.5
Gives opinion (5)	17.3	6.6
Asks for opinion (8)	17.0	4.8
Gives suggestion (4)	16.3	8.1
Asks for suggestion (9)	13.8	2.2
Agrees (3)	9.8	3.3
Disagree (10)	5.3	5.0
Shows solidarity (1)	2.3	1.3
Shows tension release (2)	1.3	0.5
Shows tension (11)	1.3	1.3
Shows antagonism (12)	0.3	0.5

FINDINGS

Analyses of the group interactions using the IPA framework show indications of a reduction in Groupthink tendency of the participants after the online RPS exercise, triangulating the same finding based on the pre- and post- exercise GTI survey. The findings from the analyses of group interactions are presented in this section.

Reduction of Cohesiveness

Due to the group homogeneity (all participants are police officers with similar years of service and training background), there is a high risk of intuitive social cohesiveness, which is an important antecedent condition for groupthink, a major challenge in crisis management decision-making. Effective communications in such context should be basically task-based (Emmitt & Gorse, 2006). The results presented in Table 5 and 6 show that the amount of task-based communications (IPA 4-9) is higher than social-emotional communications (IPA 1-3 and IPA 10-12), which is reasonable for such situations. In fact, a high level of social-emotional communications is indicative of groupthink, as high social cohesion due to friendship or social ties may lead to immature decisions, a phenomenon known as the "illusion of unanimity" (Cline, 1994). Table 7 summarizes the number and percentages of social-emotional and task-based communications across the four teams.

It can be seen that all teams have shown a decrease in social-emotional communication in Phase II, with the reduction varying from the smallest difference of 0.6% for Team Alpha, to a maximum of 4.4% for Team Delta. Team Beta, which showed the lowest gain in GTI between Phases I and II also contributed the lowest percentage (14.0% and 13.5% respectively) of task-based communication, when all the other teams contributed about 20% or more.

Table 7. Percentages of social-emotional and Task-based communications among teams*

		Team Alpha	Team Beta	Team Gamma	Team Delta
Phase I	Social-emotional	6.5%	4.6%	3.6%	7.8%
	Task-based	20.8%	14.0%	21.8%	20.8%
Phase II	Social-emotional	5.9%	2.3%	2.7%	3.4%
	Task-based	28.5%	13.5%	23.9%	19.7%

*N.B. All communications contributed by the four teams within one phase adds up to 100%.

Reduction in the Risk of Directive Leadership

Anonymity in an online RPS allows for openness in communication, which can foster equal participation and hence reduce the danger of directive leadership and groupthink tendency (Miranda, 1994). From the interactions recorded by the system, it can be shown that all learners have actively involved in the exercise. Information seeking behavior (asking and giving information) constitute the most popular interaction categories. Asking and giving opinions and suggestions constitute behavior related to the seeking of alternatives (Emmitt & Gorse, 2006). The results show that both the total amount of interactions as well as the proportion constituted by task-based interactions have increased from 78% in Phase I to 86% in Phase II, with a corresponding drop in the percentage of interactions that were socio-emotional in nature. Janis (1972) suggests that information and alternative solution seeking interactions during the decision-making process contribute positively towards the avoidance of groupthink.

Facilitation of Procedural Process in Decision-Making

From the analysis IPA (4-6) – giving suggestions, opinion and information and IPA (7-9) – asking for information, opinion and suggestion, all teams have positive differences (comparison between phase I and Phase II of the exercise), which indicates that all teams engaged in all necessary processes for decision-making: fact finding, information gathering and decision-making (Emmitt & Gorse, 2006). Hence, it can be concluded that the teams were able to communicate through the SIMS platform to establish a structured process for crisis decision-making, which is considered to be a remedy for groupthink arising from lack of methodical procedures (Miranda, 1994).

In crisis communications, the "asking for" categories (IPA 7-9) are considered more constructive than "giving" categories (4-6), as more new ideas may be generated, giving more chances for the seeking of alternative solutions, which are essential in the reduction of groupthink tendency. As a whole, all teams have shown positive contributions in those categories as shown in Figure 3 (a-d). However, it is interesting that Team Beta has shown a high level of 6% increase in "Gives opinion" (IPA 5) but a relatively low score in GTI reduction. Subsequently, a review of the transactions was conducted, which found that the quality of the opinions given was not high and some opinions were not useful. This shows that while GTI and IPA analyses are helpful indicators, qualitative semantic analysis of the communication protocol is necessary to understand the actual quality of the interactions in relation to groupthink.

Promotion of Constructive Conflict in Crisis Communications

A high level of social cohesiveness is considered harmful for crisis decision-making as some good alternatives may be neglected. In fact, constructive or task-based conflict is necessary to ensure that the group will not jump to conclusions directly by simple "agreement" (Cline, 1994). By avoiding disagreements, group members may also overlook the vulnerability of a proposal. The Watergate cover-up scandal is considered a classic case of groupthink in the crisis management literature. Cline (1994) reports on a study using the IPA framework to analyze instances of agreement and disagreement in three transcripts presented by the prosecutors in the Watergate Scandal. The study found that interactions in the Watergate Scandal exhibited a much higher ratio of "agreement to disagreement" than those reported from similar analyses of non-groupthink cases, showing evidence that those involved in this case were trapped by groupthink.

Figure 4 presents the agreement-disagreement ratios for the Watergate case and the role plays in Phases I and II. Cline (1994) suggests that ratios higher than 2:1 are prone to groupthink. In the Watergate Scandal, the ratio is 5.2: 1, which is

Figure 4.

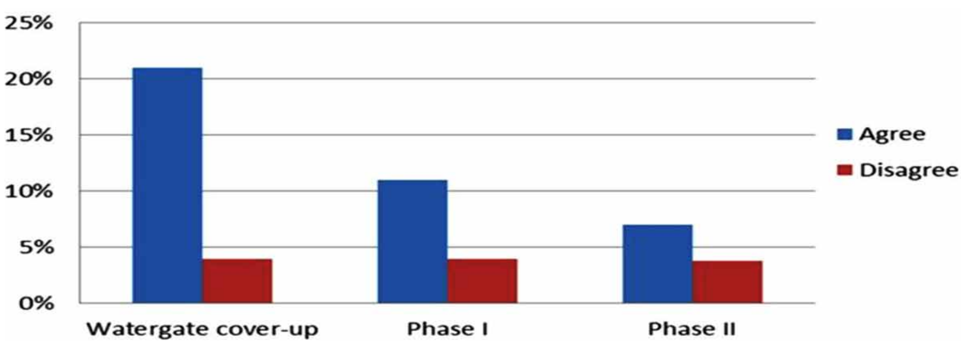


Table 8. Agreement:Disagreement Ratios for the teams during Phases I and II

	Team Alpha	Team Beta	Team Gamma	Team Delta
Phase I	2.7:1	3:1	3:1	2.2:1
Phase II	1.2:1	6.2:1	4.4:1	1.7:1
Difference (%)	-55.6	+106.7	+46.7	-22.7

considered too high and risky. In the present study, the percentage of agreements in both Phases I and II were higher than the percentage of disagreements. Further, it can be seen that there is a sizeable decrease in "Agreement" from 10.7% in Phase I to 7.0% in Phase II, and also a slight decrease in "Disagreement" from 4.2% to 3.8%. As a result, the "agreement:disagreement" ratios for the two Phases were 2.8:1 and 2.2:1 respectively. As both ratios are higher than 2:1, this indicates inadequate constructive conflicts during the online RPS interactions. On the other hand, the decrease in this ratio also shows a reduction in groupthink tendency in Phase II, triangulating with the reduction in overall GTI reported earlier.

Table 8 presents the "agreement to disagreement" ratios for each of the four teams. It can be seen that the ratios are lower than that of the Watergate Scandal for all teams except Team Beta. In fact, the groupthink tendency for both teams Beta and Gamma are high. On the other hand, Team Alpha has the lowest "agreement to disagreement" ratio among teams. In addition, the relatively high level of antagonism interactions shown by Team Beta members is indicative of barriers to constructive discussions.

Findings from this study show that online RPS can contribute positively to the reduction of groupthink tendency in crisis management training. SIMS provides a simulated environment to foster constructive discussions and provides a safe and authentic situation for crisis management training. However, it does also reveal wide variations in behavior and improvement across the different teams, which warrants further investigation.

LIMITATIONS OF THIS STUDY

The present study has shown the usability of the SIMS online RPS system for crisis management training and some indications of success in reducing participants' groupthink tendency. However, there are some important limitations in this study that needs to be addressed in future studies. First of all, although the number of interactions collected and analysed is relatively large, the number of teams and trainees participating in the exercise is small – only four teams and 16 trainees. Hence the findings from this study are only exploratory in nature, and may not be generalizable to a wider population.

The second limitation relates to participants' background. While the participants in this study are heterogeneous in terms of gender, age, culture, academic background and learning style, they were all law enforcement officers. This is different from actual crisis situations in which some of the teams would be from other agencies such as the fire department or medical emergency services. The interactions and results in this study may be influenced by the culture of the law enforcement profession, and may not be generalizable to real life crisis situations.

A third limitation relates to the ICT competence of the participants. Unlike conventional face-to-face role play, online RPS requires participants to have basic ICT skills to function effectively. In other words, online RPS can be a hurdle for participants (both facilitators and learners) who are less competent in using ICT. As a result, participants' behavior and performance in SIMS may be influenced by their ICT competence. In fact, a few learners have expressed this concern in the post-exercise questionnaire, and suggested that training should be provided beforehand to help them overcome such problems in order not to affect their participation in the RPS.

A fourth limitation relates to the fact that this study involves only one crisis management scenario. There could be differences in participant behavior and challenges to avoiding groupthink tendency due to the nature of the crisis.

While there are limitations to the generalizability of the findings from the present study, the fact that all task design, facilitation and interactions are recorded automatically in an online RPS system allows for much more systematic investigations on the pedagogical design and assessment of crisis management than would be possible in face-to-face RPS training. It is hoped that this study will stimulate further work in this area.

ENHANCING THE DESIGN OF ONLINE RPS

Both the data analysis and the facilitator's feedback indicate that the use of the SIMS online RPS system has been effective in providing an authentic simulated environment for crisis management training. There are distinctive advantages in using online instead of face-to-face RPS in crisis management training through the anonymity that online communications offer. On the other hand, the present SIMS system is designed to basically support synchronous interactions mimicking those in traditional face-to-face RPSs that have been used in past training situations. In reflecting on the observations and findings from the present study, we have seen further possibilities for enhancement of SIMS by incorporating asynchronous communications into the platform to foster deeper reflection between role plays and to support more effective debriefing.

Introducing Asynchronous Communication to Foster Reflection

In the current design, participants only have half an hour for the debriefing, which takes place immediately after the role play ends. Hence, much of what takes place during this time is for the instructor to explain what Groupthink is and to give comments on the students' performance. There is really no time for students to engage in deep reflection and learn from their experience in Phase I before launching into Phase II. With the addition of asynchronous communications, learners will have more opportunities to engage in reflection. In particular, they would be able to read their logged discourse during the RPS. They can also be asked to analyze and identify instances of groupthink, give justifications on their evaluation, and to give suggestions on how to avoid similar occurrences in the future.

Debriefing as a Blended Learning Process

The availability of automatic recording of interactions in online RPS is a valuable resource for conducting debriefing after each role play session. In contrast to face-to-face RPS, due to the lack of automated recording facilities, all interactions have to be recorded manually. In online RPS, facilitators can retrieve any interaction from the computer and display on a screen for discussion instantly. The facilitator can also select and compile recorded interactions into a knowledge database to support learning.

If the two phases of the online RPS can be conducted on different days, the debriefing process can also be conducted in two phases to allow for deeper reflection taking place between the two parts of the exercise. The first part can be conducted through asynchronous online discussions before the face-to-face debriefing. There are a number of advantages in adopting such an arrangement:

- The facilitator will have more time to prepare for the debriefing by reviewing the logged communication transactions to identify good sample excerpts for participants' exploration and discussion.
- Leaners may be able to seek expert advice or accessing external information and share with others during the online debriefing discussion.
- Some learners who are reluctant to speak up spontaneously in face-to-face discussions may be able to find their voice in asynchronous online media such as email or discussion forum.
- The online debriefing discussion can be further refined and summarized to form a useful knowledge database to be further developed through face-to-face debriefing that follows.

FINAL DISCUSSIONS

In this paper, a case study of using an online RPS platform designed according to the four theoretically grounded design principles for addressing groupthink in crisis management training is presented. The results show that participants have achieved a reduction of groupthink tendency after the Online RPS training. Moreover, the IPA analyses of the group interactions in the two phases of the RPS show evidence of reductions in cohesiveness, directive leadership, and increases in task interactions for decision-making and constructive conflict, which are all indicative of reduction in groupthink tendency.

Existing groupthink research mainly uses content analysis of retrospective information/ data or empirical experience in laboratory settings as their basis for understanding the interaction processes. Very often, only a partial model is examined. This study shows that the online RPS developed on the basis of the four design principles offers an alternative approach to groupthink research. Online RPS can support the design of holistic scenarios for crisis management training such that the different stages in the exercise can be visualised by researchers and facilitators. Furthermore, the interactions can be automatically recorded and analyzed later to reveal groupthink tendency. In fact, due to the complexity of the groupthink model, researchers using traditional methods generally only focus on a partial selection of behavior during the whole process to record and study. Online RPS can serve both as a training platform as well as a research tool for holistic groupthink research. Researchers can explore the effect of different settings and scenario designs on groupthink behavior and how to reduce groupthink using online RPS. In addition, the same set of recorded data can be used by different researchers to explore different aspects of the interactions and research questions. In this final section, we review the four design principles for online RPS systems we formulated and adopted in the light of the research findings and latest technology developments.

Virtual reality (VR) technology has become much more sophisticated and accessible, providing an alternative technology platform for the development of online RPS that can provide more authentic simulations of real world situations. In fact, the first author has piloted the deployment of VR in online RPS in late 2017 with the objective to improve the realism of the scenario. Using this pilot system, participants can observe the key training scenes in 360 degrees with the VR headsets provided. It is not within the scope of this chapter to report on this pilot study in any detail. Overall, participants agree that they can have an immersive feeling of the scene and the degree of realism is increased. On the other hand, the risk of cognitive overload may also increase. Cognitive overload occurs when a large amount of information that has exceeded an individual's capacity to process (Mayer and Moreno, 2003). Shrivastav et al. (2013) point out that the use of advanced features of educational technologies can induce the risk of cognitive overload, as these features could provide a more complex and information-rich environment. Unfortunately, current research literature cannot yet provide definitive guidelines on the relationship between cognitive overload and VR technology, or whether the adoption of VR technology is likely to enhance the training effectiveness of online RPS for crisis management training.

On the second design principle, all participants agreed that anonymity could encourage positive argument or discussion. To enhance the level of anonymity, the physical layout of the training venue is important. The participants suggested refurnishing the training facility so that the syndicate rooms can be separately located.

Thirdly, in terms of the design of the communication platform in the RPS system, we find that storage size and stability of recording module is very important. Quality of the recording as well as the ease of review can improve the effectiveness in debriefing. Further enhancements can include support for the facilitator in reviewing and analyzing dialogues from previous training exercises using the same scenario. A training database could also be established in future systems for better knowledge management in system design and facilitation.

Fourthly, feedback from our study indicates that the facilitator support aspect of the system can be further enhanced by improving the facilitator user interface to make it more user-friendly and efficient in monitoring the participants' interactions and scenario development. This would avoid the need for external technical support during the training exercise, and hence reduce the possibility of interruption while the facilitator makes sense of the situation. In fact, any interruption for whatever reason could greatly damage the effectiveness of the whole training exercise.

REFERENCES

Bales, R. F. (1950). *Interaction Process Analysis*. Cambridge, MA: Addison-Wesley.

Billings, R. S., Milburn, T. W., & Schaalman, M. L. (1980). A Model of Crisis Perception: A Theoretical and Empirical Analysis. *Administrative Science Quarterly*, *25*(2), 300–306. doi:10.2307/2392456

Boin, A., 't Hart, P., Stern, E., & Sundelius, B. (2005). *The Politics of Crisis Management: Public Leadership under Pressure*. Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511490880

Borodzicz, E. P. (2005). *Risk, Crisis and Security Management*. West Sussex, UK: John Wiley & Sons Ltd.

Bostrom, R. P., & Anson, R. G. (1992). *A Case for Collaborative Work Support Systems in a Meeting Environment* (Unpublished working paper). Department of Management, University of Georgia.

Cline, R. J. W. (1994). Groupthink and the Watergate cover up. The illusion of unanimity. In L. R. Frey (Ed.), *Group Communication in Context: Studies of Natural Groups*. Lawrence Erlbaum Associates.

Coombs, T. (2007). *Ongoing crisis communication: Planning, managing and responding*. Thousand Oaks, CA: Sage Publications.

Cornelius, S., Gordon, C., & Harris, M. (2011). Role engagement and anonymity in synchronous online role play. *International Review of Research in Open and Distance Learning*, *12*(5), 57–73. doi:10.19173/irrodl.v12i5.923

Dickens, P. (2003). Don't Be Brainwashed by Groupthink. The Scotsman, p. 9.

Emmitt, G. E., & Gorse, C. A. (2006). *Communication in construction teams*. London: Spon, Taylor & Francis.

Flin, R. (1996). *Sitting in the Hot Seat: Leaders and Teams for Critical Incidents*. Chichester, UK: Wiley.

Freeman, M., & Capper, J. M. (1999). Exploiting the web for education: An anonymous asynchronous role simulation. *Australian Journal of Educational Technology*, *15*(1), 95–116.

Glaser, R. O. (1993). *Groupthink index: can we manage our agreements? Facilitator guide.* Organization Design and Development.

Gredler, M. E. (1992). *Designing and evaluating games and simulations*. London: Kogan Page.

Hermann, C. (1963). Some consequences of crisis which limit the viability of organizations. *Administrative Science Quarterly*, *8*(1), 61–82. doi:10.2307/2390887

Hiltz, S. R. (1978). The impact of a new communications medium upon scientific research communities. *Journal of Research-Communication Studies*, *1*, 111–124.

Janis, I. L. (1972). *Victims of Groupthink: A Psychological Study of Foreign Policy Decisions*. Boston: Houghton Mifflin.

Janis, I. L. (1982). *Groupthink* (2nd ed.). Boston: Houghton Mifflin.

Mayer, R. E., & Moreno, R. (2003). Nine ways to reduce cognitive load in multimedia learning. *Educational Psychologist*, *38*(1), 43–52. doi:10.1207/S15326985EP3801_6

McGrath, J. E. (1984). Groups: Interaction and Performance. Englewood Cliffs, NJ: Prentice-Hall, Inc.

Mclaughlan, R. G., & Kirkpatrick, D. (2005). *Online text-based role play-simulation: The challenges ahead.* Simulation Industry Association of Australia.

