UiO : University of Oslo

Manas Pradhan

Interoperability for Disaster Relief Operations in Smart City Environments

Dissertation submitted for the degree of Philosophiae Doctor

The Faculty of Mathematics and Natural Sciences

Department of Technology Systems

April 2021

Series of dissertations submitted to the
Faculty of Mathematics and Natural Sciences, University of Oslo
No. 2423

ISSN 1501-7710

Cover: Hanne Baadsgaard Utigard.
Print production: Reprosentralen, University of Oslo.

Abstract

In the 21st century, humans have advanced multi-folds in the era of science and technology. Human lives are most comfortable as ever in the history of mankind but all that might just disappear with long-term devastating effects from man-made and natural disasters. The question that lingers on for mankind is: ”How to plan and prepare for disasters and emergencies over which we have no control?”.

The destruction from such disasters can either be averted or recovered with the help of the strides in technology we have made. The world of Internet-of-Things (IoT) is the new revolution in the modern technology realm after the intrusion of internet and mobile technologies. IoT technologies have matured for large-scale deployment in public and private Information and Communications Technology (ICT) domains. Along with IoT, the concept of Smart Cities is also maturing for the urban human landscape. Multiple civil and industry bodies are collaborating to frame the future of humanity when humans start living in the extremely demanding and crowded city perimeters. IoT assets along with the legacy ICT assets are getting deployed for Smart City implementations with increasing availability and reliability while becoming cheaper to procure and use.

But with all the advancement of IoT and Smart City technologies, the question remains: ”Are we ready to deal with disasters with our technological prowess?”. The questions would attract a feigned silence from the audience since not all technologies are not designed to talk to each other.

This thesis contributes by investigating the interoperability aspects amongst the various IoT technologies and Smart City concepts. The overall goal of the research is to create an architecture, propose component interactions for the architecture and show its validity using prototypical implementations for allowing the interoperable operation of ICT assets in a Smart City environment. The architecture would enable rapid deployment of Humanitarian Assistance and Disaster Recovery (HADR) relevant technology assets on the ground allowing multiple HADR agencies to seamlessly communicate while having shared Situational Awareness (SA) and complementing each others capabilities.

Preface

This dissertation is submitted to the Department of Technology Systems, Faculty of Mathematics and Natural Sciences, University of Oslo, in fulfillment for the degree Philosophiae Doctor (PhD).

My main supervisor has been Dr. Frank T. Johnsen, Principal Scientist at Norwegian Defence Research Establishment (FFI). Dr. Josef Noll, Professor at University of Oslo has been my co-supervisor.

This research has been carried out in the period September 2018 to January 2021 with 3 semesters of course work, at the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) in Germany. The study was supported by funding from the Federal Defence Forces of Germany (Bundeswehr).

The IEEE papers included in the dissertation follow the IEEE guidelines for publishing self-authored papers. Each publication included shows the entire citation including the authors, publication magazine/paper/journal name, month/year and place. Additionally the co-author's signed authorization for using the contents have been provided as part of the thesis submission.

Acknowledgments

First, and above all, I would like to thank my primary supervisor, Frank T. Johnsen, for his directed guidance when I needed it the most and for his full support throughout my PhD work. I would also express huge thanks to my co-supervisor, Josef Noll, for his continuous guidance, constructive criticism and support of my work.

I would like to thank my colleagues at Fraunhofer FKIE for discussions, feedback and support. Especially Michael Wünder who is the head of department at FKIE and Michael Gerz, who acted as a project manager for the Bundeswehr funded work. I would also like to thank the entire North Atlantic Treaty Organization (NATO) Information Systems Technology (IST) 147 and 176 groups for the collaborated research work and the joint experiments. Especially Niranjan Suri from the US Army Research Labs (ARL) and my colleague Christoph Fuchs from FKIE, who provided good research vision and a well structured approach towards the collaborative work.

Finally, I would thank to my parents, family and friends who always provided me with support and commitment and trusted in me all through the years.

Thesis structure

The thesis is divided into three parts. *Part I* introduces the field of disaster relief operations in Smart City Environments, with particular focus on IoT and Smart City ICT within the scope of this research. It includes a summary of the research contributions which have been published in magazines and international conferences, and one under publication book chapter. *Part II* contains these research contributions. In *Part III* relevant appendices are provided.

Part I – This part follows the IMRaD (Introduction, Methods, Results, and Discussion) structure of scientific discourse [1]. Based on IMRaD: Chapter 1 describes the background and motivation, and the scientific method of the thesis. Chapter 2 provides an extended contextual background that provides an overview of the background and issues that are dealt with in the research. It provides a state-of-the-art literature review and a knowledge base that can be used to enhance the understanding of the research results presented. Following this introduction and background, the discussion of the scientific contributions and a summary of each included research paper is presented in Chapter 3. The conclusion in Chapter 4 summarizes the research contributions and limitations, and provides suggestions for further research.

Part II – This part contains the following eight research papers:

1. **Paper A**: Interoperability for Disaster Relief Operations in Smart City Environments.
2. **Book Chapter B**: Architectural considerations.
3. **Paper C**: Toward an Architecture and Data Model to Enable Interoperability between Federated Mission Networks and IoT-Enabled Smart City Environments.
4. **Paper D**: Security, Privacy, and Dependability Evaluation in Verification and Validation Life Cycles for Military IoT Systems.
5. **Paper E**: Leveraging Crowdsourcing and Crowdsensing Data for HADR Operations in a Smart City Environment.

6. **Paper F**: Enabling Interoperability for ROS-based Robotic Devices for Smart City HADR Operations.
7. **Paper G**: MARGOT Dynamic IoT Resource Discovery for HADR Environments.
8. **Paper H**: Deployment Architecture for Accessing IoT and Legacy Assets in a Smart City Environment for Coalition HADR Operations.
9. **Paper I**: Federation based on MQTT for Urban HADR Operations.

A brief summary and a detailed list of the publications and related work is provided in the next chapter.

Part III – One appendix is provided:

1. **Appendix A**: List of Smart City and IoT related acronyms.

List of publications

Part II of this thesis is composed of papers A-I.

The author of this thesis is the principal contributor and first author of papers A, C, D, E, F, H and I, joint first author of paper B. He is the fourth author of paper G.

A holistic research approach towards enabling interoperability for disaster recovery scenarios is presented in paper A. It follows with the architectural considerations for IoT systems where a analysis of the IoT architectures from various standardisation organisations is presented in book chapter B. Based on the analysis, suitable integration methods and technologies for IoT and Smart City data is presented. Using the architectural concepts of IoT and related technologies, in Paper C, an approach for a distributed federated deployment of IoT assets in Smart City environments is presented. The research then continued with a close examination of the Security, Privacy, and Dependability (SPD) aspects of IoT systems and the associated Verification and Validation (V&V) Life Cycles, which is presented in paper D. The process described how to determine their properties and thus their usability in rugged and adverse scenarios in military systems which resemble application in the HADR scenarios. Further inspection of IoT in the Smart City domain led to paper E which presented Crowdsourcing and Crowdsensing concepts. It described the implemented approaches in city and adverse environments for gaining real-time SA while leveraging human intelligence from the ground. Based on the HADR scenarios that require robotic operations for SA as well as human assistance, paper F presented how to enable interoperability for robots in Smart City scenarios while enabling federated usage between HADR agencies. The MARGOT (Multi-domain Asynchronous Gateway Of Things) platform is described in paper G. It enables dynamic IoT resource discovery for HADR Environments which is necessary in a heterogeneous ICT environment in the Smart City context and collaborative action between HADR agencies. Paper H described an architecture and data model to enable interoperability between Federated Mission Networks (FMN) and IoT networks in smart city environments. Finally, a deployment architecture for accessing IoT and Legacy Assets in a Smart City Environment for collaborative and quick disaster recovery operation is presented in paper I.