Miranda, S. M. (1994, February). A voidance of groupthink: Meeting management using group support systems. *Small Group Research*, *25*(1), 105–136. doi:10.1177/1046496494251007

Orasanu, J., & Fischer, U. (1997). Finding decisions in natural environments: the view from the cockpit. In C. E. Zsambok & G. Klein (Eds.), *Naturalistic Decision Making*. Mahwah, NJ: Lawrence Erlbaum.

Poole, M. S., & DeSanctis, G. (1992). Micro level Structuration in Computer-Supported Group Decision Making. *Human Communication Research*, *19*(1), 5–49. doi:10.1111/j.1468-2958.1992.tb00294.x

Portney, K. E., & Cohen, S. (2006). Practical contexts and theoretical frameworks for teaching complexity with digital role-play simulations. In S. Cohen, K. E. Portney, D. Rehberger, & C. Thorsen (Eds.), *Virtual Decisions*. Mahwah, NJ: Lawrence Erlbaum.

Rosander, M., Stiwne, D., & Granström, K. (1998). "Bipolar groupthink": Assessing groupthink tendencies in authentic work groups. *Scandinavian Journal of Psychology*, *39*(2), 81–92. doi:10.1111/1467-9450.00060 PMID:9676161

Salas, E., Bowers, C., & Rhodenizer, L. (1998). It Is Not How Much You Have but How You Use It: Toward a Rational Use of Simulation to Support Aviation Training. *The International Journal of Aviation Psychology*, *8*(3), 197–208. doi:10.120715327108ijap0803_2 PMID:11541532

Schneid, T. D., & Collins, L. (2001). *Disaster Management and Preparedness*. New York: Lewis.

Shrivastav, H., & Hiltz, S. R. (2013). Information Overload in Technology-Based Education: A Meta-Analysis. *Proceedings of the 19th Americas Conference on Information Systems. Overload in Technology-Based education*, 1–10.

Sniezek, J., Wilkins, D., & Wadlington, P. (2001). Advanced Training for Crisis Decision Making: Simulation, Critiquing, and Immersive Interfaces. *HICSS, 3*, 3042.

Wills, S., Leigh, E., & Ip, A. (2011). *The power of role-based e-learning: Designing and moderating online role play*. New York: Routledge.

Wills, S., & McDougall, A. (2008). Reusability of online role-play as learning objects or Learning designs. In L. Lockyer, S. Bennett, S. Agostinho, & B. Harper (Eds.), *Handbook of Research on Learning Design and Learning Objects*, *Issues, Applications and Technologies*. IGI Group. doi:10.4018/978-1-59904-861-1.ch037

Wills, S., Rosser, E., Devonshire, E., Leigh, E., Russell, C., & Shepherd, J. (2009). *Encouraging role based online learning environments by Building, Linking, Understanding, Extending: The BLUE Report*. Australian Learning and Teaching Council.

Winn, W. (1997, January). Advantages of a theory-based curriculum in instructional technology. *Educational Technology*, 34–41.

This research was previously published in Exploring the Cognitive, Social, Cultural, and Psychological Aspects of Gaming and Simulations edited by Brock R. Dubbels; pages 35-61, copyright year 2019 by Information Science Reference (an imprint of IGI Global).

Chapter 18
Transferability of Voice Communication in Games to Virtual Teams Training for Crisis Management

Jan Rudinsky
University of Iceland, Iceland

Ebba Thora Hvannberg
University of Iceland, Iceland

ABSTRACT

A crisis is an emergency event that can lead to multiple injuries and damage to property or environment. Proper training of crisis management personnel is vital for reducing the impact of a major incident. In search for knowledge on how best to implement communication for virtual environments for training, communication in online games was studied. Findings on voice communication in online games were researched and formulated as a set of statements. By asking participants in an empirical study of crisis management, the statements were either confirmed or refuted. Results show that multiplayer games are highly similar to the requirements for crisis management training in virtual environments. Approximately two-thirds of the statements proved coherent in both domains. The practical significance of this work lies in the provision of design implications for a virtual environment for crisis management training. Thus, this paper contributes to demonstrating the transferability between these domains. Finally, the paper reflects the results in theories of communication and engagement.

DOI: 10.4018/978-1-7998-2535-7.ch018

INTRODUCTION

A crisis is an emergency event that can lead to multiple serious or fatal injuries and can cause structural failure or damage to a property. A plane crash, an explosion or a fire at an airport are examples of such events in the aviation sector. To minimise personal injury and limit damage, any such emergency situation should activate a rapid and well-organised crisis management response. In scale and complexity, crisis events far exceed the cognitive and communicative resources of an individual (Greef & Arciszewski, 2007). Therefore, the response to a crisis must be managed by persons who are organised in teams that belong to emergency services such as Rescue and Fire fighters, Police or Paramedics. During crisis events information is provided in face-to-face conversation or by telecommunication channels, including radio and telephone systems and multimodal information technology.

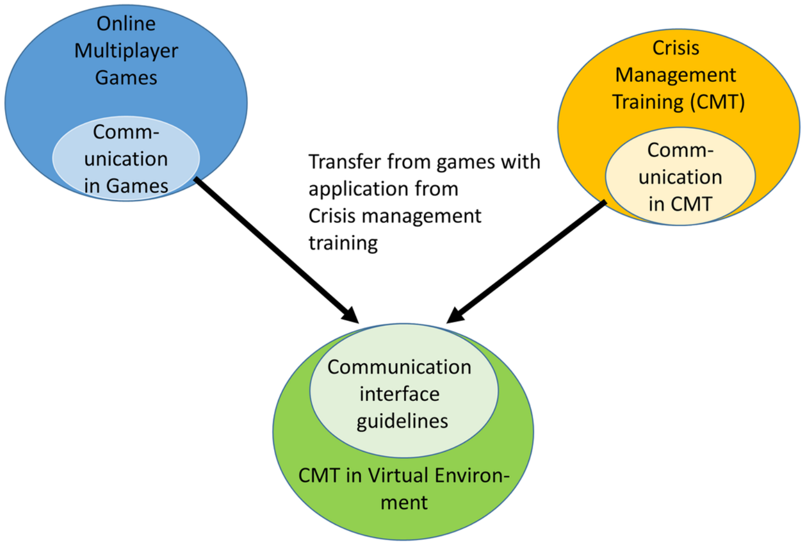
Communication and data flow between team members, e.g. first responders and commanders, is paramount and plays a crucial role through all levels of coordination (Cooke, Gorman, Myers, & Duran, 2013). A coordination structure is based on effective communication and must be deployed to drive the operation into the successful recovery of a normal situation. Examples of communication in crisis management include reports about incident scale and progress, requests for resources or information and task delegation. First responders and commanders on the scene share this information with each other and with remote command centres. Research has shown that training teams in communication skills and strategies can help them overcome hindrances in coordination (Salas, Cooke, & Rosen, 2008) but to achieve good team performance the communication training needs to be carefully designed (see (Adelman, Christian, Gualtieri, & Bresnick, 1998) and a meta-analysis of which factors improve team performance (Salas, DiazGranados, et al., 2008)) and that the design of technology needs to be founded in the needs and abilities of teams (Salas, Cooke, et al., 2008).

Motivated by the need for training of communication during crisis management, where the use of heterogeneous media and the requirement of reliable information delivery in crisis management is emphasised, we aimed to investigate the design of communication in a virtual training environment for crisis managers and first responders. Because real-life training for crisis management is expensive due to its complexity, temporal criticality and demands for resources, training in a virtual environment can be a favourable option. Predecessors of virtual environments were so called micro worlds that have been used for simulations and training (Brehmer & Dörner, 1993). Previous results of training in virtual environments have been obtained in domains such as crisis communication, decision making and emergency response (Haferkamp, Kraemer, Linehan, & Schembri, 2011), resource management (Heinrichs, Youngblood, Harter, & Dev, 2008), medical education (Creutzfeldt, Hedman, Medin, Heinrichs, & Felländer-Tsai, 2010; Grantcharov et al., 2004; Wiecha, Heyden, Sternthal, & Merialdi, 2010) and training airport emergency plans (Zarraonandia, Vargas, Díaz, & Aedo, 2009). However, reviews of the state of the art of virtual laboratories for education reveals that while communication and collaboration is one of four design criteria of virtual systems, only a few projects have fulfilled it completely (Potkonjak et al., 2016).

Virtual environments have been significantly influenced by online game technology during the past few years. Originally, developed for the purpose of amusement and recreation, games now offer training and educational opportunities, often termed serious games (Crookall, 2010). The evolution of gaming from a single player to an online multiplayer experience provides an opportunity to train for crisis management in a virtual environment. To enhance their chances of achieving a goal, players of multiplayer online games and crisis managers prefer to exchange information. In games, two modes of communication are normally used, text and voice. Typed text has been the traditional medium of communication, but the use of voice is on the rise, because speaking is a natural form of communication; speaking is faster than typing and allows for simultaneous use with other game interfaces such as a mouse or a keyboard (Wadley, 2011; Wadley, Gibbs, & Benda, 2005).

The purpose of this research was to exploit findings on communication in online games in the literature and life observations of crisis training to create guidelines for design of communication interfaces in a virtual training environment. We wanted to take advantage of the knowledge developed in games research, or what has been termed gamification by Deterding, Dixon, Khaled, and Nacke (2011), as "the use of game design elements in non-game contexts". The methodology applied in this study is depicted in Figure 1. We looked for findings on voice communication in online games in the literature and formulated as a set of statements. After inquiring about the experience of participants and observing their work practices in an empirical study of crisis management communication, the statements were validated. The results were used to create design guidelines for communication interface, usable for the development of Crisis Management Training (CMT) in a virtual environment. We will show that these guidelines can be applied in developing training systems in other safety critical domains. A secondary result of this study is how well findings on voice communication in online games fit for crisis management training in virtual environment.

Figure 1. A model of online games findings and applicability to the Crisis Management Training (CMT) environment



BACKGROUND

Safety-Critical Communication

One of the required components of crisis management is effective communication that must ensure reliable information delivery to the appropriate destination, carrying clear content with a satisfactory level of detail. In this respect, previous research addresses information exchange, media, and the repercussions of problems in communication.

Reliable information exchange is a significant activity for safety-critical communication. A study in the aviation domain showed that approximately three quarters of the errors on information exchange that were reported and assessed for situation awareness resulted from a failure to perceive information correctly; one-fifth of the errors were because of failing to fully comprehend a situation and only three percent of the errors were related to the projection of a future situation (Jones & Endsley, 1996). This model of situation awareness consisting of perception, comprehension and projection is a fundamental one for system design, but it needs to be expanded to include team situation awareness. Although most of the research on situation awareness has been conducted in the area of aviation, it has spread to other domains, which then prompts addressing unique situational awareness challenges (Endsley & Jones, 2013).

The use of different media and their impact on work has been studied in the literature. In the theory of communications grounding, Clark and Brennan (1991) introduced characteristics of different media and described their influence on information delivery and understanding. These media characteristics and their importance for safety-critical communications were evaluated in a field study of communication in the oil-drilling industry (Bayerl & Lauche, 2010). The study showed that compared to media like phone, e-mail and audio, more recently adopted ICT media, such as video and desktop sharing, did not have a radical impact on team coordination, but resulted in modification and adaptation of existing routines.

Problems in communication can have various implications for team performance. A field study and literature research (Bharosa, Lee, & Janssen, 2010) found that a lack of information sharing among response agencies can cause major problems such as a negative influence on collective decision-making and the coordination of action. The results showed that problems occur at all levels of coordination (individual, team, and agency), and thus, they must be tackled at these levels simultaneously. A descriptive study of the challenges of communication in emergency response (Manoj & Baker, 2007) identified three problem types: 1) technological challenges, such as rapid deployment of a communication system or multi-agency interoperability; 2) sociological challenges, including the sharing of information or the lack of a common vocabulary; and 3) organisational challenges that vary with respect to changes between hierarchical, flat or hybrid organisations. We will address these again in the discussion of the results.

Crisis Management Training

Training provides the opportunity to evaluate options, while a lack of training will cause delays with negative consequences for casualties in a real-life situation. Training should expose responders to a range of situations that are based on potential scenarios that could occur in their jurisdiction. People who learn how to solve a complex situation during a training exercise can respond more efficiently during a real-life event compared to those without the training (Jain & McLean, 2005; Klein, 1993).

The ability of teams to coordinate their actions effectively determines the success of crisis management (Toups, Kerne, & Hamilton, 2011). Security, medical, rescue and fire-fighting teams that are deployed at the site of an incident have different professional backgrounds and have varying skills that are acquired in individual and team training. Therefore, in inter-team training responder teams could develop similar mental models, allowing emergency managers to establish comparable approaches towards the teams and towards responders within the teams. Coordination of skills that should be taught include information exchange, decision making, causal analysis and prediction of situation development. Training in communications is fundamental to the training of coordination skills.

A valuable training method for emergency preparedness in the aviation sector is a full-scale exercise. A large-scale, multi-agency, real-life exercise improves crisis coordination and communication in close-to-real environment training conditions and results in thorough preparation across professional domains. However, the exercise requires a considerable number of personnel and substantial organisational complexity, which imply significant financial and temporal demands. Such an exercise is typically carried out every two years in the aviation sector, but because of a lack of resources the interval can be almost doubled. While a large-scale exercise can yield credible results, a subset of the required skills can be obtained by performing a simpler table-top exercise. Such an exercise requires only the team commanders' participation and less preparation time and resources, and it provides the advantage of testing hypothetical situations without causing disruption in the community. Typically, every year, airport crisis management trains in such exercises. Because of the complexity and cost of comprehensive real-life training, the most frequent training method to date is an individual exercise, comprising several subtasks, that does not require coordination with others and which a trainee repeatedly practices to solidify emergency response skills.

Training in a Virtual Environment

With the fast development of virtual environment technology, especially in the gaming industry, a number of opportunities have arisen to exploit it for training. A digital game that is designed with the intent of learning and entertaining has been termed a serious game (Johnston & Whitehead, 2009; Zyda, 2005). Boyle et al. (2016) have done a systematic literature review of the impacts and outcomes of serious games. Their results show that positive impact of serious games is increasing. The study concluded that games mainly support knowledge acquisition, although some examples could be seen where games support skill acquisition or collaborative interactions. It is likely that before games can support training of these skills, we will need further research on instruments that support communication.

Training in a virtual environment can reduce the costs to one-tenth compared to live exercises (Jain & McLean, 2005). A trainee in a virtual environment is allowed to train more frequently during a time that is suitable for his or her work, and trainees who are distributed in distant geographical locations can still cooperate in a collaborative training environment. Most importantly, the use of virtual environments allows responders to gain experiences from many different scenarios. They can be easily prepared based on a template and later reused without the need to organise resources, such as in a real-life exercise. In turn, a virtual environment will significantly shorten the preparation time and expand emergency preparedness. Finally, a virtual environment has the possibility of real-time observation of multiple trainees, which makes the after-action review and debriefing fast and accurate.

RESEARCH METHODS

As mentioned in the introduction, the research study had two parts. First, we collected data from the crisis management area and how it is practiced. The next subsection describes how this data was collected. Second, we derived knowledge about communication in online games and formulated statements from the literature. The second subsection describes the literature analysis and how the groups of statements were derived. Third, we used the data collected from crisis management to validate the statements derived in observation of crisis management training to learn whether they could be valuable for developing a CMT system. The research process is described in Figure 2.

Data Collection

Data on how crises are managed were collected from three European Incident Command Systems (ICS) over a period of nine months. Three examples of crises were provided, as described in Table 1. Four rounds of data collection were conducted to learn about crisis incidents, roles, tasks, procedures, artefacts and contexts at

Figure 2. Study process – data collection and analysis

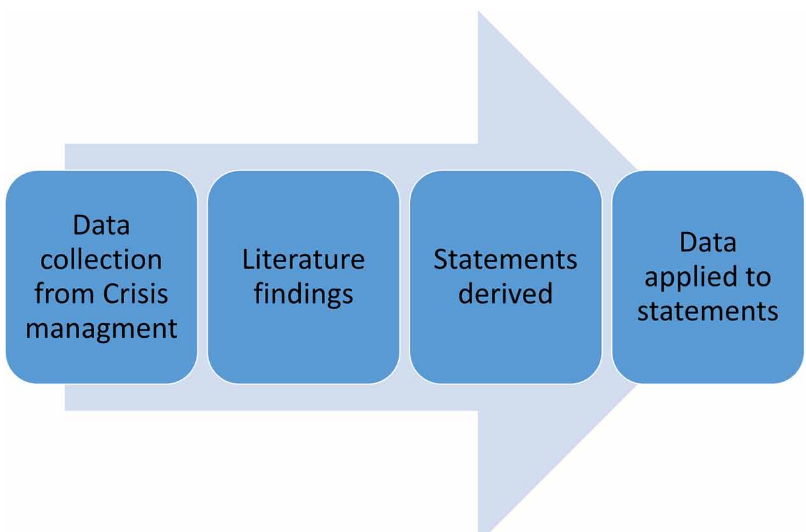


Table 1. Crisis examples

Incident	Description
Aircraft incident	An aircraft accident when engine failure caused a crash landing at an airport
Bomb threat	A deliberate incident of a bomb explosion in an airport building
Train crash	A train and vehicle collision at a railway crossing due to faulty signaling

the three sites. The data collection instruments used included site visits, elicitation workshops, observations of training exercises and end-user sessions.

During initial site visits, crisis training managers of each ICS introduced a command and a coordination structure and provided an overview of procedures, roles, their responsibilities, physical contexts and current training methods. The data were elicited during site visits to airports, train stations and emergency response agencies.

The second round of data elicitation was held at all three sites, comprising informal discussions and semi-structured interviews with crisis management personnel across field and all command levels. There were 38 participants with roles ranging from a first responder to a national commander. Workshop discussions lasted approximately an hour and were followed by semi-structured interviews that lasted up to three hours. The interviews recordings contained a description of specific roles and their responsibilities, participants' experiences from real-life incidents and training that took place.

Two types of crisis management training sessions were observed in the third round of data elicitation at one of the sites. The first was a table-top exercise that used a simulated scenario (i.e. an aircraft incident), allowing crisis managers to train for communication and coordination. We observed two table-top exercises, each lasting approximately one hour.

The second type of training session was a large-scale, multi-agency, live training exercise that took place in a small rural airport. The training session involved approximately fifty participants across four different emergency response agencies (fire fighters, ambulance, police and volunteers acting as casualties). The data described the physical context of the crisis management, including environments and artefacts, and the social context, such as the interaction between people in different roles and their coordination. Further information was solicited in semi-structured interviews with the exercise participants. Three persons provided their own experience, which represented multiple roles, ranging from a first responder to an on-scene commander. Thirty-four interview questions were organised into groups of current practices in crisis management, verbal communication, and problems encountered during communication.

Informal discussions and semi-structured interviews were a part of the third round of elicitation which was conducted with the crisis training managers at all three sites and took half a day at each site.