Main Contributions

Paper A Manas Pradhan, ”Interoperability for Disaster Relief Operations in Smart City Environments,” 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 711-714.

Abstract: *Internet-of-Things (IoT) technologies in the past decade have matured both in the hardware and software aspects for large-scale deployment. Alongst IoT, the Smart Cities Concept is also taking shape. Pilot projects and implementations in multiple cities are trying to find out the feasibility and applicability of Smart City Information and Communications Technology (ICT). IoT assets along with the legacy assets are essential for Smart City ICT implementations. With the evolution of Smart Cities and concentration of people in the cities, it becomes necessary to be ready for future Humanitarian Assistance and Disaster Recovery (HADR) operations. But the huge void in heterogeneous IoT and legacy technologies create a big hurdle in establishing and handling the HADR operations. This aim of this PhD is to investigate the interoperability aspects amongst the various IoT technologies and Smart City concepts. The goal is to create a framework and an architecture for allowing the interoperable operation of ICT assets in a Smart City environment. This framework would enable rapid deployment of HADR relevant technology assets on the ground allowing multiple HADR agencies to seamlessly communicate while having shared Situational Awareness (SA) and complementing each others capabilities.*

Book Chapter B (under Publication) Christoph Fuchs, Manas Pradhan, Niranjan Suri, Mauro Tortonesi, and Frank T. Johnsen. Architectural considerations. In Niranjan Suri, Konrad Wrona, and Zbigniew Zielinski, editors, Military applications of Internet of Things, chapter 3. Springer, 2021.

Abstract: The emergence of Smart City initiatives in many areas of the world has led to the rapid development and proliferation of Internet of Things (IoT) technologies. Successful deployments of IoT have resulted in the military looking at the impacts and benefits of IoT, both for directly leveraging IoT within the military environment as well as to interface with smart city environments for urban operations such as Humanitarian Assistance and Disaster Relief (HADR). This chapter describes the outcomes of the research focused on IoT Architectures from the

NATO IST-147 Research Task Group's activities. Architectural considerations both from the civilian and the military domains are examined in order to explore interoperability between them in Smart City environments. Challenges related to interfacing these two disparate domains are discussed and a reference architecture is proposed, which will allow multiple partners to exchange data, share resources, and achieve better situational awareness. The concepts discussed reuse and extend existing NATO (military) and commercial Information and Communications Technology (ICT) architectures for faster adoption by both parties. Finally, open research challenges are discussed as future research directions.

Paper C Manas Pradhan, Niranjan Suri, Christoph Fuchs, Trude H. Bloebaum and Michal Marks, "Toward an Architecture and Data Model to Enable Interoperability between Federated Mission Networks and IoT-Enabled Smart City Environments," in IEEE Communications Magazine, vol. 56, no. 10, pp. 163-169, October 2018.

Abstract: *The emergence of smart city initiatives in many areas of the world has led to rapid development and proliferation of Internet of Things (IoT) technologies. Successful deployments of IoT have resulted in the military looking at the impacts and benefits of IoT, both for directly leveraging IoT within the military environment as well as to interface with smart city environments for urban operations such as humanitarian assistance and disaster response. This article describes some of the outcomes of the NATO IST-147 Research Task Group that was established to explore the military applications of IoT. Within the NATO context, the concept of federated mission networks (FMNs) enables coalition partners to plan, prepare, establish, use, and terminate mission networks in support of federated operations. In this article, we propose an architecture and data model to enable interoperability between FMN and IoT networks in smart city environments. We review the various bottlenecks involved for such an environment and how a reference implementation can be set up to allow multiple partners to exchange data for sharing resources and provide better situational awareness. The concepts discussed reuse and improvise upon the existing NATO and commercial IoT standards for faster adoption. Finally, open research challenges are discussed as future research directions.*

Paper D Manas Pradhan and Josef Noll, "Security, Privacy, and Dependability Evaluation in Verification and Validation Life Cycles for Military IoT Systems," in IEEE

Communications Magazine, vol. 58, no. 8, pp. 14-20, August 2020.

Abstract: *The Internet of Things (IoT) is a disruptive technology that complements the usage of modern day information and communications technology (ICT) systems. IoT systems, with their small form and cost factor coupled with their increasing reliability, have made huge inroads in all markets. Connected to some form of interconnected networks, either to the mainstream Internet or private networks, they enable ubiquitous and to a large extent autonomous operation. This has taken away the idea that sensing, actuation, and computing needs to be dependent on expensive and complicated legacy systems. Although complete discontinuation of legacy systems is still quite a long journey and would not be completely possible, IoT systems show the waypoints as to how the ICT industry will evolve. The military domain is not far away from adopting IoT technologies in its operational construct. The NATO IST-147 and 176 research task groups have closely examined applicability of IoT for federated and ubiquitous military applications. Introducing IoT devices in the military domain requires verification and validation (V&V) of ICT systems as per operational guidelines. This article proposes and applies a concept for security, privacy, and dependability evaluation of IoT systems that could be used for V&V processes. This would enable more streamlined and standardized evaluations of IoT systems before they can be deemed usable for military contexts.*

Paper E Manas Pradhan, Frank T. Johnsen, Mauro Tortonesi and Sabine Delaitre, ”Leveraging Crowdsourcing and Crowdsensing Data for HADR Operations in a Smart City Environment,” in IEEE Internet of Things Magazine, vol. 2, no. 2, pp. 26-31, June 2019.

Abstract: *The future of the world's population concentration lies within the bounds of urban cities. Citizens, or humans, are the most important tangible resources in a smart city environment, and they need to be served as well as protected. The concept of smart cities is trying to accomplish the idea of serving the citizens by leveraging the potential of information and communications technology assets. Citizens have access to smart technologies and applications, and thus they form an indispensable component to complement and supplement a smart city's operation. Especially in humanitarian assistance and disaster recovery (HADR) operations, where a smart city's core infrastructure might be compromised, the assets of citizens can* *be put to use. This article aims to describe the current state of affairs for safety in cities and humanitarian assistance in emergency situations, which require leveraging situational awareness data. We discuss and propose mechanisms for connecting to and utilizing Crowdsourcing and Crowdsensing data in a smart city environment, which can assist in efficient HADR operations.*

Paper F Manas Pradhan and Sushma Devaramani, ”Enabling Interoperability for ROS-based Robotic Devices for Smart City HADR Operations,” MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, 2019, pp. 1-6

Abstract: *Smart Cities of the future come with the promise of betterment of human civilization. Technology usage in Smart Cities rely heavily on Internet-of-Things (IoT) concepts along with the legacy Information and Communications Technology (ICT) assets. Apart from the static assets deployed across the city such as sensors, the IoT revolution has enabled the development of cheaper yet effective robotic devices. While the robots in the market are becoming more accessible enabling adoption by private individuals as well as governmental agencies, there is the lack of interoperability between the robotic devices. Especially during Humanitarian Assistance and Disaster Recovery (HADR) operations in Smart City environments, robotic devices deployed from a single agency might not scale for HADR operations. In such cases, it is necessary to ensure multi-agency sharing of robotic capabilities. This paper proposes a ROS-based platform-independent architecture for robotic devices that can be adopted by civilian and military agencies to share capabilities during HADR operations.*

Paper G Lorenzo Campioni, Rita Lenzi, Filippo Poltronieri, Manas Pradhan, Mauro Tortonesi, Cesare Stefanelli and Niranjan Suri, ”MARGOT: Dynamic IoT Resource Discovery for HADR Environments,” MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, 2019, pp. 809-814.