To better understand the roles of agencies during crisis management, a set of procedures and manuals about the incident command systems was collected. The documents provided additional information about the command structure and overall agency roles and responsibilities. Table 2 gives an overview of the instruments and materials that were collected at each event and incident type.

Derived Statements from Online Game Research

To review research results on communication in online games, we searched ACM, IEEE and Springer digital libraries with the keywords voice and communication in combination with video games, serious games and collaborative virtual environment. After an analysis of the retrieved papers, several subtopics of communication emerged that were organised into seven groups relevant to communication in virtual environments. These groups are Media richness selection, Groups of people, Identities of people, Avatar behaviour, Learning, Trust and the Problem group. The main ideas were consolidated within each group and formulated into statements that we attempted to verify from the crisis management perspective (see next section).

We refined the set of statements by selecting only the statements that had the following characteristics: 1) Applicable to crisis management or to training, 2) Reliable and backed by multiple references, and 3) Validated easily by empirical data. A simple scoring method was applied, in which each of the above-mentioned characteristics resulted in the corresponding statement earning one point. Ten statements, those with the highest scores, were selected from the 19 original statements and are identified with a number in the last column, as shown in Table 3. All except one of the seven groups were retained, but the group Trust did not contain any statements after the validation.

RESULTS

The data collected during the elicitation of requirements to the crisis management training environment were used to verify the statements derived in the previous section. The data were analysed for validity of the statements using the following criteria:

- Do the data support or refute the statement?
- Do the data call for modifying or creating a new statement?
- If the statement is refuted, can it be explained by differences in the two domains, games and crisis management training?

Table 2. Material collected from stakeholders for each incident case

Source	Participants		Method	Collected Data	Data Content
	Role	Agency			
Site visits	Crisis managers	Airport operators	Presentation	Presentation	Crisis organisation structure, procedures. Introduction to: roles, resources, responsibilities, physical context, current training
			Discussion	Interview recordings	
		Railways police force	Unstructured interview	Notes	
Elicitation workshop	First responders	Police force Fire fighters	Discussion	Discussion recordings	Roles and responsibilities. Real-life training and experiences (partial focus on communication)
	Commanders	Medical service Search and Rescue	Semi-structured interview	Interview transcripts	
Observation	First responders	Police force	Observations of: real-life, exercise, table-top exercise and emergency service premises	Videos	Physical context: environment, resources. Social context: roles, interaction and coordination. Training prep. and evaluation
		Fire fighters Medical service			
	Commanders	Search and Rescue		Photos	
		Emergency centre (112 /911)			
		Airport operator Civil Protection			
Interviews	First responders	Police force Fire fighters	Structured interview	Interview recordings	Roles and responsibilities (focus on communication)
	Commanders	Search and Rescue			
Evaluation session	Crisis managers	Airport operators	Semi-structured interview	Interview transcripts	Verification of details of: roles, responsibility, environment, communication
		Railways police force			
Manuals		Airport operators, Railways police force		Emergency plans	Roles, procedures, tasks (partial focus on communication)

Table 3. Statement selection based on: Applicability (A), Reliability (R) and Validity (V)

Group / Statements	Score				Statement No.
	A	R	V	Sum of Scores	
Media Richness Selection					
The social richness of the communication medium must be matched with the task characteristics (urgency of the task or cues necessary to perform the task), fellow communicators (number of communicators, their preferences and their required presence) and a person's organisation or users' prior experience with the medium (Sallnäs, 2002; Tan, Tan, & Teo, 2012; Wadley, Gibbs, & Benda, 2007).	1	1	1	**3**	**1.**
Leaner medium (e.g. text) can cause impulsive or reserved behaviour, but can be used as a medium for initial contact (e.g. with unknown participants) or for asynchronous communication that allows easy information processing (e.g. search in conversation history) (Halloran, Rogers, & Fitzpatrick, 2003; Wadley et al., 2007; Wadley, Gibbs, & Ducheneaut, 2009)	1	1	0	**2**	**2.**
Currently, there are four metaphors for designing voice channels in games: broadcasting, landline, mobile phone, and proximity voice chat (Wadley et al., 2005).	1	0	1	**3**	**3.**
Solving tasks (e.g. making a decision) through CMC takes twice as long as F2F but with half of the utterances and gives the same result. However, in F2F, socio-emotional functions are more frequent (as well as with voice compared to text), which has a negative impact on group effectiveness (Li, 2007).	1	0	0	**1**	**-**
Voice compared to text communication improves performance and social experience. Video does not add significant advantages to task performance compared to audio, but video supports informal communication and relation building (Sallnäs, 2002).	1	0	0	**1**	**-**
Preference for anonymity is one of the main reasons that is cited by Second Life users for rejecting voice (Wadley et al., 2009).	1	0	0	**1**	**-**
Using verbal communication, especially real voice, can break the sense of immersion in a game (Bartle, 2003).	1	0	0	**1**	**-**
Groups of people (players/trainees)					
Voice communication that simulates a radio channel is most useful for a small group of players (6-10) who know each other and are playing a fast-paced game, to coordinate their tactics (issue directions, call for help) and achieve a goal while moving around a geographical area. However, as players reported, the use of multi-channels can cause fragmentation of the party into sub-teams (Raybourn, 2007; Wadley et al., 2007). Voice does not scale well to large groups (Wadley, Carter, & Gibbs, 2015)	1	1	1	**3**	**4.**
Proximity voice chat, which is a virtual metaphor for face-to-face in the real world, may be necessary where a large number of players would clutter a shared radio channel, players are close to each other in the virtual environment, and the benefit of cues that indicate which direction a sound is travelling from outweighs the inability to speak with distant players (Gibbs, Wadley, & Benda, 2006). Proximity chat enables enjoyable game play experiences and user interactions (Carter, Wadley, & Gibbs, 2012)	1	0	1	**2**	**5.**
The proximity of other players' avatars is the most useful learning aid for the less experienced gamer, who could follow their actions and speech to find out how the game works (Halloran et al., 2003).	1	0	0	**1**	**-**

continued on following page

Table 3. Continued

Group / Statements	Score				Statement No.
	A	R	V	Sum of Scores	
Identity of people (players/trainees)					
Players engaged in a virtual environment had difficulty identifying who was speaking, determining who could hear what they said and knowing whether it was heard at all. Players reported that the voice channel had inadequate facilities to control what was heard and what was sent and that it introduced delay. As a result, it can inhibit convivial computer-mediated social interaction (Gibbs, Hew, & Wadley, 2004; Gibbs et al., 2006; Wadley et al., 2009). Voice reveals identity better than text which makes it more sociable but can interfere role-play and pseudonymity (Wadley et al., 2015).	1	1	1	**3**	**6.**
Not knowing who is talking in a distributed player setting can have a negative effect on learning and coordination in team-based war games (more/longer utterances to find out who is present, what is their level of skills or to address the person). On the other hand, knowing a partner results in fair decision making (Halloran, Fitzpatrick, Rogers, & Marshall, 2004; Halloran et al., 2003; Yamamori, Kato, Kawagoe, & Matsui, 2008).	1	1	0	**2**	**7.**
Avatar behaviour					
Where visual representation is available (e.g. videoconference, collaborative virtual environment), verbal actions should be coupled with postural, gestural and proximity information of the player embodiment. This information can help identify the speaker and can increase communication during participants' performances (Cassell & Thorisson, 1999; Cheung, Chang, & Scott, 2012; Chodos et al., 2010; Halloran et al., 2003).	1	1	0	**2**	**8.**
Learning					
Communication in a virtual world not only provides experience of the participant's own area but also provides experience in a variety of other areas (Chodos et al., 2010; Raybourn, 2007).	1	1	1	**3**	**9.**
Development of a training game should focus on communication principles (rather than domain-specific knowledge). Such development ensures that the training content is general enough to be applicable to all students (who can switch roles) and still be meaningful (by seeing role conflicts) and useful (Chodos et al., 2010).	0	0	1	**1**	**-**
Trust					
Trust is higher in a smaller group (e.g. a guild in WoW) and it depends on the interdependence of members, the persistence of their identity, and the strength of reputation systems within the group. Voice chat was not related to the trust of others in the game; it was related to trust in guild members. Self-disclosure was positively related to trust, but a higher number of public messages sent does not reveal trust to a group (Ratan, Chung, Shen, Williams, & Poole, 2010).	1	0	0	**1**	**-**
Problems					
Players reported a number of voice communication problems (e.g. speech not intended for the listener, background talk, natural or synthetic noise, intentional or unintentional), which caused lower usability (Gibbs et al., 2004).	1	0	1	**2**	**10.**
Where a specific domain exists (i.e., a limited domain), a conversational entity can be represented by a computer (Gustafson, Boye, Fredriksson, Johanneson, & Königsmann, 2005).	1	0	0	**1**	**-**
Players reported voice communication problems with synchronicity (e.g. one party out-of-game for a moment) or identity and privacy issues causing a performance decrease (Sallnäs, 2002; Wadley et al., 2007).	0	1	0	**1**	**-**

In the following subsections, we present the results of this analysis by answering the above questions for each of the ten statements. Furthermore, we provide guidelines for design of a crisis management training virtual environment.

Media Richness Selection

The first group of statements describes media richness selection and its relation and influence on communication in a virtual environment. Media richness refers to its capacity to process rich information and its ability to provide immediate feedback (Daft & Lengel, 1986).

Selection of Media is Based on Tasks, Fellows, Organisation, and Prior Experience

Statement 1: The social richness of the communication medium must be matched with the task characteristics (urgency of the task or cues necessary to perform the task), fellow communicators (number of communicators, their preferences and their required presence) and a person's organisation or users' prior experience with the medium (Sallnäs, 2002; Tan et al., 2012; Wadley et al., 2007).

Selection of a channel as a communication medium that is based on task characteristics has been identified in several cases, where a commander selects a channel based on the importance of information, message content, intended call length and to convey essential emotions or to avoid recording.

Selection of media richness based on fellow communicators has been confirmed by several examples including using a leaner medium to address many people, alerting a commander with multiple messages intended for lower level command to ensure delivery, and selecting face-to-face conversation for sensitive information delivery to the next of kin, in addition to selecting a phone to call the emergency centre rather than contacting an on-scene commander because of the estimated availability (busy or free) of the recipient and, finally, by responders selecting a person to talk to, based on his/her level of domain knowledge.

The selection of a channel that is based on organisation guidelines has been confirmed by airport emergency plans, police force guidelines, emergency manuals, commanders and first responders who are reporting. These findings indicate the strong influence of pre-defined methods of communication over other characteristics such as task characteristics or the fellow communicators, named in statement one. The selection of a channel that is based on prior experience has been confirmed by commanders that select a mobile phone over radio because of habit.

Furthermore, the data revealed that statement one could be extended by the channel availability and the type of training instrument that determines the richness of the selected medium. An example of the latter is when the rules of the exercise (e.g. a table-top exercise) prohibit a person from speaking when someone else is talking.

Our conclusion was that statement one was confirmed by the data, and it can be applied when designing a crisis management training environment. Table 4 provides design guidelines derived from this statement, which can be used for the training environment. It describes media from high to low richness and their use in crisis management. Additionally, a leaner medium can be used as a simultaneous channel with a richer medium.

Although the selection of media richness in crisis management should be guided by organisational procedures, the official communication structure can be bypassed for sensitive, technical or longer calls. In addition, the training conditions may allow for higher media richness than real-life.

A Leaner Medium Can Cause Impulsive or Reserved Behaviour but Can be Used for Initial Contact or for Asynchronous Communication

Statement 2: A leaner medium (e.g. text) can cause impulsive or reserved behaviour, but can be used as a medium for initial contact (e.g. with unknown participants) or for asynchronous communication that allows easy information processing (e.g. search in conversation history) (Halloran et al., 2003; Wadley et al., 2007; Wadley et al., 2009).

Table 4. Design guidelines on the selection of media richness

Richness	Medium	Purpose
High	Face to face	Communication at a command centre
		Highly sensitive information
	Radio	Negotiation of resources
	Radio or phone	Highly important information
		Verification of information received through leaner medium
	Phone	Alert high level command
Low	Video link	Monitor a scene
	Radio	Monitor a channel
	Text	Address a number of people
		Deliver large data sets

The use of a leaner medium for asynchronous communication has been confirmed by commanders and first responders using personal and command centre logs, setting up a responder status on a radio device and by high-level commanders who use asynchronous communication for regular updates between command centres with emails or web-based logs. The use of a leaner medium for asynchronous communication and initial contact has been confirmed by observing participants who send text or a pre-recorded voice message during an alert procedure.

The use of a leaner medium for information processing has been confirmed in manuals and by commanders' statements. The manuals state that command centre communication must be recorded and logs can be processed at any time. Commanders and first responders report that communication is recorded for later information reuse. The commanders move from voice to text for communication between command centres because text enables recording and information processing at a suitable time and requires less attention. Moreover, the commanders stated that they take notes in personal logs that are later used for briefing others or answering questions about an incident, and they issue regular updates in the command centres that are used for press releases.

The above analysis has required modification of the statement in several ways. First, the statement should be amended to include the use of leaner medium and asynchronous communication as a back-up channel for voice. Second, the statement should be revised to include the use of verbal communication instead of text under stressful conditions. We have not observed any evidence of impulsive or reserved behaviour when using leaner media and, therefore, a part of the statement is refuted.

To summarise, the statement has been confirmed partially. The difference between crisis management and games lies in the characteristics of crisis management that means that, in crisis management, participants cannot allow themselves to show impulsive or reserved behaviour. Furthermore, the reliability needed in crisis management requires back-up channels, and stressful situations will affect which medium is selected. Table 5 describes the design guidelines for leaner media use.

Table 5. Design guidelines for leaner media

Medium Richness	Purpose
Leaner media	Logging of actions and decisions Transcription of radio communication Access to operation log for a commander Back-up channel for voice communication Communication between command centres Setting up a responder status

Four Metaphors for Voice Channels

Statement 3: Currently, there are four metaphors for designing voice channels in games: broadcasting, landline, mobile phone, and proximity voice chat (Wadley et al., 2005).

The use of a broadcasting channel (i.e. push-to-talk radio) was confirmed by the commanders and first responders, who reported frequent use of different forms of radio (e.g. a personal device, car radio or public address systems) for communication with distant members in crisis management or during training. Moreover, this was confirmed by lower-level commanders on the scene, who reported the use of two radio channels simultaneously to filter information from a lower level before sending it to a higher level command.

Face-to-face communication that can be represented by a proximity chat in the virtual environment has been confirmed by commanders and responders' reports about exchanging information face-to-face in the command centre and on the scene and further by observations of first responders and lower-level commanders on the scene during a real-life exercise.

The use of mobile phones or landlines has been confirmed by experienced commanders, who acknowledged mobile phone use for inter-agency coordination and by commanders and first responders, who said they used them in the case of a radio system failure, and further by teams of commanders and responders, who said they were not equipped with radio and who used mobiles or landlines as an alternative means of communication or to deliver sensitive messages. Finally, manuals indicated their use in certain phases of the response, e.g. during an alert, but some report that landline phones have been replaced by radio to call national emergency services.

The use of radio broadcasting, mobile phones and landlines has been confirmed by procedures presented by crisis managers (e.g. an alert procedure) and by observations of air traffic controllers and emergency service centre operators who showed regular use of radio and phone.

The statement should be modified to include a simultaneous use of two channels, e.g. two radios, and it should be modified to include channel re-configuration such as a change from broadcasting to mobile phone.

The conclusion from this analysis is that crisis management communication can take full advantage of current metaphors of voice channels in team-based games. The broadcasting channel could carry Push-to-talk radio and Public Address communication, the proximity chat could emulate face-to-face conversations, and the mobile and landline phone channels could be used as an alternative form for information exchange. The design guideline from statement three are described in

Table 6. Design guidelines for metaphors

Design Metaphor	Represented By	Extensions
Broadcasting	Push-to-talk personal or car radio (portable) Public address system (fixed location)	Push-to-talk radio should be reconfigurable and allowed to change between channels
Mobile	Personal portable embodiment Call, text or pre-recorded voice message	Backup to broadcasting
Landline	Fixed location embodiment	
Face to face	Proximity chat	Backup to broadcasting

Table 6. Depending on the context, simultaneous use of multiple channels or an alternative medium (mobile phone as a backup of radio) should be offered.

Groups of People

The category groups of people define the correlation between the communication channel selection and the organisation of the participants within a group.

Radio for Small Groups

Statement 4: Voice communication that simulates a radio channel is most useful for a small group of players (6-10) who know each other and are playing a fast-paced game, to coordinate their tactics (issue directions, call for help) and achieve a goal while moving around a geographical area. However, as players reported, the use of multi-channels can cause fragmentation of the party into sub-teams (Raybourn, 2007; Wadley et al., 2007). Proximity chat enables enjoyable game play experiences and user interactions (Carter et al., 2012).

The sharing of a simulated radio channel by a small group that was participating in fast-paced activities and coordinating tactics was confirmed by the observation of five participants in a table-top exercise. The sharing of a simulated radio channel by a small group to coordinate tactics while moving around an area was confirmed by training managers and commanders. The training managers' presentations offered the use of radio in a fully connected network (everyone talks to everyone) and a tree topology (e.g. one-to-many). The commanders on the scene and in the regional command centre reported being in charge of a group of five to ten people during a real-life crisis or training, which was also confirmed by observation during a large-scale exercise.

The fragmentation of a party into sub-teams by the use of multi-channels has been rejected by manuals, which state that members of a particular group (e.g. Medical or Police) must use a single channel and by the fact that only on-scene commanders were observed to use two radios simultaneously in a large-scale exercise. By doing so, they connect two groups of different command levels.

These statements should be extended to include the possibility of a participant's need to step-out of the communication temporarily. Communication during crisis management can be stressful, and a commander may need to step-out for the purpose of processing information or making a decision. Communication can also exceed the capability of a single person when monitoring multiple channels. In those cases, a representative person is appointed to monitor the communication and to ensure that no information was missed by regularly reporting to the commander. Whether or not knowing each other has an impact on the communication, is analysed in statement seven.

The conclusion from the analysis of statement four is that the use of radio in crisis management highly resembles voice communication, simulating a radio channel in games. Radio is used for coordination of tactics among a small group of responders, who move around an area during a fast-paced action. The main difference observed between games and crisis management was that the inherent organised structure of crisis management mitigated the threat of group fragmentation. However, in cases where a channel becomes overloaded with information, an auxiliary is appointed to listen to the channel. Due to stressful situations in crisis management, it has proven necessary for commanders to step back and take a break from communication. Thus, crisis management has built-in measures to address information overload, whereas games do not. The design guideline from statement four are described in Table 7.

Table 7. Design guidelines for small groups

Metaphor	Purpose	Configurability
Radio	Communication in a small group	Fully connected member or a tree topology
	(5-10 people)	One or more instances
		Turn off or assign to another person
Radio and face-to-face	Information relay by a single person	

Proximity Chat

Statement 5: Proximity voice chat, which is a virtual metaphor for face-to-face in the real world, may be necessary where a large number of players would clutter a shared radio channel, players are close to each other in the virtual environment, and the benefit of cues that indicate which direction a sound is travelling from outweighs the inability to speak with distant players (Gibbs et al., 2006).