Abstract: *Smart City services leverage sophisticated IT architectures whose assets are deployed in dynamic and heterogeneous computing and communication scenarios. Those services are particularly interesting for Humanitarian Assistance and Disaster Relief (HADR) operations in urban environments, which could improve Situation Awareness by exploiting the Smart City IT infrastructure. To this end, an* *enabling requirement is the discovery of the available Internet-of-Things (IoT) resources, including sensors, actuators, services, and computing resources, based on a variety of criteria, such as geographical location, proximity, type of device, type of capability, coverage, resource availability, and communication topology / quality of network links. To date, no single standard has emerged that has been widely adopted to solve the discovery challenge. Instead, a variety of different standards have been proposed and cities have either adopted one that is convenient or reinvented a new standard just for themselves. Therefore, enabling discovery across different standards and administrative domains is a fundamental requirement to enable HADR operations in Smart Cities. To address these challenges, we developed MARGOT (Multi-domain Asynchronous Gateway Of Things), a comprehensive solution for resource discovery in Smart City environments that implements a distributed and federated architecture and supports a wide range of discovery protocols.*

Paper H Manas Pradhan, Christoph Fuchs and Josef Noll "Deployment Architecture for Accessing Smart City and Coalition Assets for Multi-Agency HADR Operations," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2020, pp. 1-6.

Abstract: *The future of human civilization is evolving towards dense city environments where people concentrate for economic and strategic reasons. On parallel lines, cities are being transformed into Smart Cities with the help of progress in science and technology. One of the primary goals of a Smart City is to be people-centric i.e. to serve the citizens. Due to the global climate change the necessity to set-up methods and infrastructures to deal with disasters has become even more urgent. The cities need to be prepared for future Humanitarian Assistance and Disaster Recovery (HADR) Operations. The success of these operations will depend to a large degree on the quality of Situational Awareness (SA) and the instantaneous sharing of all relevant information among the various disaster recovery agencies. Future HADR operations that require multi-agency or even multi-country cooperation will thus be dependent on interoperability concerning information exchange. This paper presents an architecture and system concept for fast Situational Awareness (SA) assimilation and provisioning in HADR operations. The concept aims to enable the coalition disaster recovery agencies to cooperate with each other by utilis-*

ing existing Smart City assets and parallelly deploying their own assets.

Paper I Manas Pradhan "Federation based on MQTT for Urban HADR Operations," in IEEE Communications Magazine, vol. 59, no. 2, February 2021.

Abstract: *Today's age of Information and Communications Technologies (ICTs) in urban areas revolve around the application of Internet-of-Things (IoT) and application of IoT in Smart City constructs. IoT has enabled cheap and yet reliable ubiquitous computing for modern day ICT needs. As a result, the military community is actively looking into application of IoT for its operational needs. Federation and interoperability becomes complex for IoT implementation in the huge jungle of protocols and technologies available for IoT. This problem becomes critical in Humanitarian Assistance and Disaster Recovery (HADR) Operations where multiple agencies need to collaborate to bring quick and effective relief to disaster struck areas. Message Query Telemetry Transport (MQTT) is such an IoT-based protocol that is widely adopted in the industry for lightweight yet reliable messaging. This paper tries to provide an insight into federation based on MQTT with a prototype implementation between military and civilian ICT systems. This federation concept would enable lightweight, vendor-agnostic and interoperable message exchange while using existing information sources and preventing stove-piped systems.*

Related Work

R1 Manas Pradhan, Alexander Tiderko and Daniel Ota, "Approach towards achieving interoperability between military land vehicle and robotic systems," 2017 International Conference on Military Communications and Information Systems (ICMCIS), Oulu, 2017.

Abstract: *The battlefield scenarios are changing around the world presenting new challenges for the military. Battlefield environments have moved from the open to urban and constricted spaces forcing the military to adopt new doctrines and tactics for effective attack and defence. Whilst there have been many advances at the equipment level to support the ground forces i.e. the evolution of military vehicles and the introduction of robotic systems, there still exists a big gap in making these two* *entities work together. This gap also makes the idea of achieving a fully functional Network-Centric Warfare (NCW) environment less feasible. The data collected by the vehicles and robots need to be exchanged flawlessly so that the best operational picture of the battlefield can be presented to the ground forces for taking the correct action. Since the military operations nowadays require multinational forces conducting operations together, it is essential that the equipments from various countries are able to interoperate with each other in a coalition environment. Furthermore, the range of legacy sensors and other sub-systems available need to be interoperable with the new vehicles and robots to provide the teeth to the military for conducting operations. In order to support NATO military land vehicles for standardisation and interoperability, the NATO Generic Vehicle Architecture (NGVA) proposes an open architecture approach to land vehicle platform design and integration. The Robotics and Autonomous Systems Ground (RAS-G) Interoperability Profiles (IOPs) from the US Army, on the other hand, describe hardware and software interfaces for Unmanned Ground Vehicles (UGVs). In this paper, we present an approach towards achieving interoperability between the NGVA and IOP to support the future coalition battlefields. It allows the NGVA-based military land vehicles to be able to control UGVs and allows the exchange of ISR and other required data without any dependencies and bottlenecks.*

R2 Manas Pradhan, Fahrettin Gökgöz, Nico Bau and Daniel Ota, ”Approach towards application of commercial off-the-shelf Internet of Things devices in the military domain,” 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016, pp. 245-250.

Abstract: *Battlefield environments are evolving and presenting new challenges for the military all around the world. This is pushing the necessity for evolution of military sensor technologies at an unprecedented rate. While military contractors and manufacturers are coming up with newer and improved technologies, the commercial domain is growing at a much faster rate. It is high time that the military introduces the use of Commercial off-the-Shelf (COTS) sensors due their inherent advantages. In this paper, we present an approach towards using the COTS Internet of Things (IOT) sensors for sensing and surveillance on Unmanned Ground Vehicles (UGVs) which form a part of a convoy. The data gathered is processed and distributed be-*

tween the UGVs, over the convoy vehicles and to higher echelons using existing military communication framework extended by the MIOT architecture. The data distribution on the ground between the UGVs and convoy vehicles is carried out using the NATO Generic Vehicle Architecture (NGVA). The publishing of consolidated and processed data from the ground to the higher echelons like command centres is carried out using the Multilateral Interoperability Programme (MIP) specification.

R3 Manas Pradhan, "A Survey of Smart City Assets for Future Military Usage," 2018 International Symposium on Networks, Computers and Communications (ISNCC), Rome, 2018, pp. 1-6.

Abstract: *The primary purpose of military anywhere around the world is to protect and serve the people. Over the years, the role of the military has diversified which has required the military to serve countries in several capabilities. Be it active wars, intelligence gathering, rescue operations, anti-terrorist operations etc. , the modern military has to play a role. Since the military has to adapt to, prepare for and respond to the ever changing dynamics of people and surroundings around the world, it becomes necessary to look into what exists currently and what will form the future. Smart cities are such a phenomenon. The cities around the world are transforming to be "Smart", to meet various future challenges such as population migration and how to manage the living of such a huge number of people in a relatively small area, improving the quality of various services delivered to citizens, saving and optimizing resource utilization and so on. In such a scenario, where the population and assets need to be protected in Smart Cities, the militaries need to get a hold of the technologies and know the emerging trends in the smart cities. This would give the defence sector a head-start in knowing what capabilities are and would be available so that they are ready to employ their services alongside the Smart City solutions and thus serve their motto optimally. This paper entails the various Smart City assets from various cities as well as involved Internet-of- Things (IoT) technologies and tries to provide a picture of what the military in future can integrate with their solutions to serve the Smart Cities.*

R4 Konrad Wrona, Manas Pradhan, Mauro Tortonesi and Niranjan Suri. "Civil-Military Collaboration in Smart Environments under Adversarial Conditions". 2019 In The First International Workshop on Internet of Things for Adversarial Environments (in conjunction with IEEE INFOCOM 2019) (pp. 1-6). IEEE.