The use of face-to-face communication by people who are close in the (real) environment and who benefit from cues of sound direction has been confirmed by observations of training and during interviews. The observation showed that small teams of first responders communicated face-to-face frequently during the large-scale exercise. During the interviews, commanders reported frequent use of face-to-face in command centres. When within a close distance of each other on the scene, they preferred face-to-face communication over the use of radio.

The prevention of channel cluttering was refuted by commanders, who stated that the size of a face-to-face group in a command centre is similar to the size of a group that shares a radio channel (5-10 people), and then by commanders in a control room who said they decide on a radio channel configuration that prevents congestion.

In addition to the above confirmation and refusal of the statement, the data indicated that modification is needed. It has to be tailored to regular meetings between commanders and adopted to environmental and technological constraints. Hence, as reported by commanders from different response agencies, the statement should be modified to include the use of face-to-face communication for regular meetings between commanders on the scene. Furthermore, the statement should be modified to include the use of face-to-face communication because of environmental constraints. For example, the use of radio becomes difficult in a noisy environment (machine noise or wind), where the commanders report to meet each other and talk face-to-face instead. Finally, the statement should be modified to include speaking face-to-face as a backup for technology failure or unavailability. For example, when radio fails, the commanders meet face-to-face to exchange information and coordinate response.

Statement five was confirmed, but with the exception of the cluttering of a shared radio channel, which is avoided in crisis management by certain communication configurations. Also, instead of filtering out the number of people on the channel, in crisis management, face-to-face communication is used when talking to people within reach. The benefits of face-to-face communication are enjoyed by first responders and commanders, and face-to-face communication is preferred over radio. Again, in this statement, we see the differences in the two areas emerging in the inherent structures

Table 8. Design guidelines for proximity chat

Metaphor	Purpose	Trigger of Proximity Chat
Face-to-face	Small group of 5-10 people who work on the same task and are close	Characters get close in virtual environment Regular time intervals Noise can make radio communication difficult and hence a face-to-face meeting is required. As a backup when there is technology failure, e.g. radio fails.

of crisis management. Furthermore, the required reliability of crisis management and the difficult working surroundings, which are affected by synthetic or natural noise due to extreme weather, distinguishes crisis management from games. The design guidelines implied from statement five are described in Table 8.

Identity of People

The identity of people group focuses on identity management and addressing people during communication in a virtual environment.

Addressing People and Channel Control

Statement 6: Players engaged in a virtual environment had difficulty identifying who was speaking, determining who could hear what they said and knowing whether it was heard at all. Players reported that the voice channel had inadequate facilities to control what was heard and what was sent and that it introduced delay. As a result, it can inhibit a convivial computer-mediated social interaction (Gibbs et al., 2004; Gibbs et al., 2006; Wadley et al., 2009). Voice reveals identity better than text which makes it more sociable but can interfere role-play and pseudonymity (Wadley et al., 2015).

The problem of identifying who was speaking has been refuted in crisis management by three indicators. The commanders and training managers and crisis management procedures reported the use of call signs. Then commanders stated that they know each other and those (at a certain level) who knew each other were able to recognise each other's voices. Finally, the use of one-to-one communications such as landlines, mobile phones, radio between two persons/command centres and radio display help with the identification of a speaker.

However, the problem of identifying who was speaking has been recognised when the participants occasionally forgot to use call signs. One of the causes was a lack of training. Another one was that participants started to introduce themselves too early, and the first two seconds of the radio speech are not transmitted.

The uncertainty that a message has been received was refuted by the following statements. First, response agencies confirmed reception of an alert message and, when unsure, they called back. Then, personnel at the command level regularly confirmed the message reception and the personnel called by a call sign replied using the call sign of the origin. Finally, during the real exercise a commander on the scene could perform a visual check to see whether a task had been performed as requested and during a table-top exercise visual cues (e.g. nodding) were sent out in simulated radio communication. Uncertainty about message delivery was supported by first responders on the scene, who did not confirm the reception of a message.

The problem of identifying a message recipient has been refuted by speaking to a specific person using a call sign or addressing all of the receivers who use or monitor the channel. The problem of controlling the communication channel has been refuted by the use of appropriate devices (discussed in statement three), the use of push-to-talk radio, where speaking occurs only when a button is pressed and speaking on a selected channel only. Finally, the problem is refuted by commanders, who have stated that problems with channel control depend on a person's individual skills, his or her age and previous skills.

Certainly, as described by statement six, there is a difference between games and crisis management with respect to voice communication. Although there was some contradictory evidence, we concluded that problems with the identification of who is speaking or addressed, whether the message is delivered or how to control the channel, have been mostly refuted. Additionally, the findings on communications in crisis management did not reveal any inhibited interactions or any indication of delay caused by inadequate control. Thus, we can conclude that this statement does not apply to crisis management. Again, the reason is the difference in the inherent communication protocol of crisis management. From the analysis of this statement, we suggest further design guidelines as presented in Table 9.

Table 9. Design guidelines for addressing people and controlling channel

Metaphor	Type of Control
One-to-one (mobile, landline, face-to-face)	Select recipient Indicate source of communication
Broadcasting	Use of call signs Push-to-talk functionality Should allow recipient to contact the source Voice recognition not considered relevant
All voice metaphors	Avatars should be anonymized for voice

A Player's Identity Affects Learning and Coordination

Statement 7: Not knowing who is talking in a distributed player setting can have a negative effect on learning and coordination in team-based war games (more/ longer utterances to find out who is present, what is their level of skills or to address the person). On the other hand, knowing a partner results in fair decision making (Halloran, 2009; Halloran et al., 2004; Yamamori et al., 2008).

We could not validate the effect of unknown identity on learning and coordination because, as stated in statement six, first responders and commanders know whom they are talking to. However, we can say that, in a single interview, a crisis commander confirmed good coordination between response agencies in which commanders know each other. This is in accordance with (Wadley et al., 2015) who states that identifying someone by voice makes the communication more social. An implication for design from this statement is that, for training purposes, avatars should be anonymised (see Table 7). All of the players will then have the opportunity to follow the training procedures and practice role-play without someone having the advantage of knowing others.

Avatar Behaviour

Because players in a virtual environment are represented by avatars, the group avatar behaviour queries the visual appearance of the virtual character and the embodiment of non-verbal communication functions.

Coupling of Players' Verbal and Visual Actions

Statement 8: Where visual representation is available (e.g. videoconference, collaborative virtual environment), verbal actions should be coupled with postural, gestural and proximity information of the player embodiment. This information can help identify the speaker and can increase communication during participants' performances (Cassell & Thorisson, 1999; Chodos et al., 2010; Halloran et al., 2003)

The coupling of verbal and visual representation has been confirmed by several cases where commanders' actions were visibly coupled with verbal description during a table-top exercise and by a commander pointing to a location on the scene while tasking first responders during a real-life exercise. Because we conclude that statement eight has been validated in crisis management, we can recommend that proximity chat in a virtual environment should allow gestures.

Learning

The learning group focuses on the training aspects that communication provides in a virtual environment.

Experience Sharing

Statement 9: Communication in a virtual world not only provides experience of the participant's own area but also provides experience in a variety of other areas (Chodos et al., 2010; Raybourn, 2007).

Provision of experience from other roles has been confirmed by observations of real-life exercises and by interviews on crisis management training.

They indicated that the coordinators learn about the other teams' tasks while monitoring a shared communication channel, Police learn about Fire fighters' needs while making a secure area for them, Police teams learn about each other's methods while negotiating security responsibilities, and Police learn about the medical domain while organising casualty transport with a medical team. Then the responders, who change roles during incident response, also learn skills in the new field (e.g. fire fighters as medics).

Although, as one commander said, a person learns through the scenario itself, he or she mainly learns from the discussions that take place in the training room and in the plenary meetings. Furthermore, commanders prefer to get to know each other well and to learn their roles in a large-scale exercise and one commander pointed out that training can fight off rivalry between coordinating teams.

Thus, a number of examples have validated this statement. We concluded that experience sharing is important in crisis management and that there are ample opportunities for learning from each other, about procedures, situations and roles. The reason that experience sharing is particularly important is that, especially in smaller locations, human resources are scarce, making it important for a person to perform the tasks required in different roles. For example, a fire fighter who participates in a rescue by fighting fire may later be triaging patients or driving an ambulance. We did not see the need to propose a design guideline from this statement. Communication, as we have described it until now, facilitates experience sharing.

Problems

The final group, the problem group, contains statements that point to technical or contextual problems.

Problems of Voice Communication

Statement 10: Players reported a number of voice communication problems (e.g. speech not intended for the listener, background talk, natural or synthetic noise, intentional or unintentional) which caused lower usability (Gibbs et al., 2004).

The communication hindrances such as environmental noise or unrelated conversation were confirmed by all of the participants including training managers on the scene or in a command centre during a large-scale exercise, and confirmed as well by commanders who had reported experiencing problems with environmental noise, which is louder on the scene and lower in the command centre. One commander reported special communication training, teaching how to deliver a clear message.

Because several additional types of problems were observed in crisis management, a few amendments to statement ten were required. Some of the issues have been mentioned in previous sections but appear here again. Examples are technical constraints and the context of the crisis. Other examples are new but draw their characteristics from the nature of the crisis management, e.g. the need for concise expression and the need for high reliability. Yet others result from the heterogeneous background of the large number of participants and require accessibility of the technology to all regardless of their background and abilities. First, the statement should be modified to include the problems that are related to the use of the channel, such as unanswered calls, unsatisfied requests for information or selection of an incorrect communication channel. Second, the statement should be extended to include the use of multiple channels simultaneously (e.g. using two radios). Third, the statement may be modified to include channel liability due to technical or contextual problems (e.g. a handheld radio on the scene is subject to environmental noises, or certain technology may be liable to breakdown). Fourth, the statement may be modified to include communications problems that are related to a person such as individual communication skills, previous experience with computers, inadequate communication skills of the participants or their respect for the communications plan. Fifth, the statement should be modified to include problems with respect to the delivery of irrelevant information. Sixth, the statement may be changed to include communications problems resulting from competition, such as fighting over the scene primacy.

We concluded that this statement has been validated with the data analysed, albeit with several additions. All of the participants in our study confirmed that environmental noise was a major problem in communication. Other problems, such as background talk or speech that is not intended for the listener, were also confirmed. Some of these problems resulted from an incorrect communication setup. However, no music or intentional disturbances of the channel have been reported. Finally, as

Table 10. Design guidelines for problems in communication

Metaphor Extension	Solution to a Problem
Alternative to the primary metaphor	Reach a person who does not reply or is not reachable. Training to avoid bad habits (e.g. talk face-to-face instead of keeping all informed by radio, use of mobile phone when not recommended)
Noise	Realistic training conditions represented by environment and technology-induced noises. The noise should depend on a trainee's action (e.g. distance from the noise-emitting object).

elicited above, several additional communication problems have been observed or reported during interviews. The design guidelines derived from statement ten are described in Table 10.

Summary of Results

The summary of results is provided in Table 11. It organises the statements by group. For each statement, there is a brief summary and a conclusion on its support or refusal in crisis management. If applicable, each statement has additions that were deemed necessary while transferring the statement from online games to crisis management training in a virtual environment. Two out of the ten statements were refuted in crisis management, five were confirmed and three were partly confirmed. In six of the eight sentences that were confirmed or partly confirmed, additions had to be made for crisis management.

CONCLUSION

Outcome of the Research Study

At the onset of this research study, we aimed to answer the question of whether and to what extent crisis management training in a virtual environment could take advantage of voice communication in online multiplayer games. Given the results summarised in the previous section we conclude that virtual environments for crisis management training can take advantage of communication in online multiplayer games. From a practical standpoint, we have suggested design guidelines to be used in the design of a virtual environment for crisis management training. Theoretical implications will be discussed later in this section.

While a majority of the statements, which were derived from on-line games, could be confirmed and thus adopted in crisis management training, others had no match in the crisis management domain. These results accorded with our expectations

Table 11. Summary of statements, their validation and extensions for crisis management

Statement Group	Statement No.	Statement of Online Games	Confirmed in Crisis Management	Additions for Crisis Management
Media richness selection	1	Selection of media based on tasks, fellows, organisation and prior experience	Yes	Medium availability and type of training instrument used
	2	Leaner media (e.g. text) can cause impulsive or reserved behaviour but can be used for initial contact or for asynchronous communication	Partially, but not for impulsive or reserved behaviour	Media with higher richness should be used under stressful conditions, and to achieve higher reliability lower medium should be used as a backup channel.
	3	Four metaphors for voice channels: broadcasting, landline, mobile phone and proximity chat	Yes	Multiple, simultaneous channels and reconfigurable channels or media depending on context.
Groups of people	4	Radio channel is most useful for a small group of players who know each other but multi-channels can cause fragmentation	Partially, but fragmentation is prevented	Possibilities to step out of the conversation and to monitor multiple channels simultaneously.
	5	Proximity chat is useful where a large number of players would clutter a shared radio channel and players are close to each other in the virtual environment.	Partially, but cluttering is not identified	Face-to-face is used for regular meetings and when there are environmental or technology constraints.
Identity of people	6	Players had difficulty identifying who was speaking. Difficult to control what was heard and what was sent.	No	
	7	A player's identity can negatively affect learning and coordination	No	
Avatar behaviour	8	Where visual representation is available, verbal actions should be coupled with postural, gestural and proximity information of the player embodiment.	Yes	
Learning	9	Experience sharing	Yes	
Problems	10	Problems of voice communication, e.g. background talk, natural or synthetic noise, intentional or unintentional	Yes	Unnecessary information delivery, problems resulting from competition such as fighting over the scene primacy and skill dependence.

at the onset of the validation part of the study. However, what we could not have predicted was which statements from the broader online games are transferrable to crisis management training. For example, statement one, which links media richness selection with communication characteristics, has been fully confirmed, while statement six, which discusses the identity problems of players, has been refuted. Especially noticeable is the need for addressing environmental and situated noise in crisis management. According to participants in the study, this is a paramount feature of a virtual environment because it can have a great impact on work performance.

The characteristics of crisis management are especially influential and apparent in the results. What is most obvious is that such an operation follows organisational guides (e.g. statement one, selection of the medium according to the guidelines), is formal (e.g. statement two, no impulsive or reserved behaviour, and statement six, identifying who is speaking), is characterised by a complexity in the topology of the communication (e.g. statement three, using two or more channels simultaneously), produces reliable data and the decision making is highly critical (e.g. statement four on the logging of information or pausing to enable decision making). The operation shows impact of a noisy environment on task performance (statements five and ten), has identification of speaker or recipient by call signs or by channel selection (statement six) and allows members to share each other's experiences by communication or coordination (statement nine). While these characteristics are not entirely unique for crisis management, we expect that they are not generic for all domains.

Other statements, which have been confirmed in crisis management training, are likely to be usable in other similar domains, e.g. training in the military domain or individual response agencies. A few examples are the selection of media based on fellows, tasks and organisation; the asynchrony of information; metaphors, gestures and postures increasing the meaning of the communication, and the proximity of the conversation being dependent on the size of the group.

The design guidelines that were identified for each statement can be useful for crisis management training environments and, depending on their generality, for other virtual environments. Some of the design guidelines are especially useful for training because they can be variable from one training level to the next. For example, a trainee can train first without environmental noise and then, as difficulty levels increase, with it. Thus, he or she would receive, gradually, an increasingly more difficult training environment. This scenario is in accordance with the Variable Uncertainty Framework which has been proposed for designing scenarios for training environments and includes three variable dimensions, the number of events, the randomness of events, and the situational complexity around events (Field, Rankin, Pal, Eriksson, & Wong, 2011).

Despite the positive results of this research study, it leaves open several avenues for further study. First, a more in-depth research analysis of a communication protocol could provide further information on impulsive or reserved behaviour (second statement) or a delay of the message delivered (statement six). Second, future research should include an evaluation of the design guidelines. The evaluation of their validity for a virtual environment for learning is necessary in any prototype of a training system. Previous review of validation of simulators has illustrated that the area has few accepted definitions and measurement methods, making it a challenging area (Schout, Hendrikx, Scheele, Bemelmans, & Scherpbier, 2010). Schout et al. (2010) have proposed that a prerequisite for validating a simulator researchers should conduct a training needs analysis to evaluate the existing requirements for training and to look at program requirements in a training program design. Third, it could be worthwhile to evaluate, in practice, how the variable factors characterised in the statements can be used for designing training scenarios. Fourth, the findings on communication were collected from the related domains of online multiplayer games and collaborative virtual environments. These findings provide information about textual and voice communication. This work should be extended to include other forms of communication in the virtual environment (e.g. videoconferencing) and their applicability for crisis management training.

Relation to Theories

This section describes several theories that can be related to the results and that can afford grounds for further research. The results describe voice communication in the crisis management domain as a safety-critical process that must provide reliable information delivery to an appropriate destination. Problems of communications have been identified and they can have implications for collective decision-making and coordination of action. Categorically, the problems were, first, technological, such as communications failure and simultaneous use of multiple devices; second, sociological, including the lack of a common vocabulary, the habitual use of channels, the overwhelming nature of the tasks and the stressful environment; and third, organisational, because of different hierarchical structures in communication. In addition to these three categories identified by Manoj and Baker (2007) and confirmed by this study, the results suggest that the physical environment or the context is a prominent characteristic that has an effect on communication.

Another theory or a model to which this research can relate is Berlo's (1960) communication model, which describes the nature of the receiver, the sender, the message and the channel. The communication between the source and receiver is mediated by messages sent over a channel. A source is a person with the intention of transmitting a message that represents his/her thoughts. It is influenced by communication skills (e.g. ability to speak, write), attitude towards the audience, subject of communication and oneself, knowledge of the subject and the social system and culture (e.g. beliefs, religion). The message component represents the information as expressed by the source, which consists of the content, elements, treatment, structure and code. The content is the entire information of a message assembled from elements such as words or gestures, into a structure (e.g. a sentence). The selected treatment can include formal or natural communication. Code refers to the language that is used or other rules and conventions governing verbal and gestural communication. The channel is the medium by which the message is encoded and decoded, as represented by five senses. A receiver is a person at the destination of the communication chain trying to understand the message using their own communication skills, knowledge and social system. Statements one, two, four, six and seven relate to the social systems of the source or the receiver. Statement eight relates to the message, specifically the channel (e.g. visual or verbal) and code (e.g. gestures). Finally, statement nine relates to knowledge of the subject.