Abstract: *Natural disasters occur unpredictably and can range in severity from something locally manageable to large scale events that require external intervention. In particular, when large scale disasters occur, they can cause widespread damage and overwhelm the ability of local governments and authorities to respond. In such situations, Civil-Military Cooperation (CIMIC) is essential for a rapid and robust Humanitarian Assistance and Disaster Relief (HADR) operation. These type of operations bring to bear the Command and Control (C2) and Logistics capabilities of the military to rapidly deploy assets to help with the disaster relief activities. IoT, Smart Cities, and Smart Environments can significantly improve the ability for the military to quickly obtain Situation Awareness (SA) about the disaster and optimize the planning of rescue operations and allocation of resources to achieve the best possible effects. However, there are several interoperability and security challenges related to achieving an effective federated SA under adversarial conditions. In particular, one of the significant threats is the ability for an adversary to exploit the reduced effectiveness of local law enforcement, trust management, and cyber defence capabilities, as well as the overall uncertainty in the situation, to interfere with the HADR operation, for example, by injecting mis-information. The focus of this paper is to further examine this challenge of achieving Civil-Military cooperation for HADR operations while countering potential adversarial activities.*

R5 Niranjan Suri, Zbigniew Zielinski, Mauro Tortonesi, Christoph Fuchs, Manas Pradhan, Konrad Wrona, Janusz Furtak, Dragos Bogdan Vasilache, Michael Street, Vincenzo Pellegrini, Giacomo Benincasa, Alessandro Morelli, Cesare Stefanelli, Enrico Casini and Michal Dyk, ”Exploiting smart city IoT for disaster recovery operations,” 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 458-463.

Abstract: *Disaster recovery operations are extremely challenging and place significant demands on multiple resources, including local and international emergency response personnel, non-governmental organizations, and the military. In the immediate aftermath of a disaster, one of the most pressing requirements is for situational awareness (SA) so that resources, including personnel and supplies, may be prioritized to have the most impact and help those in the most need. As the recov-*

ery operations continue, the SA needs to be continuously updated based on changing conditions in the affected areas. There are many sources of information to provide SA, including reporting by the victims of the disaster as well as observations made by responding personnel. In this context, SA can be significantly enhanced via information obtained from Internet of Things (IoT) devices, especially in a smart city environment. This paper explores the potential to exploit Smart City IoT capabilities to help with disaster recovery operations.

R6 Manas Pradhan, Filippo Poltronieri and Mauro Tortonesi, ”Generic Architecture for Edge Computing Based on SPF for Military HADR Operations,” 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 225-230.

Abstract: *Internet-of-things (IoT) devices have led to ubiquitous, remote and autonomous computing at the edge of the networks. These devices offload sensing, actuation and processing tasks away from the core of the network. The concept of Smart Cities tries to leverage Edge Computing based on IoT technologies for remote and distributed computing. Sieve, Process and Forward (SPF) is a Value-of-Information (VoI) based Fog as a Service (FaaS) solution for dynamic IoT applications in Smart City scenarios. The military has been looking to utilize the SPF platform for Edge Computing to assist in Human Assistance and Disaster Recovery (HADR) operations. A recent NATO IST 147 RTG demonstration proved the validity of SPF, but also highlighted the need of extending the current architecture to support specific use-case scenarios for HADR systems. This paper tries to propose a generic architecture based on SPF to enable interoperability between military C2 (Command and Control) and core computing systems to support future HADR operations in Smart City environments.*

R7 Manas Pradhan, Filippo Poltronieri and Mauro Tortonesi, ”Dynamic Resource Discovery and Management for Edge Computing Based on SPF for HADR Operations,” 2019 International Conference on Military Communications and Information Systems (ICMCIS), Budva, Montenegro, 2019, pp. 1-6.

Abstract: *The Smart City concept tries to inherit the advantages of Internet-of-Things (IoT) into its realm to function alongside the existing legacy systems. One of the most promising aspects of IoT is Edge Computing, which tries to move the* *computing, traditionally done via a centralized infrastructure like the cloud to the edge of the network. This allows remote deployment of IoT assets closer to the source and application area of information enabling faster response times of action. Smart Cities of future envision using Edge Computing to their advantage for remote and distributed computing. Sieve, Process and Forward (SPF) is an Edge Computing solution for dynamic IoT applications for Smart City scenarios. The military is looking forward to use, as well as develop the SPF platform for its Edge Computing requirements. But currently, the SPF platform does not have the mechanism for remote discovery of edge resources and their management to leverage its potential completely. This paper tries to propose a resource discovery and management architecture and methodology for SPF to support future Human Assistance and Disaster Recovery (HADR) operations in Smart City environments with the vision of enabling interoperability between civilian and military platforms.*

R8 Frank T. Johnsen et al., ”Application of IoT in military operations in a smart city,” 2018 International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, 2018, pp. 1-8.

Abstract: *This paper addresses a scenario where a medium sized smart city in an Alliance nation has been struck by disaster. A small, multi-national force is deployed for disaster relief. Situational awareness (SA) is important so that resources, including personnel and supplies, may be prioritized to have the most impact and help those in the most need. This SA can be significantly enhanced via information obtained from Internet of Things (IoT) devices, especially in a smart city environment. This paper, which presents work performed by the NATO IST-147 “Military Applications of Internet of Things” group, explores the potential to exploit smart city IoT capabilities in military operations.*

Other scientific activities and achievements

1. Research and Development lead for IEEE IoT Smart Cities Working Group (2018-2021)

2. Vice-chair for IEEE P1951.1 working group: Standard for Smart City Component

Systems Discovery and Semantic Exchange of Objectives (2020-present)

3. Working Task Group lead for IEEE P1951.1 "Discovery of Smart City Assets" (2020-present)

4. German representative for NATO IST-147 group for Military applications of IoT (2017-2020)

5. German representative for NATO IST-176 group for Federated Interoperability of Military Command and Control (C2) and IoT Systems (2020-present)

6. Winner of Safety Days Hackathon at the University of Paderborn, Germany: designed and demonstrated a live system for the German Red Cross for evacuation of citizens during a disaster situation (2019)

7. Panel member for International Conference on Military Communications and Information Systems (ICMCIS) Conference (2021).

8. Winner of NATO Information Systems Technology (IST) Panel Young Scientist Award (2020)

9. Winner of NATO Science and Technology Organization (STO) Young Scientist Award Award (2021)

10. Special mention in NATO Secretary General's Annual Report (2021)

Contents

PART I: Introduction

1 Introduction

> "It wasn't raining when Noah built the ark."
>
> - *Howard Ruff, author and financial advisor*

Noah knew that the flood was coming and he prepared for it to save the earthlings. He gave a chance for life to spring back on earth. But real world does not work precisely that way, in the sense that disasters be it natural or man-made do not let us know beforehand that they are going to happen. They occur most of the time abruptly and when they occur, the damages echo for a very long time. In some cases, we can predict and to an extent prepare for them but in many, we have absolutely no prediction for such events. Damages to lives and property vary in proportion but they do have unprecedented impact on our lives. We recover from some, while some linger with us forever.

The only way to avert such disaster scenarios is to build our "*ark*". Noah had his tools and methods to build his ark which sufficed his needs. We also need tools and methods that can support the current age of Humanitarian Assistance and Disaster Recovery (HADR) operations. The circumstances around us in the 21st century have changed a lot for the good with respect to our technological advancements. On the other hand, the population demographics, tangible and intangible property characteristics have worsened with respect to how and at what scale we have to enable HADR agencies to secure our lives.

Internet-of-Things or IoT refers to: *"An ecosystem of physical objects that are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes and everyday people's lives."* [2]. In a broad sense, IoT encompasses everything connected to the internet or a network, where the physical objects such as simple sensors to smartphones, wearables and computing platforms are connected together and talk to each other. These interconnected objects gather and analyse information and accordingly create an action to help users perform tasks. Advancements in IoT technologies has affected our daily lives and the modern Information and Communication Technology (ICT) domain has adopted IoT as its integral component.

A Smart City is another such popular concept in the modern ICT deployment domains. It is a combination of services offered to the citizens and the government, bidirectionally to improve city functions, drive economic growth, provide inclusive and sustainable development all around [3]. Often the terms such as “digitalisation” or “digital transformation” are used in the context of Smart Cities. The idea underlying is the use of ICT to increase operational efficiency of the government’s functioning and share information with the city inhabitants for their welfare [4]. It plans to counter the service needs of modern demographics of human concentration in city and urban areas. The concept tries to build the modern utopia of human civilizations trying to provide inclusive, distributed, horizontal and vertical growth to its citizens. IoT has been one of the biggest enablers of Smart City concepts by providing the ubiquitous computing needed for modern day ICT strategies [5, 6]. Further details regarding IoT and its application for Smart Cities is provided in Chapter 2.

While we have the tools to build our “*ark*” and we know how to deploy those tools, the tools in many cases can not work with each other. It implies the lack of “*interoperability*” between the ICT technologies and their subsequent usage in Smart Cities. Smart Cities are mushrooming everywhere as isolated islands with no-to-less common components allowing them to talk to each other [7]. So, when a time comes when the HADR agencies have to deploy on the ground for post disaster operations, they would be at loss of time and resources. Owing to stove-piped nature of Smart City components and also of the HADR agencies, it will be a waste of their ICT capabilities. There needs to be interoperable architectures, frameworks and interfacing components deployed from Smart City and HADR agencies’ ends, to enable them to ensure fast and effective disaster recovery operations.

1.1 Use Case and Motivation

The five images 1.1, 1.2, 1.3, 1.4 and 1.5 are used to illustrate the use cases for this thesis. The back ground of the use case is: *“Natural Disasters around the World and their*

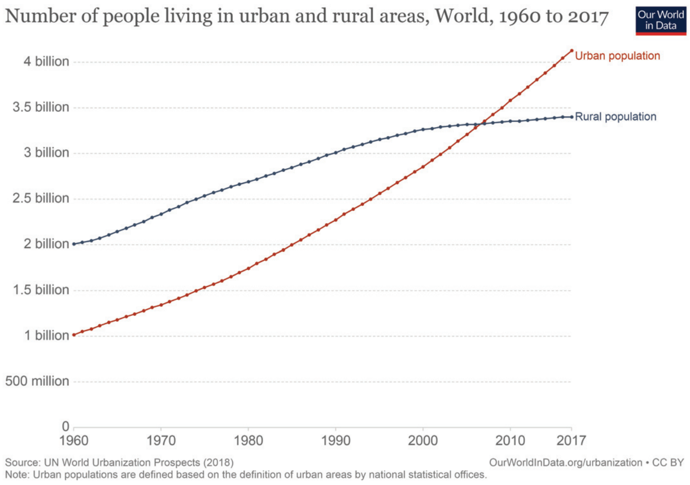


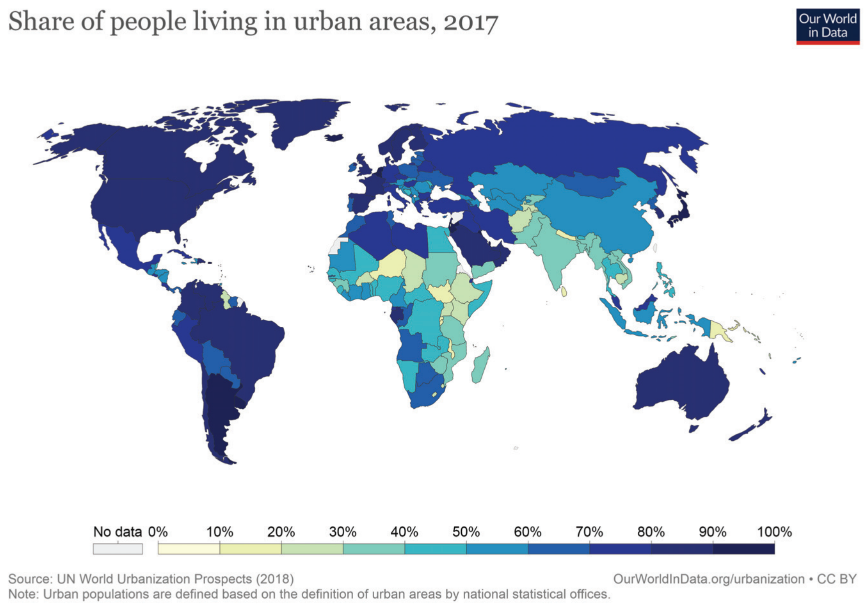
Figure 1.1: *Population Growth in Urban Areas [9]*

Impact on Human Civilization" [8].

Figure 1.1 shows the change in demographic landscape between the rural and urban areas since the 1960's. Humans are always drawn to areas of prosperity, sustainability and security (food, economic, social and political) [13]. Although selfish, its in every organism's nature to be more comfortable. With humans its just that, we need not just food but also inputs for other senses to perceive a complete life. Figure 1.2 on the other hand shows where these shifts are most visible. It shows the clear divide between countries able to industrialize faster than relatively lesser industrialized countries [14]. Population shifts in these industrialized countries tend to be more towards urban than rural.

Another trend is shown in Figure 1.3, where the lesser industrialized countries are trying to catch up and thus show a major shift in their city growths [15]. According to the United Nations (UN), 68% of the world population is projected to live in urban areas by 2050 [16]. Many Asian, African and South American countries are now experiencing inclusive growth and are fast shifting towards urban rather than rural cultures.

Further, figure 1.4 shows the global annual deaths by natural disasters. As seen in the graph, in the early 20th century, deaths due to droughts and floods contribute the most. Partly the reason is the two world wars and the post-effect of the wars in the countries to reconstruct themselves [17]. This hindered providing food securities and establishing



Source: UN World Urbanization Prospects (2018)
OurWorldInData.org/urbanization • CC BY
Note: Urban populations are defined based on the definition of urban areas by national statistical offices.

Figure 1.2: *Population Share in Urban Areas [9]*

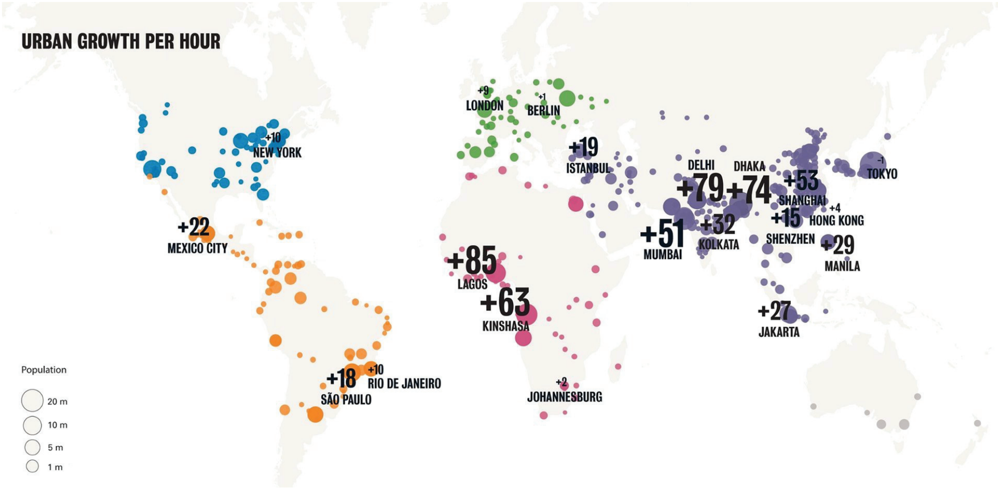
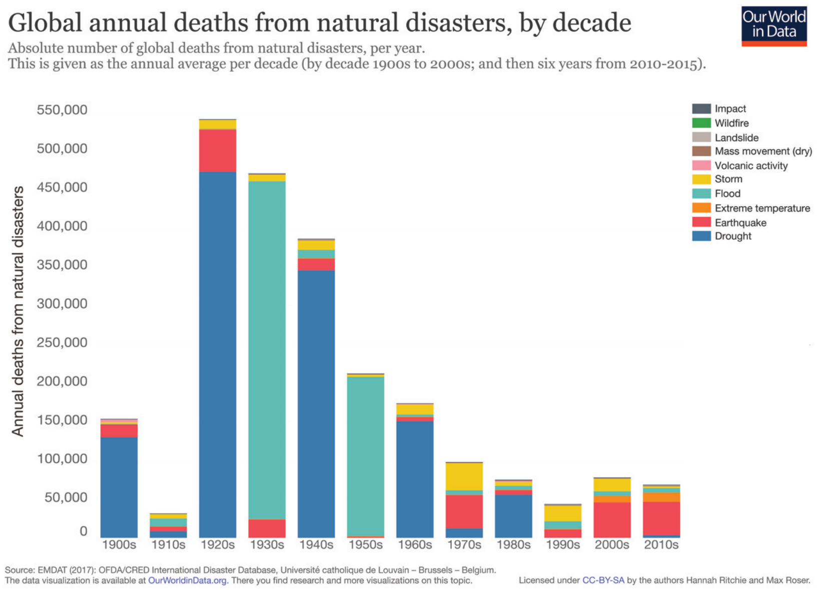