Whereas communication can be viewed as the medium of content, it is not concerned with the behaviour of the trainee. It is worth considering how the communication relates to a theory of engagement, which describes how well a player (a trainee) is pulled into the game. Engagement has been characterised by Benyon (2010, p. 95) as including identity as a sense of authenticity for the expression of self, adaption relating to change and personalisation along with changing levels of difficulty, and the narrative concerns of telling a good story, immersion in the sense of feeling wholly involved, and flow, defined as the gradual flow of one state to the next. Based on 12 in-depth interviews and on existing theories in gaming, Whitton (2011) has constructed a model of engagement in which learning consists of five factors, i.e. challenge, control, immersion, interest in the activity, and purpose. Applying Whitton's theory (2011) to our results we take a few examples. Noise will increase immersion, and a selection of communication devices, i.e. face-to-face. Radio or mobile phones provide different avenues of communication and thus control. On the other hand, noise can provide a challenge for the trainee and can introduce uncertainty in completing a task, which can also be increased by a complex topology of communication, such as multiple simultaneous channels. The last two factors, interest in the activity and purpose, could not be found in the ten statements.

This paper contributes to the transferability of knowledge between domains. It adds to previous work, which has proposed ways of designing user interfaces by adaptation from other domains, such as games (Shepherd & Bleasdale-Shepherd, 2011). Thus, it contributes to answering the question to what extent technology can be transferred between application domains (Harris & Harris, 2004).

REFERENCES

Adelman, L., Christian, M., Gualtieri, J., & Bresnick, T. A. (1998). Examining the effects of communication training and team composition on the decision making of Patriot air defense teams. *IEEE Transactions on Systems, Man, and Cybernetics. Part A, Systems and Humans*, *28*(6), 729–741. doi:10.1109/3468.725346

Bartle, R. A. (2003). Not Yet you Fools! games+girls=advance. Retrieved from http://www.gamegirladvance.com/archives/2003/07/28/not_yet_you_fools.html#000424

Bayerl, P. S., & Lauche, K. (2010). Technology Effects in Distributed Team Coordination High-Interdependency Tasks in Offshore Oil Production. *Computer Supported Cooperative Work*, *19*(2), 139–173. doi:10.100710606-010-9107-x

Benyon, D. (2010). *Designing interactive systems: a comprehensive guide to HCI and interaction design*. Pearson Education.

Berlo, D. K. (Ed.). (1960). *The process of communication*. New York, New York: Holt, Rinehart, & Winston.

Bharosa, N., Lee, J., & Janssen, M. (2010). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises. *Information Systems Frontiers*, *12*(1), 49–65. doi:10.100710796-009-9174-z

Boyle, E. A., Hainey, T., Connolly, T. M., Gray, G., Earp, J., Ott, M., ... Pereira, J. (2016). An update to the systematic literature review of empirical evidence of the impacts and outcomes of computer games and serious games. *Computers & Education*, *94*, 178–192. doi:10.1016/j.compedu.2015.11.003

Brehmer, B., & Dörner, D. (1993). Experiments with computer-simulated microworlds: Escaping both the narrow straits of the laboratory and the deep blue sea of the field study. *Computers in Human Behavior*, *9*(2–3), 171–184. doi:10.1016/0747-5632(93)90005-D

Carter, M., Wadley, G., & Gibbs, M. (2012). Friendly, don't shoot!: how communication design can enable novel social interactions. *Paper presented at the 24th Australian Computer-Human Interaction Conference*. 10.1145/2414536.2414548

Cassell, J., & Thorisson, K. R. (1999). The power of a nod and a glance: Envelope vs. emotional feedback in animated conversational agents. *Applied Artificial Intelligence: An International Journal*, *13*(4), 519–538. doi:10.1080/088395199117360

Cheung, V., Chang, Y.-L. B., & Scott, S. D. (2012). Communication channels and awareness cues in collocated collaborative time-critical gaming. *Paper presented at the ACM 2012 conference on Computer Supported Cooperative Work*, Seattle, Washington, USA. 10.1145/2145204.2145291

Chodos, D., Stroulia, E., Boechler, P., King, S., Kuras, P., Carbonaro, M., & Jong, E. d. (2010). Healthcare education with virtual-world simulations. *Paper presented at the 2010 ICSE Workshop on Software Engineering in Health Care*, Cape Town, South Africa. 10.1145/1809085.1809097

Clark, H., & Brennan, S. A. (1991). Grounding in communication. In L. B. Resnick, J. M. Levine, & S. D. Teasley (Eds.), *Perspectives on socially shared cognition*. doi:10.1037/10096-006

Cooke, N. J., Gorman, J. C., Myers, C. W., & Duran, J. L. (2013). Interactive Team Cognition. *Cognitive Science*, *37*(2), 255–285. doi:10.1111/cogs.12009 PMID:23167661

Creutzfeldt, J., Hedman, L., Medin, C., Heinrichs, W. L., & Felländer-Tsai, L. (2010). Exploring virtual worlds for scenario-based repeated team training of cardiopulmonary resuscitation in medical students. *Journal of Medical Internet Research*, *12*(3), e38. doi:10.2196/jmir.1426 PMID:20813717

Crookall, D. (2010). Serious Games, Debriefing, and Simulation/Gaming as a Discipline. *Simulation & Gaming*, *41*(6), 898–920. doi:10.1177/1046878110390784

Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness and structural design. *Journal Management Science, 32*(5).

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining "gamification". *Paper presented at the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, Tampere, Finland. 10.1145/2181037.2181040

Endsley, M. R., & Jones, W. (2013). Situation awareness. The Oxford Handbook of Cognitive Engineering, 88.

Field, J., Rankin, A., Pal, J. d., Eriksson, H., & Wong, W. (2011). Variable Uncertainty: Scenario Design for Training Adaptive and Flexible Skills. *Paper presented at the European Conference on Cognitive Ergonomics*. 10.1145/2074712.2074719

Gibbs, M., Hew, K., & Wadley, G. (2004). Social Translucence of the Xbox Live Voice Channel. In M. Rauterberg (Ed.), Entertainment Computing – ICEC 2004, LNCS (Vol. 3166, pp. 407-499): Springer Berlin / Heidelberg. doi:10.1007/978-3-540-28643-1_48

Gibbs, M., Wadley, G., & Benda, P. (2006). Proximity-based chat in a first person shooter: using a novel voice communication system for online play. *Paper presented at the 3rd Australasian conference on Interactive entertainment*, Perth, Australia.

Grantcharov, T. P., Kristiansen, V. B., Bendix, J., Bardram, L., Rosenberg, J., & Funch-Jensen, P. (2004). Randomized clinical trial of virtual reality simulation for laparoscopic skills training. *British Journal of Surgery*, *91*(2), 146–150. doi:10.1002/bjs.4407 PMID:14760660

Greef, T. d., & Arciszewski, H. (2007). A closed-loop adaptive system for command and control. *Paper presented at the 3rd international conference on Foundations of augmented cognition*, Beijing, China. 10.1007/978-3-540-73216-7_31

Gustafson, J., Boye, J., Fredriksson, M., Johanneson, L., & Königsmann, J. (2005). Providing computer game characters with conversational abilities. In Intelligent Virtual Agents IVA 2005, LNCS (Vol. 3661, pp. 37–51). Springer-Verlag. doi:10.1007/11550617_4

Haferkamp, N., Kraemer, N. C., Linehan, C., & Schembri, M. (2011). Training disaster communication by means of serious games in virtual environments. *Entertainment Computing*, *2*(2), 81–88. doi:10.1016/j.entcom.2010.12.009

Halloran, J. (2009). It's Talk, But Not as We Know It: Using VoIP to Communicate in War Games. *Paper presented at the 2009 Conference in Games and Virtual Worlds for Serious Applications*. 10.1109/VS-GAMES.2009.36

Halloran, J., Fitzpatrick, G., Rogers, Y., & Marshall, P. (2004). Does it matter if you don't know who's talking?: multiplayer gaming with voiceover IP. *Paper presented at the CHI '04 extended abstracts on Human factors in computing systems*, Vienna, Austria. 10.1145/985921.986027

Halloran, J., Rogers, Y., & Fitzpatrick, G. (2003). From text to talk: Multiplayer games and voiceover IP. *Paper presented at the 2003 Digital Games Research Association Conference*, Utrecht.

Harris, D., & Harris, F. J. (2004). Evaluating the transfer of technology between application domains: A critical evaluation of the human component in the system. *Technology in Society*, *26*(4), 551–565. doi:10.1016/S0160-791X(04)00055-7

Heinrichs, W. L., Youngblood, P., Harter, P. M., & Dev, P. (2008). Simulation for team training and assessment: Case studies of online training with virtual worlds. *World Journal of Surgery*, *32*(2), 161–170. doi:10.100700268-007-9354-2 PMID:18188640

Jain, S., & McLean, C. R. (2005). Integrated simulation and gaming architecture for incident management training. *Paper presented at the 37th conference on Winter simulation*, Orlando, Florida. 10.1109/WSC.2005.1574338

Johnston, H., & Whitehead, A. (2009). Distinguishing games, serious games, and training simulators on the basis of intent. P*aper presented at the Proceedings of the 2009 Conference on Future Play on @ GDC Canada*, Vancouver, British Columbia, Canada. 10.1145/1639601.1639607

Jones, D. G., & Endsley, M. R. (1996, June). Sources of situation awareness errors in aviation. *Aviation, Space, and Environmental Medicine*, *67*(6), 507–512. PMID:8827130

Klein, G. (1993). A recognition-primed decision (RPD) model of rapid decision making. In G. Klein, J. Orasanu, R. Calderwood, & C. Zsambok (Eds.), *Decision making in action: Models and methods*. Westport, CT, US: Ablex Publishing.

Li, S.-C. S. (2007). Computer-mediated communication and group decision making. *Small Group Research*, *38*(5), 593–614. doi:10.1177/1046496407304335

Manoj, B. S., & Baker, A. H. (2007). Communication challenges in emergency response. *Communications of the ACM*, *50*(3), 51–53. doi:10.1145/1226736.1226765

Potkonjak, V., Gardner, M., Callaghan, V., Mattila, P., Guetl, C., Petrović, V. M., & Jovanović, K. (2016). Virtual laboratories for education in science, technology, and engineering: A review. *Computers & Education*, *95*, 309–327. doi:10.1016/j.compedu.2016.02.002

Ratan, R. A., Chung, J. E., Shen, C., Williams, D., & Poole, M. S. (2010). Schmoozing and Smiting: Trust, Social Institutions, and Communication Patterns in an MMOG. *Journal of Computer-Mediated Communication*, *16*(1), 93–114. doi:10.1111/j.1083-6101.2010.01534.x

Raybourn, E. M. (2007). Applying simulation experience design methods to creating serious game-based adaptive training systems. *Interacting with Computers*, *19*(2), 206–214. doi:10.1016/j.intcom.2006.08.001

Salas, E., Cooke, N. J., & Rosen, M. A. (2008). On Teams, Teamwork, and Team Performance: Discoveries and Developments. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *50*(3), 540–547. doi:10.1518/001872008X288457 PMID:18689065

Salas, E., DiazGranados, D., Klein, C., Burke, C. S., Stagl, K. C., Goodwin, G. F., & Halpin, S. M. (2008). Does Team Training Improve Team Performance? A Meta-Analysis. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *50*(6), 903–933. doi:10.1518/001872008X375009 PMID:19292013

Sallnäs, E.-L. (2002). *Collaboration in multi-modal virtual worlds: Comparing touch, text, voice and video. In The social life of avatars* (pp. 172–187). New York: Springer.

Schout, B. M. A., Hendrikx, A. J. M., Scheele, F., Bemelmans, B. L. H., & Scherpbier, A. J. J. A. (2010). Validation and implementation of surgical simulators: A critical review of present, past, and future. *Surgical Endoscopy*, *24*(3), 536–546. doi:10.100700464-009-0634-9 PMID:19633886

Shepherd, I., & Bleasdale-Shepherd, I. (2011). The design-by-adaptation approach to universal access: Learning from videogame technology. *Universal Access in the Information Society*, *10*(3), 319–336. doi:10.100710209-010-0204-x

Tan, W.-K., Tan, C.-H., & Teo, H.-H. (2012). Conveying information effectively in a virtual world: Insights from synthesized task closure and media richness. *Journal of the American Society for Information Science and Technology*, *63*(6), 1198–1212. doi:10.1002/asi.22600

Toups, Z. O., Kerne, A., & Hamilton, W. A. (2011). The Team Coordination Game: Zero-fidelity simulation abstracted from fire emergency response practice. *ACM Transactions on Computer-Human Interaction*, *18*(4), 23. doi:10.1145/2063231.2063237

Wadley, G. (2011). *Voice in virtual worlds. (Ph.D.)*. The University of Melbourne.

Wadley, G., Carter, M., & Gibbs, M. (2015). Voice in Virtual Worlds: The Design, Use, and Influence of Voice Chat in Online Play. *Human-Computer Interaction*, *30*(3-4), 336–365. doi:10.1080/07370024.2014.987346

Wadley, G., Gibbs, M., & Benda, P. (2005). Towards a framework for designing speech-based player interaction in multiplayer online games. *Paper presented at the Proceedings of the second Australasian conference on Interactive entertainment*, Sydney, Australia.

Wadley, G., Gibbs, M., & Benda, P. (2007). Speaking in character: Using voice-over-IP to communicate within MMORPGs. *Paper presented at the Proceedings of the 4th Australasian conference on Interactive entertainment*, Melbourne, Australia.

Wadley, G., Gibbs, M., & Ducheneaut, N. (2009). You can be too rich: Mediated communication in a virtual world. *Paper presented at the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7*, Melbourne, Australia.

Whitton, N. (2011). Game Engagement Theory and Adult Learning. *Simulation & Gaming*, *42*(4).

Wiecha, J., Heyden, R., Sternthal, E., & Merialdi, M. (2010). Learning in a virtual world: Experience with using second life for medical education. *Journal of Medical Internet Research*, *12*(1), e1. doi:10.2196/jmir.1337 PMID:20097652

Yamamori, T., Kato, K., Kawagoe, T., & Matsui, A. (2008). Voice matters in a dictator game. *Experimental Economics*, *11*(4), 336–343. doi:10.100710683-007-9168-y

Zarraonandia, T., Vargas, M., Díaz, P., & Aedo, I. (2009). A virtual environment for learning airport emergency management protocols. In J. Jacko (Ed.), *Human-Computer Interaction. Ambient, Ubiquitous and Intelligent Interaction* (Vol. 5612, pp. 228–235). Springer Berlin Heidelberg. doi:10.1007/978-3-642-02580-8_25

Zyda, M. (2005). From Visual Simulation to Virtual Reality to Games. *Computer*, *38*(9), 25–32. doi:10.1109/MC.2005.297

This research was previously published in the International Journal of Sociotechnology and Knowledge Development (IJSKD), 9(1); edited by Lincoln Christopher Wood and Brian J. Galli; pages 1-25, copyright year 2017 by IGI Publishing (an imprint of IGI Global).

Chapter 19
Analysis of a Training Package for Law Enforcement to Conduct Open Source Research

Joseph Williams
Canterbury Christ Church University, UK

Georgina Humphries
Canterbury Christ Church University, UK

ABSTRACT

Law enforcement officials (LEOs) in the UK conduct open source research (OSR) as part of their routine online investigations. OSR, in this instance, refers to publicly available information that is accessed via the Internet. As part of the research, identifying and tracing the electronic suspect (RITES) course provided by the UK's College of Policing, LEOs are introduced to the open source internet research tool (OSIRT); a free software tool designed to assist LEOs with OSR investigations. This article draws on analyses from questionnaires and observations from a RITES course; mapping them to Kirkpatrick's evaluation model. Results showed the positive impact the RITES course had in transferring knowledge back on-the-job, with LEOs applying knowledge learned to real-life investigative scenarios. Additionally, results showed OSIRT integrated both in the RITES course and into the LEOs investigative routine.

DOI: 10.4018/978-1-7998-2535-7.ch019

INTRODUCTION

The World Wide Web plays host to a veritable breadcrumb trail of potential evidence which could provide intelligence to Law Enforcement Officials (LEOs). From Facebook posts to Tweets, all are avenues that may prove useful and warrant exploration. One tool to help navigate these routes is Open Source Research (OSR). OSR is concisely defined by the Association of Chief Police Officers (ACPO) as "The collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise, to use as intelligence or evidence within investigations" (ACPO, 2013, p.8).

To aid digital investigators in conducting OSR, the UK's College of Policing, a professional training body for police in England and Wales, runs a five-day Researching, Identifying and Tracing the Electronic Suspect (RITES) course. The RITES course provides an opportunity for LEOs, regardless of skill-level, to gain proficiency in lawfully obtaining intelligence and artefacts from the web. In addition to investigatory skills, the RITES course adopts the usage of the free and open source investigative software package Open Source Internet Research Tool (OSIRT); a tool designed specifically to assist in conducting OSR.

A growing trend for the use of OSR is continuously expanding among UK law enforcement agencies. In order to conduct rigorous OSR investigations, law enforcement require a multitude of tools and techniques. A problem surrounding OSR is the cost associated with software tools, along with the legal, ethical, and procedural issues that are exacerbated by the reduction in police funding. It is imperative, then, that the training LEOs receive is robust and applicable in the digital age. The objective of this study is to offer an insight into how LEOs are trained to conduct OSR and whether the training package, in conjunction with OSIRT, is effective for those officers both during the course and when they are back on the job.

BACKGROUND

Designing Training Courses for Law Enforcement and Applying Learning Styles

Similarly to courses structured for training law enforcement in digital forensic investigations (Genoe, Toolan, & McGourty, 2014; Stephens, 2012), the RITES course requires an ability to problem solve, pay attention to detail, and have a mindset for investigation and intelligence. Considerations are directed by course aims "to provide investigating officers with the skills necessary to obtain, evaluate and use online information … apply[ing] best practice in respect of proper authorization and recording processes for online investigations" (College of Policing, 2017, para. 3).

For a number of years, police training programs adopted a "militaristic environment" (Birzer, 2003, p.30) which a number of authors (Birzer, 2003; Haberfeld, Clarke, & Sheehan, 2011; Vodde, 2009) state is not conducive to learning, as "it is essential that training is conducted in such a way as to be as meaningful as possible to the adult participants" (Birzer & Roberson, 2007, p. 226). The RITES course adopts both andragogic (i.e. self-directed learning and sharing of experiences) and pedagogic (i.e. dictating learning in the form of traditional lectures) approaches to learning which seemingly prove efficacious when training police officers (Birzer, 2003; Haberfeld et al., 2011; Queen, 2016). Tong, Bryant, & Horvath (2009, p.210) state that "training and learning styles need to reflect that uncertainty of police work and the principles that should inform practice." Traditionally, lecture style approaches to educating learners are "almost always the most inefficient way of learning" (Grace, 2001, p.125), and while it is unlikely for the RITES course to accommodate every style of learning, a concerted effort is made to engage their audience. By embracing modern approaches, College of Policing trainers afford the officers a better chance of applying their acquired skills to real-life scenarios.