Figure 1.3: *Growth of Urban Population in World Cities [10]*



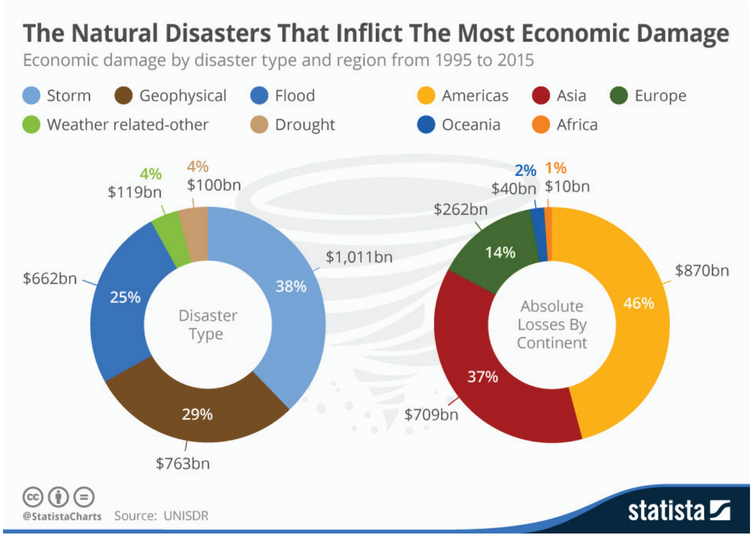
Global annual deaths from natural disasters, by decade

Absolute number of global deaths from natural disasters, per year.
This is given as the annual average per decade (by decade 1900s to 2000s; and then six years from 2010-2015).

Source: EMDAT (2017): OFDA/CRED International Disaster Database, Université catholique de Louvain – Brussels – Belgium.
The data visualization is available at OurWorldinData.org. There you find research and more visualizations on this topic.

Licensed under CC-BY-SA by the authors Hannah Ritchie and Max Roser.

Figure 1.4: *Global Annual Deaths by Natural Disasters per Decade [11]*



The Natural Disasters That Inflict The Most Economic Damage

Economic damage by disaster type and region from 1995 to 2015

Source: UNISDR

Figure 1.5: *Economic Damage by Natural Disasters [12]*

economic and social safety leading to more deaths. Comparing that to the 21st century, the deaths due to natural disasters contribute the most. Earthquakes and extreme temperature related events have killed more people than ever. This is due to the dense and in many cases unstructured population constructs in the urban areas which catapult the death numbers per unit area in cities [18]. These are either immediate effects of the disasters or after effects of disasters like epidemics.

Adding on, figure 1.5 similarly shows the economic losses due to the disasters. As seen, these disasters have always immediate and post impacts [19]. These disasters will continue to grow in the coming years attributed to *Global Warming and Climate Change*. Maybe such events are not directly visible to us who are very much safe and secure for now, but they will slowly show impacts on us. Large population migrations are slowly and in hidden crescents happening already in many African and Asian countries [20]. We will experience greater climatic variability with depleting fresh water levels and increasing rates of drought in coming decades.

As cities grow and people living in close proximity splurges, the chances of them being direct addressees of disaster impacts also increases [21]. Similarly, the economic losses also exponentially compound due to these dense networks of cities. A very recent event has been COVID-19, where due to close contacts in city environments and effects of globalization has led to situation of human and economic losses in forms not experienced before [22].

While cities ensure the securities to its populations, the underlying population inflows are a waiting time-bomb which can explode anytime [23]. Social disorders, public unrest, lack of resources to feed and sustain huge human concentrations will be the side-effects of urbanisation. According to the European Union (EU) urbanisation will grow upto 83.7 % by 2050 which would put severe constraints on natural resources leading to further environmental degradation [24]. People will have to live in closer bounded areas with more vertical accommodations rather than horizontal. Urban areas will get more congested with urban mobility restricted, increased social inequalities, and segregation and depleting heath of citizens. These indicators raise an alarm for the future of humans in the urban areas.

The scale of effects of man-made disasters also compounds in densely populated environments. Nuclear fallouts such as the Fukushima Daiichi nuclear disaster is a prime example of a compounded disaster. An earthquake caused a Tsunami which caused the widespread destruction in Fukushima. Following that the nuclear power plant meltdown added to the woes. This fallout not only had local implications but large scale and long term world wide effects such as radiation leaking into the oceans [25]. The German city of Aachen close to the Tihange nuclear plant in Belgium started distributing Iodine tablets fearing nuclear fallout in 2017 [26]. Industrial disasters end up killing and maiming large populations at an instant for which populations are not often ready [27].

The inferences based on the discussion presented are the following:

- *What can we do to make our cities safer?*
- *How to provide sustainability to future populations?*
- *How can we prepare to prevent and recover from disasters?*
- *How industrialization and technological achievements can be used to aid HADR operations?*

There have been multiple progresses in this regard. As discussed in Section 1, the concept of *Smart Cities* aims for this *inclusive and sustainable growth while providing safety and security for its citizens* [28]. HADR directives and protocols are instrumental to every city and municipality in some degree [29]. Ensuring *Public Safety and Security* through organisations such as police, firefighters, military etc. have become part of the agenda through policies tailored for HADR ops and the economic resources made available for it. Medical services from both government and non-government organisations (NGOs) are constantly updated and tested out to remain prepared for such exigencies [30]. HADR agencies through governments, businesses and civil societies plan for and try to reduce the impact and aftermath of disasters. HADR capabilities of agencies allow them to react during and after a disaster to provide relief and enable an environment for rehabilitation to the affected.

Further, the concept of IoT as discussed has become an integral concept in Smart City and industrial deployment through the integrated ICT constructs. Thus, establishing this *Interoperability* is extremely important for the HADR and ICT context for provide fast and effective relief to the citizens. Agencies have their own capabilities built around their organisational construct and often lack all the resources needed in such crunch times. So, they need to *talk and exchange information*, and *complement each others' capabilities.* Their digitization and thus their ICT capabilities need to interface to each other. The following sections detail the scope and the questions related to interoperability for HADR agencies.

1.2 Scope

The discussion of the intended research background and motivation shows the nature and importance of establishing interoperability for future HADR operations. Most of the research done in this regard and discussed in this thesis are a result of hands-on experience with operational systems, methods and strategies used for HADR operations. In particular, working with multi-national interoperability mechanisms within the scope of following:

- NATO IST-147 Working Group for Military Applications of IoT
- NATO IST-176 Working Group for Federated Interoperability of Command and Control (C2) Systems
- German Red Cross
- German Armed Forces
- IEEE IoT Consortium for Smart Cities Working Group
- IEEE Working Group: Standard for Smart City Component Systems Discovery and Semantic Exchange of Objectives

HADR agencies encompass a whole lot of governmental and NGOs with every organisation having its processes and deployment methods. In addition, many of these organisations do not let information related to their ICT systems and operational protocols be public. This is due to the safety and security concerns of their organisational protocols [31, 32].

The observation with regards to the operational systems and working processes clearly indicate stovepiped systems and organisational processes widespread across nations. Although, there has been a lot of effort to converge such systems by applying standardization methods, such convergence takes a long time. Even if they are interfaced using some standards, in the background, still there are existing silos which are very difficult to bridge [33]. So, a *"single solution"* that solves all interoperability issues is practically *"just not possible"* [34, 35]. Partly, the reason for this is the jungle of multiple components involved with ICT systems and economics involved within the organisations. Using all standardized hardware, software, organisational working processes, information exchange mechanisms etc. where the overall systems are *"plug-and-play"* systems where every organisation comes and joins to interact, is still a far way ahead.

The next section presents the research methods used during the thesis development. Based on the analysis and implementation methodologies, various interoperability PoCs were tested in lab as well as field environments. As an end result, this thesis tries to provide a general methodology and research scenario for interoperability between accessible ICT systems while working with the mentioned organisations. But at the same time, the deployments and PoCs presented are based on state-of-the-art operational systems, which if intended by the HADR agencies can be adopted and reused.

1.3 Method of the thesis

Based on the background discussion and scope of the research for the dissertation, methods for conducting of the research need to be identified. This is needed in order to formulate and lay down the waypoints based on which the research follows on. As mentioned in the thesis structure, the thesis follows the IMRAD (Introduction, Methods, Results, and Discussion) structure for presenting the thesis [1]. Thus all the publications, hypothesis and inferences presented in the dissertation follow this structure.

Further on, the primary method used for thesis derivatives are based on scientific research methods underlined in [36], [37] and [38]. The methods infer the Computing Research Methods (CRM) in engineering and ICT development disciplines to facilitate collaborative exploration of the research content. It covers the *Epistemological* and *Ontological* orientations of research philosophies [39] which revolves around knowledge and how to reach it. It might even be inferred as the *"ontology of knowledge"*. It tries to present what knowledge is possible and what is not, its scope and legitimacy.

The nature and kind of research involved in the dissertation requires one to aware of the *"existing reality"* since disasters and human lives are a reality. This domain of research needs mechanisms to avoid loss of human lives and thus needs to be closer to reality. It requires following the Ontological approach which lets sticking close to real-world functions [40]. On the other hand, considering the futuristic nature of evolving ICT systems and the capabilities that can be exploited to assist human civilization, requires to follow the Epistemological approach [41]. Research for HADR operations is an interdisciplinary research domain combining topics and components from computer science such as communications, software engineering, human factors, sociological, security and privacy etc. Investigations thus involve using a mixture of various methods to drill into the respective phenomenon. The combination of methods is then used to zero-on results, so resulting in a clearer picture of a phenomenon.

Below is the brief description of the methods used:

1. The scientific method: It involves observation of problem use-case, proposing a viable solution or theory, analyzing and validating proposed solution.
2. The engineering method: It is a more objective or practical solution based approach which includes observing existing solutions, proposing and building better solutions, and finally measuring and analyzing the solutions engineered.

These further incorporate sub-methods such as:

1. Action Research (AR): It allows for collaborative research with multiple inside and outside the organisation/community scope. It involves proposing theories within the practical domain and testing out the theories using experiments [42].

2. Descriptive/Exploratory Survey (ES) : It allows for discovery of ideas and insights defining underlying issues, areas for potential growth, multiple courses of action, and prioritizing areas [43].

3. Case Study (CS): It involves taking up a problem case and performing in-depth, and detailed examination of a particular case. It takes up a real-time phenomenon within its naturally occurring context, with the goal that context will provide a solution to the problem case [44].

4. Concept Implementation/Proof of Concept (PoC): It is is concerned with the users or the direct benefactors of research, developing something for the research context which is directly usable and not just for knowledge production [45]. It tries to understand and work within real world conditions or context and provide solutions through implementations for these real-world solutions.

5. Field Experiment (FE): it involves studies using experimental design that occur in a natural settings and are applicable in real-time, not just in ideal laboratory conditions [46]. Field experiments enable delivering actionable tools to practitioners or users which is critical for the use-cases presented in dissertation.

1.3.1 Research Questions

Based on the research methods identified in 1.3, first the problem space and hypothesized solution approaches were identified using the scientific and engineering i.e. a combination of CS, ES, AR, PoC and FE methods. Correspondingly the following research questions were formulated:

- **Question 1:** What are the different methods and architectures for ICT deployment that can be used by HADR agencies?

  - This research looked into the general literature and hands-on operational background working with military and other agencies for operational methods of deployment and utilization of technology assets for HADR ops. The inferences of these findings were used to create and test out proposed architectures as presented in

(Goal 1, G2(c), G3(c) and G4(c)). This involves deployment of the architectures with the ICT assets and providing the interoperability aspects of the architectures.

- **Question 2:** What are the hindrances faced by the HADR agencies when being deployed in real-time environments?

  - Following the methods and architectures identified in Question 1, this research looked into the overall hindrances of HADR operations. It is related specifically to ICT usage with focus on *interoperability* aspects inter- and intra-HADR agencies. It involved looking at literature as well as hands-on experimentations with ICT systems available within the scope of the thesis. The *(Goals G1(b) and G2)* propose solutions based on the hindrances identified and provide PoC implementations to show how these hindrances can be avoided.

- **Question 3:** How can concepts of IoT and Smart Cities be utilized to further the goal of HADR operations?

  - This question targeted the evolving domain of IoT and Smart Cities and finding the use-case and applicability for HADR operations. It involved exploring the hardware and software aspects as well as their security and privacy related abilities for inclusion within the existing asset infrastructures and processes of HADR agencies. The *(Goal 3 and 4)* demonstrate the working use-cases and case study application in providing better Situation Awareness (SA) to HADR agencies.

- **Question 4:** How can the end users from cities or citizens and agencies' human assets be brought into the HADR operations scenario?

  - Humans either from cities or agencies are a necessary component of any HADR operation. This question targets the issue of gaining information from human sources who work closely with the deployed ICT assets. *(Goal 4)* shows the requirements and applying the concepts developed from the requirements for working prototypes.

Figure 1.6 shows the keywords presenting the overall topics related to research questions dealt in the thesis. The keywords are grouped together based on related topics of the research goals as presented in 1.3.2. Each research goal is associated with an end deliverable, and one or more measurable and achievable outcomes.