Design of the RITES Course

The course is split into one to two-hour chunks of key topic areas, covering approximately five topic areas a day (Figure 1). Each topic area is then either proceeded or injected with practical sessions or discussion from the cohort, which is facilitated by the instructors. Practical sessions also include building upon a fabricated case using OSIRT over the five days. On the final day, the group members are examined by means of an unseen open source investigation. The artefacts they obtain through OSIRT from the 'investigation' are then applied to answer questions on a computer-aided, open book, multiple-choice examination. The course is then concluded with a reflection of the previous five days. Figure 2 represents the layout of the learning environment.

Using Software for Investigative Work

In an ever-growing digital age, and with changing expectations in police competencies, LEOs require essential skills and abilities to conduct online investigations. However, the skill-level of officers requiring such training is diverse with many not being, or having had the need to be, skillful with computers during their daily roles. The requisite for software-based solutions has a crucial element to aid the proficiency of conducting OSR and go some ways towards making "officer[s] more efficient,

Figure 1. RITES course structure

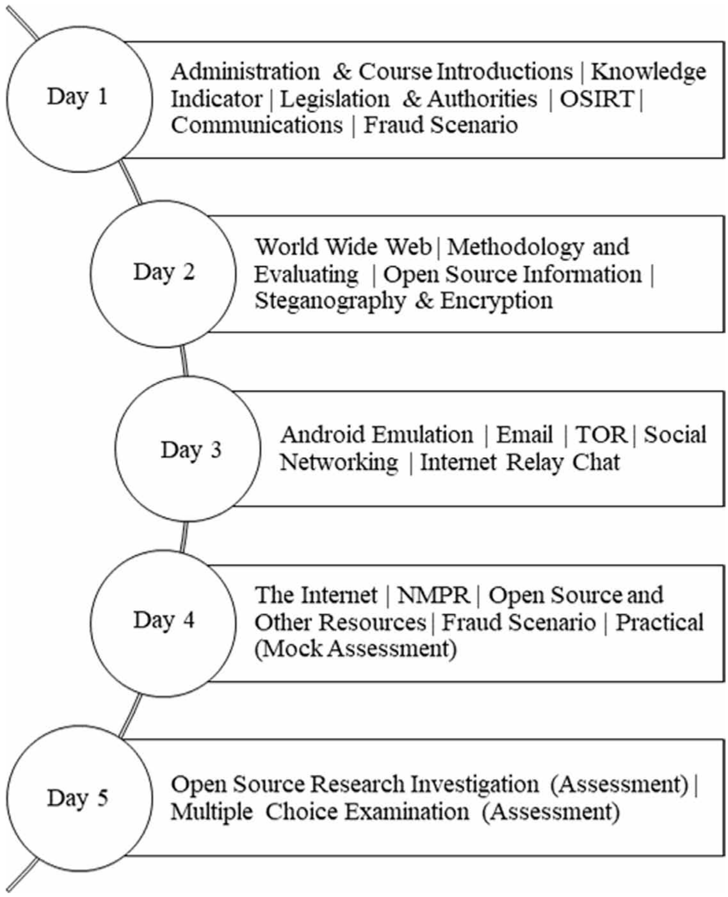
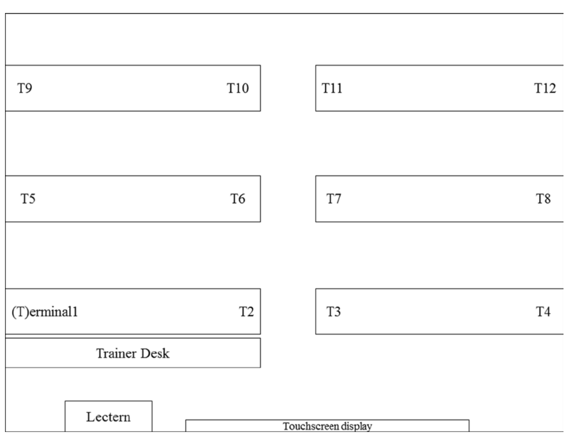


Figure 2. RITES course room layout



more effective, more knowledgeable, and better able to spend [their] time … and by improving reporting capabilities" Roberts (2011, as cited in Hess et al., 2013, p.16).

Using Kirkpatrick's Training Evaluation Model

A number of courses within the policing context (Capacity Building and Training Directorate, 2012; Genoe et al., 2014; Stephens, 2012) have utilized Kirkpatrick's evaluation model. Developed in the 1950s (Kirkpatrick & Kirkpatrick, 2006; Kirkpatrick & Kirkpatrick, 2016), it is now the "most widely used framework" due to its design and levelled implementation (Tamkin, Yarnall, & Kerrin, 2002, p. 3). Furthermore, Kirkpatrick's model encourages learner participation via four levels: Reaction, Learning, Behavior, and Results. The model is popular as it places value on learners' views, suggestions and opinions. The four levels look at several key areas to evaluate effectiveness such as;

- **Reaction – Level 1:** participants thoughts on the course, its relevance and their own engagement
- **Learning – Level 2:** knowledge, skills and abilities (e.g. performance), attitudes and confidence
- **Behavior – Level 3:** changes in job behavior due to training and the applicability of learned skills/content
- **Results – Level 4:** impact of the training and content on the business

METHOD

A mixed method approach was adopted, using questionnaires, evaluations, and observations. These methods were chosen due to their ease of mapping with Kirkpatrick's evaluation model. Evaluations in this study included key questions to examine the courses effectiveness based on the Hybrid Kirkpatrick's Evaluation tool (Kirkpatrick Partners, LLC, 2010), which provides example questions for levels one to four. For example, knowledge retention and applicability to real world environments were sought through free-form answers and Likert scale statements. Limitations of Kirkpatrick's model are abated by looking at the value of information across each level; avoiding the linear approach criticized by Tamkin et al. (2002). Using this approach ensures the most valued information of course effectiveness is collated. This study evaluates levels three and four from the perspective of attending officers; taking into consideration their experience, rank and own ability to assess their behavioral change, including the impact of the course on the working environment. Participants were made up of an opportunity sample of twelve serving

LEOs attending a RITES course, containing six males and six females. Participant jobs ranged from Detective Constables and Sergeants, to Analysts. The average service time was sixteen years; with a minimum of 8 and a maximum of 26 years.

A pre-course questionnaire was completed electronically to gain insight into the participant's expectations of the RITES course and to establish current skill-levels at conducting OSR. Additionally, the questionnaire asked participants of any software they currently use to conduct OSR, if any. At the end of each training day, the cohort completed a paper-based questionnaire asking to evaluate each day's topic areas ("Easy" to "I'm lost"), the pace of the session ("Too slow" to "Too fast") and whether OSIRT was effective in that day's session ("Strongly disagree" to "Strongly agree"). The participants were also afforded an opportunity to freely express their thoughts for the day.

An electronic immediate post-course questionnaire was distributed on the final day; covering a range of areas such as course content coverage, course assessment, and the applicability of OSIRT. All statements conformed to a ranked multiple-item Likert scale, and took a flipped phrased approach to reduce response bias (Field, 2006). Finally, eight weeks after course completion, an on-the-job questionnaire was distributed electronically to identify if the RITES course had an impact on their role.

Both immediate and delayed post-course evaluations contain multiple-item measures across the four levels of Kirkpatrick's model. In the case of this study, factor analysis was infeasible due to population size, however, Gliem & Gliem (2003) note the importance of calculating Cronbach's alpha for scale items. Cronbach's alpha is a popular statistical analysis to measure reliability among variables of interest (Tavakol & Dennick, 2011). Cronbach's alpha is adopted in this study to measure statements relating to the different levels of the Kirkpatrick's model. Analysis of Cronbach's alpha was conducted using IBM SPSS 24.0.

Furthermore, for flipped phrased items and to prevent a negative impact on the reliability score, the negative statements were reversed before calculation. Common levels of internal reliability/consistency of alpha (α) were employed with acceptable values of 0.7, through to excellent values of $\alpha >= 0.9$ (George & Mallery, 2016; Loewenthal & Lewis, 2015; van Griethuijsen et al., 2015).

Observations were adopted providing instructors with the chance to look at each participant's level of engagement, demonstration of skills, through to how the course, and OSIRT would be useful on-the-job. Mindful of the role the observer plays on the learner, considerations were made towards how the learner's behavior can be affected, by the presence of an observer within the training environment. Hallenberg, O'Neil, & Tong (2016, p.109) write that "Van Maanen describes four typologies" of a researcher. In this study the author, as an observer, can be classified as a 'fan', i.e., a researcher who is "interested in observing police practice as it happens" (Hallenberg et al., 2016, p.109). The observer kept a daily diary of events, with reflections made to correlate with learner comments and ratings from course evaluations.

RESULTS AND DISCUSSION

Pre-Questionnaire Results

Challenges faced by participants when conducting OSR generally fell into one of three categories: the need to be trained in OSR, an absence of IT knowledge, or software tool 'overload'. Current software tool usage is consistent with feedback previously received in that officers use a varied array of software that is either free or built into the computer's operating system. Three respondents said they did not use any software, with one noting they do not have access to the necessary technology. No participants have previously used OSIRT as part of their investigations.

All participants said they prefer practical learning where a "realistic" and "hands-on" approach can be applied to real-life investigative scenarios. Responses show that expectations of learning were centered around having the necessary tools available to "research and capture" and "how to best use these practically" to "maximise [the] chances of finding what [they] want to find". Additionally, participants wanted to know "the 'correct and best' way of completing research" using "OSR techniques" that was both "safe [as well as showing] potential pitfalls when conducting OS research".

Finally, "certification", "knowledge", and "confidence" were stressed as attributes officers were wanting to achieve throughout the course. Other responses showed concern with monitoring their own digital footprint while conducting an open source investigation. Replies also showed that participants were using the course to pass knowledge and understanding back to colleagues in the working environment.

Daily Evaluations and Observer Comments

Course Pace and Difficulty

Daily averages and the immediate post-course evaluation show the overall difficulty noted by most participants to be 'Just Right'. Figure 3 demonstrates, overall, two learners felt the course was 'Very Difficult', speculatively this may have been linked with their perceived computer literacy (Figure 4) and three felt the course to be 'A Little Tough'. These results are not unexpected, as observations showed a small number of the cohort readily admitting they were computer novices, one going as

Figure 3. Overall difficulty of the course

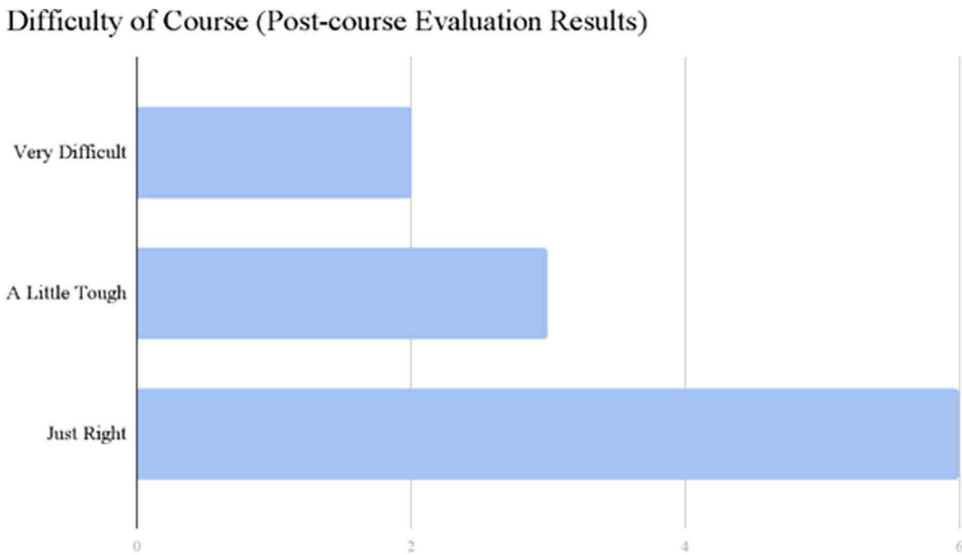


Figure 4. Cohorts' rating of own computer literacy

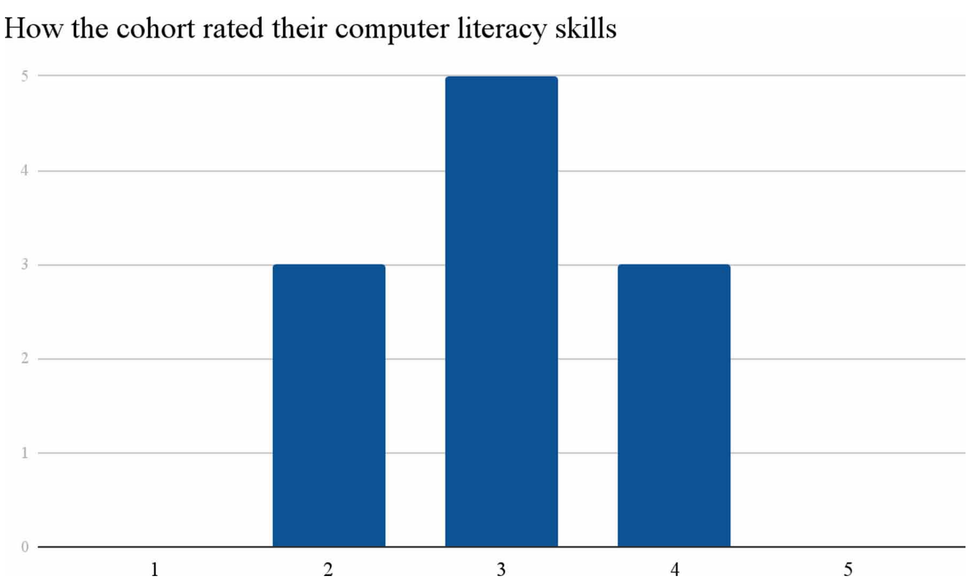
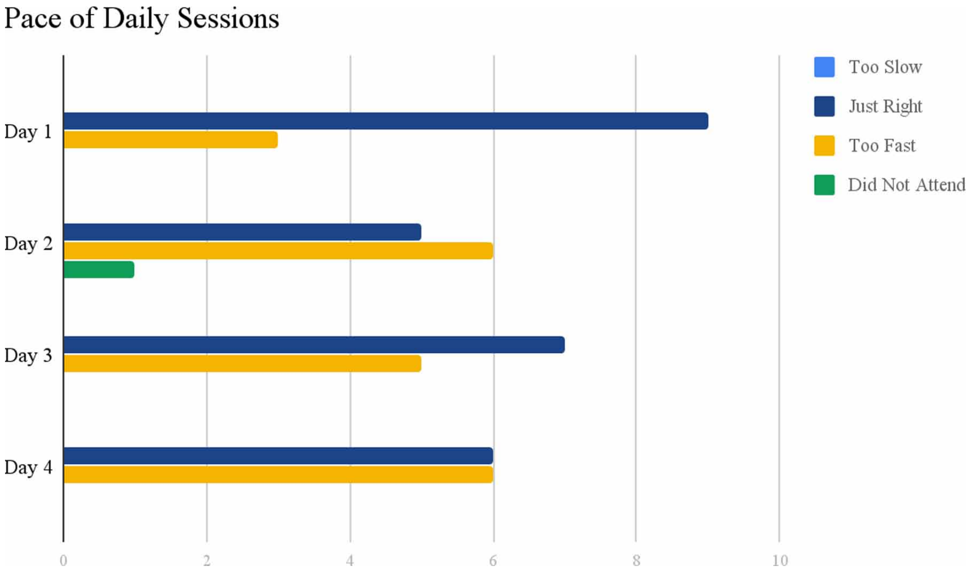


Figure 5. Perception of daily session pace



far to say they were a 'technophobe'. Other comments lend themselves towards aspects of learning, where one respondent felt the course to be tough as their basic knowledge was poor, however, they emphasized that the trainers were helpful in assisting as much as possible, and being patient with them. The respondent felt these points helped make the course thoroughly enjoyable and "took a lot" from it.

The cohort throughout the week were engaged and responsive to interactive sessions. Additionally, observations showed that the trainers addressed issues with pacing, providing one-to-one guidance when needed. While the cohort were frequently split about pacing of the daily sessions, as seen in Figure 5, pace was observed to be problematic on days where complex topics, such as encryption, were taught. Participants offered feedback in their daily evaluations for these challenging topics, one noting they "saw some people confused about terminology" and suggested that "perhaps … more basic explanation[s]" could be provided. Given the technical complexity of some of the topics, it is understandable the cohort would find these difficult to immediately absorb. As with any learning, the time taken to master and acquire knowledge differs per learner, and added with technical complexity of a topic, a "too fast" response would not be atypical given these circumstances.

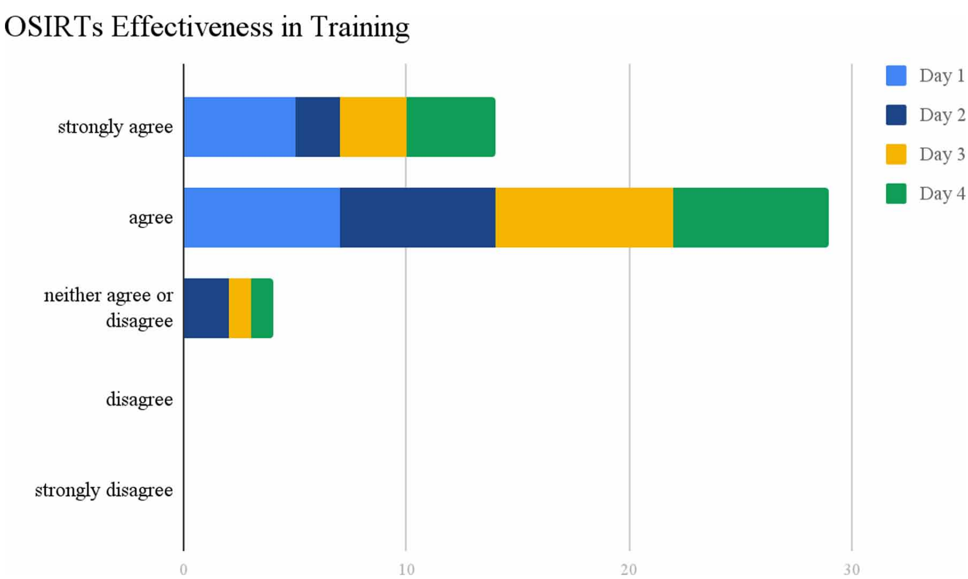
Observations showed that there was good communication during these particularly tough sessions, with the use of analogies by the trainers making complex topics relatable to everyday life. One participant highlighted this in their comments, saying "comparing 'digital' to 'real-life events' assists in understanding". Feedback also showed that although some sessions were "hard work", they were still "very interesting" and "enjoyable".

OSIRT

To capture the usage and effectiveness of OSIRT, officers were asked to rate the tool using a Likert scale, from strongly disagree to strongly agree, and provide comments based on the statement "OSIRT has been effective in today's training" considered by the learners.

Results showed that OSIRT was successfully applied and received by learners throughout the course. Across the four days, which were analyzed for OSIRT's effectiveness, 91 percent felt they "agree" or "strongly agree" with the statement presented (Figure 6). Prior to the course, none of the officers had used OSIRT. Daily evaluations support this assertion, with many officers using freeform answers to praise the tool noting its usefulness with comments such as: "it is extremely useful for structuring search and investigation process", "[it is] very useful and makes things easy", "it streamlines the process and makes it easier as an investigator", "[it is] very very useful! - couldn't have done it without OSIRT", and "everything can be done in OSIRT".

Figure 6. OSIRTs effectiveness



In the post-course evaluation, learners were asked "Was OSIRT useful during the course?". Everyone responded "yes", expressing their praise for the tool with eight participants stating they would be using OSIRT to enhance the capabilities within their role for conducting OSR. Two participants expressed they were 'unsure' and one stated they would not be using the tool. The reasons for not being able to use OSIRT were concerns over IT restrictions. A positive response from the cohort on the toolkit also meant that OSIRT was mentioned as a specific skill they would apply back on-the-job and as an important aspect learned on the course. The toolkit satisfies several challenges noted by the learners in their pre-course questionnaire, for instance: the current state of use of a number of tools, etc., where a number of participants noted the tool as "excellent" and "fantastic" which is "well designed" with participants "amazed" that the software is free.

Participant Course Evaluation

Eleven officers completed the immediate post-course evaluation, with eight completing the delayed post-course evaluation. Participants identified their attendance on the course was "to acquire new skills" (nine), "to improve current knowledge" (seven), "to familiarise [themselves] to train other in OSR" (five), and "to become certified in OSR" (four). One officer expressed the course was "mandatory", with two others stating, "to use at work" and "to ensure those in my office with no training do not have to carry the responsibility of conducting and capturing open source research without that training" respectively. The course, at the time of writing, is the only accredited course in the UK to help officers conduct online investigations efficiently and with ease and knowledge of processes and relevant data. Findings demonstrate the course is delivered well, meeting expectations of officers.

Reaction – Level 1

Level one statements look at, for instance, the engagement of officers and relevance of training. When applying Cronbach's alpha to four statements categorized as 'reaction', an alpha (α) score of 0.70 was found; an acceptable reliability. Further to this, results from the immediate post-course evaluation demonstrate a strong percentage of officers who agree they took responsibility for their learning and that trainers enhanced the learning on the course.

Results from both evaluations showcase OSIRT's usefulness and effectiveness at helping investigating officers "capture online resources" as well as helping to retain and maintain audit trails. Respondents expressed that capturing and finding open source information was the most relevant information taken from the course, with all recalling OSIRT and evidential capture as their most memorable content.

To assess training satisfaction, participants were asked open-ended questions on whether anything could be improved on the course. Several yielded responses such as “no, it was pitched about right” and “no I liked it”. While three officers felt the course could run longer due to the quantity of content covered. Others provided positive and constructive improvements, mentioning they would have liked more on topics such as social media, cryptocurrency and “more about research of an individual”. Officers express no real issues, showcasing the courses effective delivery for this cohort.

Expanding on this, the delayed post-course evaluation also sought feedback to discover what topics could be added. Officers felt the course needed more on the “levels of open source research”, “case law”, “how websites are created” and “social media”. Many of the suggestions will be considered for future delivery of the course.

Learning – Level 2

To achieve level two of Kirkpatrick’s model (i.e., identifying learning and its effectiveness), several questions and statements focused on knowledge, skills, confidence, relevance, and learning styles. A key element useful to identifying the effectiveness of the course content was to ask learners to pick three important concepts/topics they learned during the course. Results show that using OSIRT was the most mentioned topic (nine), followed by steganography (four), and social networking (three). These topics were also specific skills which officers plan to use in their job when asked.

Eight statements covering aspects from quality of content, delivery, and confidence of application were asked of participants. A tally of the collated responses for level two demonstrated that 86% of the cohort achieved learning on the course, with 91% feeling that there was sufficient time allocated to delivering the course content. Applying Cronbach’s alpha shows a score of 0.88 across statements demonstrating a strong reliability between item correlation across eleven participants. Additionally, it was a strong indication that officers felt they learned skills transferable to the workplace.

To build a comparison between the immediate post evaluation questionnaire, officers were asked to identify what content they remembered the most. Mentioned were: OSIRT (1) and searching, capturing (6) and analyzing (1) open source information. Although OSIRT was not explicitly mentioned by all officers, capturing open sources was mentioned by all. The only tool used on the course to capture evidential data was OSIRT, so it can be inferred that OSIRT was an aid to their learning. Further testament to this are free comments provided which mention how it was “nice to discover OSIRT”.

Behavior – Level 3

So far results have shown participants were satisfied with the training and OSIRT, while demonstrating digestion of the subject matter. Level three is used to determine how much knowledge, skills, and attitudes have been transferred following training and how on-the-job behavior has consequently changed.

A strong consensus was illustrated by participants, in the delayed post-course evaluation, towards the practical application of course learning and OSIRT within four weeks. A few mentioned short delays due to work commitments, however, found the course materials sufficient in refreshing learning. Other officers noted no difficulties or "nothing unusual" when applying gained skills. One officer positively reflected by articulating "there were some things on the course [they] wondered why [they] were shown but it made more sense a few weeks after the course". Demonstrating development and maintenance of relationships between the training and business requirements.

Officers were then asked to consider and rate, using a Likert scale from 'little or no application' (recoded to 1) to 'very strong degree of application, and desire to help others do the same' (recoded to 5), their on-the-job behavior in accordance with course objectives. In the first instance, Cronbach's alpha returned a negative result. Field (2006) states that in cases where poor correlation between items [is found,] then some should be revised or discarded. In this instance two statements were removed leading to $\alpha = 0.76$ and demonstrating a strong internal reliability among the items.

The two statements excluded asked officers to consider their "Ability to navigate the web in order to capture and evaluate relevant data" and "Obtain familiarity with social networking sites". While these introduced a negative alpha, a breakdown of the statements demonstrates a positive impact from course back in the workplace. Results showed that each officer felt a strong degree of application (7) or very strong degree of application with desire to help others (1) with their ability to capture and evaluate relevant data. Furthermore, these concepts were formatively fed back by officers in free-form throughout post-course questionnaires.

A varied response was given for the statement "obtain familiarity with social networking sites", where three officers expressed a 'moderate degree of application' and five who expressed a 'strong degree of application'. The reason for this disparate response is not known, but speculatively it may be due to the statement's phrasing. For example, "moderate degree of application" for the statement "Obtain familiarity with social networking sites" does not align. On reflection, a statement such as "Usage of social networking sites" would have been less ambiguous.

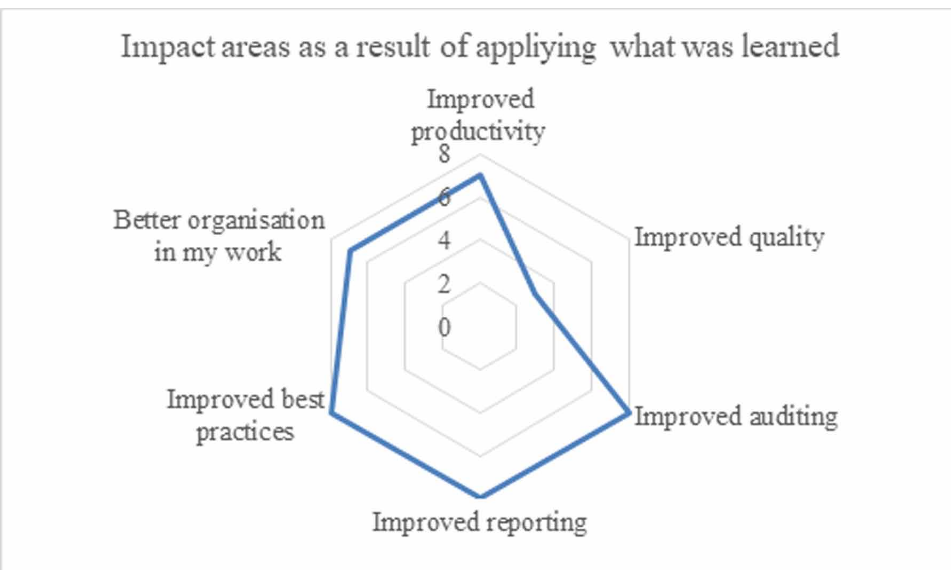
Results – Level 4

This level looks at the impact of the course and OSIRT on the business through perspectives of the attending officers. Both post-course evaluations are used to assess 'results' e.g., the perceived, and resulting, impact of the application of learning to the job for departments and/or organization.

Immediate post-course evaluation found all, bar one, officers express the course would make a difference to the way they do their job. Officers expected to see positive impact in areas such as "greater confidence in conducting OSR" and "feeling better equipped to understand, speed-up and improve the OSR process". Responses from delayed post-course evaluation corroborate this, finding OSIRT and capturing of open sources as the main enhanced areas in officers' jobs. Course materials and OSIRT "slotted into [their] role quite nicely" and the "course … help[ing] with some of the finer details". OSIRT's success as an investigative tool, its influence on officers' roles and asset to police departments was epitomized by one officer noting: "our team now uses OSIRT and the majority of us use it most days".

Officers saw improvements in most areas of their work, as demonstrated by Figure 7. Interestingly, only three respondents saw an increase in the quality of their work. The authors speculate this is caused by professional bias, whereby officers may have felt the work they previously produced before the course to already be of high quality, and hence nothing to improve upon.

Figure 7. Impacts felt due to application of learning by officers



DISCUSSION

The daily course evaluations represented well-rounded views that sessions matched the learning styles officers had noted in the pre-course survey. Occasionally, topics challenged a few of the cohort, but this was abated with trainers providing one-to-one sessions. Observations also confirmed that some of the cohort were forthright with their IT abilities. This may explain why the advanced topics, such as encryption, were a challenge to those participants.

While the pre-survey showed little OSR experience among the officers, results indicated that all LEOs learned OSR skills during the course. This was highlighted by the fact that all the cohort passed the examination. For a majority of officers present, the overall pace of the program was just right for their learning style and speed. However, given the variety of skill-sets on the course, several participants did feel the course went a little fast for them. Suggestions for improvements to slow down the pace of certain sessions were relayed to trainers. Although these problem areas were identified, the consensus was the course provided a number of key topics and skill-sets which LEOs can utilize in the workplace. Results demonstrated that many turned back to their course notes and materials on-the-job, again showing the application of knowledge and skills learned.

The success of the RITES course was further strengthened with the use of OSIRT and its function in aiding OSR. Responses sought throughout this study, from daily surveys to direct and delayed post-course evaluations, saw the cohort provide positive responses to the tool's effectiveness. Further praise was vocalized by LEOs to the usefulness and ease-of-use of the tool, particularly for helping officers in its versatility and ability to methodically conduct OSR.

LIMITATIONS AND FUTURE RESEARCH

The main limitation of this article is the number of participants, a small group of officers. Future research will look at multiple cohorts of officers trained under the RITES course to analyze, compare and discuss findings toward the effectiveness of the course and OSIRT in helping investigating officers conduct OSR.

CONCLUSION

This article looked to evaluate the overall effectiveness of the RITES course offered by the UK's College of Policing, OSIRT's integration into the course, and its subsequent usage on-the-job by LEOs. Results showed the RITES course as an effectual training aid to LEOs conducting OSR, and OSIRT as an effective tool for LEOs who conduct open source investigations as part of their role. Evaluation of the course took the approach of Kirkpatrick's model, where study responses showed knowledge transfer to real-life investigations, skill-sharing and the integration of OSIRT within their teams.

As the march of technology forges ahead, so must the education of those having to navigate its ever more complex wake. The police must evolve symbiotically with modern life to stay on top of the types of crime that now dominate the headlines. To grow effectively, their learning techniques and educational ethos must harness the most efficient teaching styles and tools; the RITES course and OSIRT is helping do just that. By engaging learners and diversifying their classroom experience, the police are encouraging the best retention for information. Incorporating OSIRT into this experience can improve the efficacy of learned skills in providing a successful and efficient tool. The RITES course and OSIRT are an ideal integration of modern learning and modern tools, to help police keep up with this modern world.

ACKNOWLEDGMENT

Thank you to the College of Policing and all the participants, and an extended thank you Russell Taylor, the lead trainer on the RITES course. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

ACPO. (2013). *Online Research and Investigation Guidance* (No. 1.2). Retrieved from http://library.college.police.uk/docs/appref/online-research-and-investigation-guidance.pdf

Birzer, M. L. (2003). The theory of andragogy applied to police training. *Policing: An International Journal of Police Strategies & Management*, *26*(1), 29–42. doi:10.1108/13639510310460288

Birzer, M. L., & Roberson, C. (2007). *Policing today and tomorrow*. Pearson/ Prentice Hall.

Capacity Building and Training Directorate. (2012). *Transfer Evaluation (International Police Training Journal No. 3)*. Lyon, France: INTERPOL.

College of Policing. (2017). Researching, Identifying and Tracing the Electronic Suspect. Retrieved from http://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Researching-Identifying-Tracing-Electronic-Suspect.aspx

Field, A. (2006). Reliability Analysis | C8057 (Research Methods II): Reliability Analysis. University of Sussex. Retrieved from http://www.discoveringstatistics.com/docs/reliability.pdf

Genoe, R., Toolan, F., & McGourty, J. (2014). Programming for Investigators: From Zero to Hero in 4 Days. Presented at the Cybercrime Forensics, Education and Training (CFET), Canterbury Christ Church University. Retrieved from https://www.researchgate.net/publication/271511408_Programming_for_Investigators_From_Zero_to_Hero_in_Four_Days

George, D., & Mallery, P. (2016). *IBM SPSS Statistics 23 step by step: A simple guide and reference*. Routledge. doi:10.4324/9781315545899

Gliem, J. A., & Gliem, R. R. (2003). Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-type Scales. *Presented at the Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education*, Columbus, OH: The Ohio State University.

Grace, M. (2001). Continuing professional development: Learning styles. *British Dental Journal*, *191*(3), 125–128. doi:10.1038j.bdj.4801116 PMID:11523883

Haberfeld, M. R., Clarke, C. A., & Sheehan, D. L. (2011). *Police organization and training: innovations in research and practice*. Springer Science & Business Media.

Hallenberg, K., O'Neil, M., & Tong, S. (2016). Watching the detectives: researching investigative practice. In *Introduction to Policing Research: Taking Lessons from Practice* (pp. 101–114). Abingdon, Oxon: Routledge.

Hess, K. M., Orthmann, C. H., & Cho, H. L. (2013). *Police operations: theory and practice*. Cengage Learning.

Kirkpatrick, D., & Kirkpatrick, J. D. (2006). *Evaluating training programs: The four levels* (3rd ed.). San Francisco, California: Berrett-Koehler Publishers.

Kirkpatrick, J. D., & Kirkpatrick, W. K. (2016). *Kirkpatrick's four levels of training evaluation*. Association for Talent Development.

Kirkpatrick Partners L.L.C. (2010). Kirkpatrick Hybrid Evaluation Tool Template. Retrieved from http://www.kirkpatrickpartners.com/Portals/0/Resources/Certified%20Only/Kirkpatrick%20Hybrid%20Evaluation%20Tool%20Template.docx

Loewenthal, K., & Lewis, C. A. (2015). *An introduction to psychological tests and scales*. Psychology Press.

Queen, C. R. (2016). *Effectiveness of problem-based learning strategies within police training academies and correlates with licensing exam outcomes*. Western Michigan University.

Stephens, P. (2012). An evaluation of Linux cybercrime forensics courses for European Law Enforcement. In N. Clarke & S. Furnell (Eds.), *Proceedings of the Sixth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2012)* (pp. 119–128). Plymouth University.

Tamkin, P., Yarnall, J., & Kerrin, M. (2002). *Kirkpatrick and beyond: A review of models of training evaluation (IES Research Networks No. 392)*. Brighton, United Kingdom: The Institute for Employment Studies; Retrieved from https://pdfs.semanticscholar.org/6845/52ac8528bfaed28fc8337a1a57b94c27aa39.pdf

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, *2*, 53–55. doi:10.5116/ijme.4dfb.8dfd PMID:28029643

Tong, S., Bryant, R. P., & Horvath, M. A. H. (2009). *Understanding criminal investigation*. John Wiley & Sons.

van Griethuijsen, R. A. L. F., van Eijck, M. W., Haste, H., den Brok, P. J., Skinner, N. C., Mansour, N., ... BouJaoude, S. (2015). Global patterns in students' views of science and interest in science. *Research in Science Education*, *45*(4), 581–603. doi:10.100711165-014-9438-6

Vodde, R. F. (2009). *Andragogical Instruction for Effective Police Training*. Cambria Press.

This research was previously published in the International Journal of Cyber Research and Education (IJCRE), 1(1); edited by Lawrence A. Tomei; pages 13-26, copyright year 2019 by IGI Publishing (an imprint of IGI Global).

Related Readings

To continue IGI Global's long-standing tradition of advancing innovation through emerging research, please find below a compiled list of recommended IGI Global book chapters and journal articles in the areas of emergency services, emergency services, and policing technologies. These related readings will provide additional information and guidance to further enrich your knowledge and assist you with your own research.

Ahmed, A. (2018). Communication Process of Disaster Management: Shift From Web 2.0 to Web 3.0. In Z. Liu & K. Ota (Eds.), *Smart Technologies for Emergency Response and Disaster Management* (pp. 243–263). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2575-2.ch009

Akerkar, R. (2018). Processing Big Data for Emergency Management. In Z. Liu & K. Ota (Eds.), *Smart Technologies for Emergency Response and Disaster Management* (pp. 144–166). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2575-2.ch005

Anastasiou, A., Giokas, K., Koutsouri, G., & Iliopoulou, D. (2017). Intelligent Medication Adherence Monitoring System. In A. Moumtzoglou (Ed.), *Design, Development, and Integration of Reliable Electronic Healthcare Platforms* (pp. 72–85). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-1724-5.ch004

Axelrod, E. M. (2017). Employee Assistance Programs: Counseling and Psychological Services for Law Enforcement Officers. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 199–219). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch010

Bacon, L., MacKinnon, L. M., Flippoupolitis, A., & Kananda, D. (2017). Developing a Public Online Learning Environment for Crisis Awareness, Preparation, and Response. *International Journal of Information Systems for Crisis Response and Management*, *9*(2), 18–36. doi:10.4018/IJISCRAM.2017040102

Ben-Porath, Y. S., Corey, D. M., & Tarescavage, A. M. (2017). Using the MMPI-2-RF in Preemployment Evaluations of Police Officer Candidates. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 51–78). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch003

Bhattacharya, M., Wamba, S. F., & Kamdjoug, J. R. (2019). Exploring the Determinants of ERP Adoption Intention: The Case of ERP-Enabled Emergency Service. *International Journal of Technology Diffusion*, *10*(4), 58–76. doi:10.4018/IJTD.2019100104

Bohl-Penrod, N. K., & Clark, D. W. (2017). Peer Support in Public Safety Organizations. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 237–250). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch012

Bouchemal, N., Maamri, R., & Bouchemal, N. (2019). Telemonitoring Healthcare System-Based Mobile Agent Technology. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 198–205). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch008

Bougoulias, K., Kouris, I., Prasinos, M., Giokas, K., & Koutsouris, D. (2017). Ob/Gyn EMR Software: A Solution for Obstetricians and Gynecologists. In A. Moumtzoglou (Ed.), *Design, Development, and Integration of Reliable Electronic Healthcare Platforms* (pp. 101–111). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-1724-5.ch006

Boussebough, I., Chaib, I. E., & Boudjit, B. (2019). An Ambient Multi-Agent System for Healthcare Monitoring of Patients With Chronic Diseases. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 61–71). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch003

Bradford, A. C., McElroy, H. K., & Rosenblatt, R. (2017). Social Climate Change and the Modern Police Department: Millennials, Marijuana, and Mass Media. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 296–313). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch015

Brucia, E., Cordova, M. J., & Ruzek, J. I. (2017). Critical Incident Interventions: Crisis Response and Debriefing. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 119–142). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch006

Christopher, M. E., & Tsushima, V. G. (2017). Police Interactions with Persons-in-Crisis: Emergency Psychological Services and Jail Diversion. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 274–294). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch014

Clark, D. W., & White, E. K. (2017). Law Enforcement Officer Suicide. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 176–197). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch009

Costarides, V., Zygomalas, A., Giokas, K., & Koutsouris, D. (2017). Robotics in Surgical Techniques: Present and Future Trends. In A. Moumtzoglou (Ed.), *Design, Development, and Integration of Reliable Electronic Healthcare Platforms* (pp. 86–100). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-1724-5.ch005

Cotton, D., & Coleman, T. G. (2017). The Evolution of Police Interactions with People with Mental Health Problems: The Third Generation (Strategic) Approach. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 252–273). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch013

Curran, S. F., Holt, E. O., & Afanador, J. H. (2017). Transition and Reintegration of Military Personnel to Law Enforcement Careers. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 158–175). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch008

Czarnecka, K. H., & Pawliczak, F. (2018). Managed Healthcare: A Temporary Trend or a New Standard for Providing Health Services? In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 1–12). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch001

Detrick, P., & Chibnall, J. T. (2017). A Five-Factor Model Inventory for Use in Screening Police Officer Applicants: The Revised NEO Personality Inventory (NEO PI-R). In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 79–92). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch004

Evans, K. S., & Wang, E. B. (2019). Data Analysis and Integration in Healthcare. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 220–234). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch010

García-Campos, J. M., Gutiérrez, D., Sánchez-García, J., & Toral Marn, S. (2018). A Simulation Methodology for Conducting Unbiased and Reliable Evaluation of MANET Communication Protocols in Disaster Scenarios. In Z. Liu & K. Ota (Eds.), *Smart Technologies for Emergency Response and Disaster Management* (pp. 106–143). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2575-2.ch004

Garrido, S., & Nicoletti, J. (2017). First Responder Psychological Recovery Following a Mass Casualty Event. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 143–157). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch007

Gheisari, M., & Esnaashari, M. (2018). Data Storages in Wireless Sensor Networks to Deal With Disaster Management. In Z. Liu & K. Ota (Eds.), *Smart Technologies for Emergency Response and Disaster Management* (pp. 196–222). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2575-2.ch007

Grace, R., Kropczynski, J., Pezanowski, S., Halse, S., Umar, P., & Tapia, A. (2018). Enhancing Emergency Communication With Social Media: Identifying Hyperlocal Social Media Users and Information Sources. *International Journal of Information Systems for Crisis Response and Management*, *10*(3), 20–41. doi:10.4018/IJISCRAM.2018070102

Gu, B., & Mizuno, O. (2018). Application of Game Theory for Network Recovery After Large-Scale Disasters. In Z. Liu & K. Ota (Eds.), *Smart Technologies for Emergency Response and Disaster Management* (pp. 223–242). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2575-2.ch008

Gu, Y., Peng, M., Ren, F., & Li, J. (2018). WiFi Fingerprint Localization for Emergency Response: Harvesting Environmental Dynamics for a Rapid Setup. In Z. Liu & K. Ota (Eds.), *Smart Technologies for Emergency Response and Disaster Management* (pp. 86–105). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2575-2.ch003

Habiba, M., & Akhter, S. (2018). Exploring Cloud-Based Distributed Disaster Management With Dynamic Multi-Agents Workflow System. In Z. Liu & K. Ota (Eds.), *Smart Technologies for Emergency Response and Disaster Management* (pp. 167–195). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2575-2.ch006

Kamruzzaman, S. M., Fernando, X., Jaseemuddin, M., & Farjow, W. (2018). Reliable Communication Network for Emergency Response and Disaster Management in Underground Mines. In Z. Liu & K. Ota (Eds.), *Smart Technologies for Emergency Response and Disaster Management* (pp. 41–85). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2575-2.ch002

Karthick, G. S., & Pankajavalli, P. B. (2019). Healthcare IoT Architectures, Technologies, Applications, and Issues: A Deep Insight. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 235–265). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch011

Kasiviswanathan, U., Kushwaha, A., & Sharma, S. (2019). Development of Human Speech Signal-Based Intelligent Human-Computer Interface for Driving a Wheelchair in Enhancing the Quality-of-Life of the Persons. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 21–60). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch002

Kelly, J., & Hoban, J. E. (2017). Health and Wellness Programming: The Added Contribution of an Ethical Mindset. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 220–236). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch011

Komendziński, T., Mikołajewska, E., & Mikołajewski, D. (2018). Cross-Cultural Decision-Making in Healthcare: Theory and Practical Application in Real Clinical Conditions. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 276–298). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch015

Liberska, H. (2018). Building a Sense of Security in a Patient: A Psychological Perspective. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 145–173). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch008

Masoud, M. P., Nejad, M. K., Darebaghi, H., Chavoshi, M., & Farahani, M. (2018). The Decision Support System and Conventional Method of Telephone Triage by Nurses in Emergency Medical Services: A Comparative Investigation. *International Journal of E-Business Research*, *14*(1), 77–88. doi:10.4018/IJEBR.2018010105

Mayer, M. J., & Corey, D. M. (2017). Current Issues in Psychological Fitness-for-Duty Evaluations of Law Enforcement Officers: Legal and Practice Implications. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 93–117). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch005

McCutcheon, J. L. (2017). Emerging Ethical Issues in Police and Public Safety Psychology: Reflections on Mandatory vs. Aspirational Ethics. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 314–334). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch016

Mendes, D., Lopes, M. J., Romão, A., & Rodrigues, I. P. (2017). Healthcare Computer Reasoning Addressing Chronically Ill Societies Using IoT: Deep Learning AI to the Rescue of Home-Based Healthcare. In A. Moumtzoglou (Ed.), *Design, Development, and Integration of Reliable Electronic Healthcare Platforms* (pp. 32–48). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-1724-5.ch002

Mishra, S., & Panda, M. (2019). Artificial Intelligence in Medical Science. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 306–330). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch014

Mitchell, C. L. (2017). Preemployment Psychological Screening of Police Officer Applicants: Basic Considerations and Recent Advances. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 28–50). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch002

Moumtzoglou, A. (2017). Digital Medicine: The Quality Standpoint. In A. Moumtzoglou (Ed.), *Design, Development, and Integration of Reliable Electronic Healthcare Platforms* (pp. 179–195). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-1724-5.ch011

Moumtzoglou, A., & Pouliakis, A. (2017). Population Health Management and Cervical Cancer Screening Programs: Roadmap, Design, and Implementation of a Supporting IT System. In A. Moumtzoglou (Ed.), *Design, Development, and Integration of Reliable Electronic Healthcare Platforms* (pp. 1–31). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-1724-5.ch001

Mreła, A., & Sokołov, O. (2018). Formal Methods for Assessing Patient Satisfaction in a Patient-Doctor Relationship. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 201–219). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch011

Mularska-Kucharek, M. (2018). Social Capital and Subjective Quality of Life. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 174–185). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch009

Naaz, S., & Siddiqui, F. (2019). Application of Big Data in Digital Epidemiology. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 285–305). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch013

Pasternak, A. (2018). Building Relationships Within a Therapeutic Team. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 220–243). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch012

Petersen, L., Fallou, L., Reilly, P., & Serafinelli, E. (2017). European Expectations of Disaster Information provided by Critical Infrastructure Operators: Lessons from Portugal, France, Norway and Sweden. *International Journal of Information Systems for Crisis Response and Management*, *9*(4), 23–48. doi:10.4018/IJISCRAM.2017100102

Pieczka, B. (2018). Management of Risk and Adverse Events in Medical Entities. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 31–46). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch003

Pramanik, P. K., Pal, S., & Mukhopadhyay, M. (2019). Healthcare Big Data: A Comprehensive Overview. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 72–100). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch004

Rezaee, R., Baslyman, M., Amyot, D., Mouttham, A., Chreyh, R., & Geiger, G. (2017). Real-Time, Location-Based Patient-Device Association Management: Design and Proof of Concept. *International Journal of Healthcare Information Systems and Informatics*, *12*(3), 37–61. doi:10.4018/IJHISI.2017070103

Rodrigues, P. M., Freitas, D., Teixeira, J. P., Alves, D., & Garrett, C. (2017). Early Detection of Electroencephalogram Temporal Events in Alzheimer's Disease. In A. Moumtzoglou (Ed.), *Design, Development, and Integration of Reliable Electronic Healthcare Platforms* (pp. 112–131). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-1724-5.ch007

Rodrigues, P. M., Freitas, D., Teixeira, J. P., Alves, D., & Garrett, C. (2017). Early Detection of Electroencephalogram Temporal Events in Alzheimer's Disease. In A. Moumtzoglou (Ed.), *Design, Development, and Integration of Reliable Electronic Healthcare Platforms* (pp. 112–131). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-1724-5.ch007

Rosiek, A. (2018). The Assessment of Actions of the Environment and the Impact of Preventive Medicine for Public Health in Poland. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 106–119). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch006

Rosiek, A., & Rosiek-Kryszewska, A. (2018). Managed Healthcare: Doctor Life Satisfaction and Its Impact on the Process of Communicating With the Patient. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 244–261). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch013

Rosiek-Kryszewska, A., & Rosiek, A. (2018). The Impact of Management and Leadership Roles in Building Competitive Healthcare Units. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 13–30). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch002

Rosiek-Kryszewska, A., & Rosiek, A. (2018). The Involvement of the Patient and his Perspective Evaluation of the Quality of Healthcare. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 121–144). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch007

Rudinsky, J., & Hvannberg, E. T. (2017). Transferability of Voice Communication in Games to Virtual Teams Training for Crisis Management. *International Journal of Sociotechnology and Knowledge Development*, *9*(1), 1–25. doi:10.4018/IJSKD.2017010101

Sabrina, Y., & Tayeb, L. M. (2019). Edge Detection on Light Field Images: Evaluation of Retinal Blood Vessels Detection on a Simulated Light Field Fundus Photography. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 174–197). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch007

Sasikala, R., & Sureshkumar, N. (2019). Research Investigation and Analysis on Behavioral Analytics, Neuro Imaging, and Pervasive Sensory Algorithms and Techniques for Autism Diagnosis. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 206–219). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch009

Sielski, Ł., & Soczywko, J. (2018). The Physiotherapist as a Health Educator. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 262–275). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch014

Soczywko, J., & Rutkowska, D. (2018). The Patient/Provider Relationship in Emergency Medicine: Organization, Communication, and Understanding. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 74–105). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch005

T, K., & S, S. (2018). Smart Technologies for Emergency Response and Disaster Management: New Sensing Technologies or/and Devices for Emergency Response and Disaster Management. In Z. Liu, & K. Ota (Eds.), *Smart Technologies for Emergency Response and Disaster Management* (pp. 1-40). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2575-2.ch001

Tatham, P., Ball, C. M., Wu, Y., & Diplas, P. (2018). Using Long Endurance Remotely Piloted Aircraft Systems to Support Humanitarian Logistic Operations: A Case Study of Cyclone Winston. In Z. Liu & K. Ota (Eds.), *Smart Technologies for Emergency Response and Disaster Management* (pp. 264–278). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-2575-2.ch010

Trompetter, P. S. (2017). A History of Police Psychology. In C. Mitchell & E. Dorian (Eds.), *Police Psychology and Its Growing Impact on Modern Law Enforcement* (pp. 1–26). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0813-7.ch001

Usher, W. (2017). E-Health: Modern Communication Technology Platforms for Accessing Health Information. In A. Moumtzoglou (Ed.), *Design, Development, and Integration of Reliable Electronic Healthcare Platforms* (pp. 49–71). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-1724-5.ch003

Vaz, N. F. (2018). Patient Satisfaction. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 186–200). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch010

Venugopal, M. (2019). Evolution of Digital Technologies and Use of Virtual Assistants in Drug Development. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 1–20). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch001

Verma, R., Sehgal, V. K., & Nitin. (2017). Crisis Management Using Centrality Measurement in Social Networks. *International Journal of Mobile Computing and Multimedia Communications*, *8*(1), 19–33. doi:10.4018/IJMCMC.2017010102

Wójcik, A. (2018). The Impact of the Attitude of Medical Staff From Burnout on the Level of Ongoing Medical Services. In A. Rosiek-Kryszewska & K. Leksowski (Eds.), *Healthcare Administration for Patient Safety and Engagement* (pp. 47–73). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-3946-9.ch004

Xochelli, A., Stamatopoulos, K., & Karamanidou, C. (2019). Patient Involvement in Health Care. Different Terms Same Concept? *International Journal of Reliable and Quality E-Healthcare*, *8*(1), 1–10. doi:10.4018/IJRQEH.2019010101

Yellampalli, S. S., Kiran, N. R., & Malapur, I. (2019). Medi-Rings for Senior Citizens: Distributed EMR System. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 148–173). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch006

Yucesan, M., Gul, M., Mete, S., & Celik, E. (2019). A Forecasting Model for Patient Arrivals of an Emergency Department in Healthcare Management Systems. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 266–284). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch012

Zayed, N. M., & Elnemr, H. A. (2019). Deep Learning and Medical Imaging. In N. Bouchemal (Ed.), *Intelligent Systems for Healthcare Management and Delivery* (pp. 101–147). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-7071-4.ch005

Index

A

Accident Detection Kit 115, 120, 123, 138
Aegean Sea 142-143, 150, 160, 162-163, 172
Alert 21-22, 31, 35, 45, 91, 413-414, 419
App User 342, 345-346, 348, 354, 356
Apps 21, 67-73, 75-80, 82-84, 182, 348
Artificial Intelligence 41, 84
Avatar Behaviour 407, 420

B

Bomb-making 320, 327, 336
Broadcasts 24

C

Coast guard 143, 147
Computer Supported Collaborative Learning (CSCL) 377
Crime Hotspot 209-212, 219, 230-233
crisis management 17, 372-374, 376, 378-380, 383, 388, 390-392, 394-395, 399-407, 411-414, 416-426
Cybersecurity 292

D

Data Recording 67
Data Transmission 70, 72, 76, 79-80, 83, 103
Deceit 276, 290
Deception 271-281, 283-285, 289-290, 292
Deep Learning 47, 51-53, 58, 61
Denial and Deception (D&D) 271-272, 292
Design Guidelines 401, 412-413, 418-419, 423, 425
design principles 372, 379, 394
DETECT Model 271-274, 276, 280-281, 283-285, 289, 292
Digital Forensics 239, 241, 243-244, 246, 251, 255, 270
Discrete Event Simulation 144

E

Earthquake 21, 38-40, 42, 44-45, 47-51, 58, 61
Emergency doctor 88-89, 91-105
Examiners 239, 241, 246, 252, 255, 257, 266
Extortion 340-342, 345, 348, 354, 356-357
Extortionists 341, 356

F

FIR 342-344, 354, 356-357
First Responder 239, 241, 257, 260-262, 264-266, 270, 406
Flood 38, 42, 47, 49, 193, 197

G

Google Maps API 116, 121, 125, 128-129, 137
groupthink 372, 374-376, 379-381, 383-385, 388-394

H

Historical Data 38, 40-41, 58, 61, 146-147, 160, 172
Human Right App 356

I

Identification 3, 6, 8, 12, 41, 120, 272-274, 277, 290, 325, 332, 344, 418-419, 425
Incident Complaint 356
Intelligence Community (IC) 292
Interaction Process Analysis (IPA) 372, 384-385
Internet of Things 114, 117, 120, 122, 137

J

JPSC 340-341, 344-348, 352-354, 357
JPSC KP 340-341, 344-347, 353-354, 357

K

Kidnapping 341, 357
Kirkpatrick's Evaluation Model 434, 438

L

Law Enforcement 210, 212, 239-240, 256, 270-276, 279, 281, 283-285, 289-290, 292-294, 296, 298-300, 302, 317, 320-322, 324, 328-329, 333, 375, 377, 391-392, 434-435
Lexicon Based Sentimental Analysis 294, 296-297, 300, 303
Linear Hotspot 209, 225-227, 229-230, 232
Linear Regression Models 51
Linux 121, 255-256, 258, 266, 270
LiveCity 88-89, 94-96, 100-105

M

Medical simulation 96, 105
Mobile Cloud Computing 70

N

Nearest hospital 20, 114-115, 117, 121-122, 124-126, 137
Non-Verbal Cues 271, 273-274, 276, 280-281, 283-285, 292

O

Online Investigations 434, 436, 444
Online Multiplayer Games 423, 426
online role play simulation 372, 377, 379
Open Data 193, 195-196, 198, 201, 206

P

Paramedics 68, 88-93, 95-105, 400
Policing 180-183, 186-187, 189, 434-436, 438, 448-449
Predictive 180-182, 189
Prehospital emergency system 90
Prevention 58, 114, 117, 181, 183, 186, 210, 331, 417
Protection Money 341, 357
Public Service 358

R

Radio 117, 383, 400, 411, 413-419, 422, 427
Reconnaissance 320-321, 324, 331-333, 335
Red-Team 321, 324, 335
Ring-Shaped Hotspot 209, 219-222, 224, 228, 232-233

S

Search and Rescue 142, 144, 147
Security Information Service 193-195, 197-199, 206-207
Spatial Scan Statistics 209, 211-213, 218, 230, 233
Statistical Significance 209, 211, 214-216, 219-222, 224-225, 227

T

Target Selection 320-321, 329
Tele emergency doctor 89, 92-93, 95-105
Telemedicine 85, 89, 92-93, 100-105
Threat Call 357
Threat Call Report 357
Traffic Management 24

V

VANETs 19, 22, 24, 36
Verbal Cues 280, 283, 292
Video communication 88-89, 96, 100, 104-105
Virtual Environments 377, 399-401, 404, 407, 423, 425-426
Vulnerability Mapping 1, 14, 16

W

Web Application 21, 193, 195, 204, 207