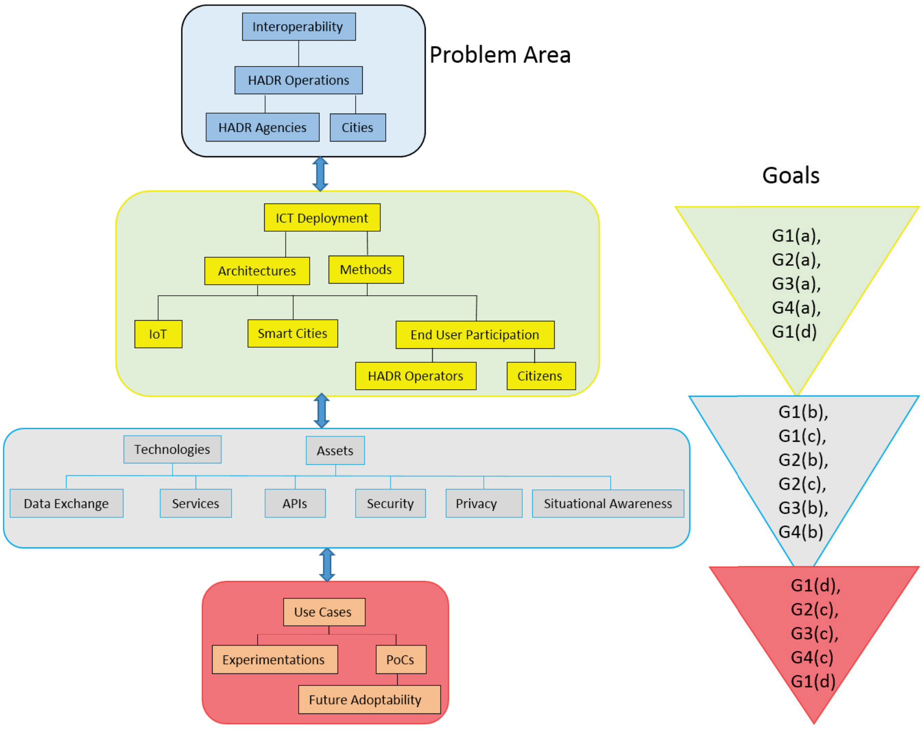


Figure 1.6: *Components for Goals based on Research Questions*

1.3.2 Goals

Based on the research questions and keywords identified, the following goals are envisioned and proposed under the scope of the dissertation:

- **Goal 1:** Explore ICT deployment architectures from various settings.

  The expected outcomes of this goal is identified as:

  – **G1 (a)**: List of deployed technologies and its corresponding components from HADR agencies and Smart Cities.
  – **G1 (b)**: Identify hierarchy and nature of interaction between the ICT components, their advantages and disadvantages.
  – **G1 (c)**: List of available services, data, APIs and accessible devices.
  – **G1 (d)**: Propose, implement and discuss an architecture for HADR operations.

- **Goal 2:** Identify and analyze the service flows and data exchange mechanisms between the ICT components and thus derive the showstoppers.

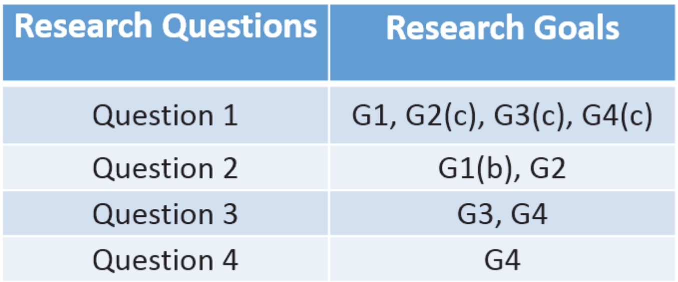
  The expected outcomes of this goal is identified as:

  – **G2 (a)**: List service interaction methods within and between the HADR agencies, their shortcomings and mitigation strategies.
  – **G2 (b)**: List service interaction methods between the HADR agencies and the cities, their shortcomings and mitigation strategies.
  – **G2 (c)**: Identify and implement services with data flows between the participating components for PoC HADR operations.

- **Goal 3:** Explore the IoT domain and its applicability to assist HADR agencies. Correspondingly identify the Smart City assets with focus on using them for real-time interaction with HADR agencies' assets.

  The expected outcomes of this goal is identified as:

  – **G3 (a)**: Identify IoT-enabled technologies w.r.t the data exchange mechanisms, existing usability and applicability, security and privacy, and service engineering.
  – **G3 (b)**: Analyse Smart City deployments, list and analyse methods to leverage Smart City services.



Research Questions	Research Goals
Question 1	G1, G2(c), G3(c), G4(c)
Question 2	G1(b), G2
Question 3	G3, G4
Question 4	G4

Table 1.1: *Mapping of Research Questions to corresponding Research Goals*

– **G3 (c)**: Implement PoC for IoT enabled services while consuming data flows from city components while ensuring interoperability with HADR agencies' ICT assets.

- **Goal 4:** Identify and analyze methods and implementations to involve end users and citizens in HADR operations.

  The expected outcomes of this goal is identified as:

  – **G3 (a)**: Identify how HADR agencies leverage their ground responders to provide SA data.
  – **G3 (b)**: Identify how Smart Cities tailor and exploit end user services to directly obtain data from them.
  – **G3 (c)**: Provide PoC implementation showing how end users' contributions can be leveraged in real-time while establishing interoperability between the interacting services.

The mapping between the research questions, the research goals and the corresponding research methods are shown in Table 1.1.

The research goals (Goal 1-4) are expected to be achieved through the scientific contributions of the thesis and are detailed in *Part I and Part II*. The details of how the research goals are addressed are discussed in Chapter 3. Table 4.1 provides metrics of the grade of achievement with respect to the research goals.

2 Contextual Background & State of Knowledge

"The Achilles' heel of emergency management is lack of interoperability. Since the beginning of the use of radio communications by police and fire and other first responders, hundreds of lives and untold dollars in damage to property can be attributed to slow responses because of communications problems"

- *Mark Hammond, Deputy Director of Monroe*
County's Department of Homeland Security
and Emergency Management

Chapter 1 presented the underlying problem scenarios and the associated research questions that are investigated in this thesis. The core of the thesis lies around engineering components related to *"IoT, Smart Cities' ICT, end users and enabling their interoperability"*. Details regarding the components built around HADR operations with focus on interoperability is described in this chapter.

2.1 IoT

IoT has its roots dating back to 1982, when a Coca-Cola vending machine at Carnegie Mellon University was modified to be connected to the Internet. It became the first Internet-connected appliance which could report its inventory and whether newly loaded drinks were cold or not [47]. Further down the line, Mark Weiser in 1991 presented a paper on ubiquitous computing: "The Computer of the 21st Century" [48]. He discussed the future possibility of ubiquitous devices owned as personal computers by people of very small size scales. He predicted architectural and technological trends to grow in near future to support this idea of personal ubiquitous computing. Academic venues such as UbiComp and PerCom presented the initial vision, challenges, possible usage scenarios and technological building blocks of the IoT [49]. In 1999, the term IoT was first documented by Kevin Ashton where he used the term to describe a system connected to the Internet via a ubiquitous network of data sensors [50].

What it basically infers is that, IoT presents a concept for universal ubiquitous computing where physical objects such as hardware platforms, sensors, actuators etc. are connected via some network, more specifically the Internet. Although, this definition presented the concept or role of IoT in its inception. In the early stages, the perception of IoT was limited to prototypes and limited specialized applications. The industry was not accepting it as a core of its deployment strategies. They were thought to be unreliable experimental devices which had limited performance and usability. But then came the Internet revolution with World Wide Web (WWW) becoming a use for everyday and everybody, and correspondingly the mobile Internet. Everyday homes and users had access to Internet which meant they could reach out to any resource, be it a person or a technology asset connected over the Internet [51]. Kevin Ashton in 2009 wrote in the RFID Journal [52]: *"The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so."*

In today's scenario, IoT means much more than just physical devices connected to the Internet. IoT has turned out to be a disruptive technology impacting all domains of technology as well as applications. One of the primary reasons for this, is the rise of Commercial-of-the-Shelf (COTS) low-cost embedded computers able to perform at fraction of the costs as compared to legacy specialized micro-computers. Along with it, the ecosystem for the associated platform additions such as Graphical Processing Units (GPUs), sensors, actuators, network technologies etc. have enabled the access of these IoT devices by private individuals as well industry [5, 53].

In 2015, Center for Strategic and International Studies (CSIS) presented a report envisioning and showcasing the various domains and applications of IoT for the foreseeable future [54]. Figure 2.1 shows the various categories of domains, their associated users, enablers for the domains, possible devices involved, the resulting applications and infrastructures needed.

As shown in figure 2.1, the physical aspect of devices does still form the core of IoT providing low-cost computing with other advantages such as [55]:

1. Low power consumption owing to their embedded and scaled down design as compared to traditional computing devices used.

2. Ability to be powered on and run for long cycles using minimal battery power or

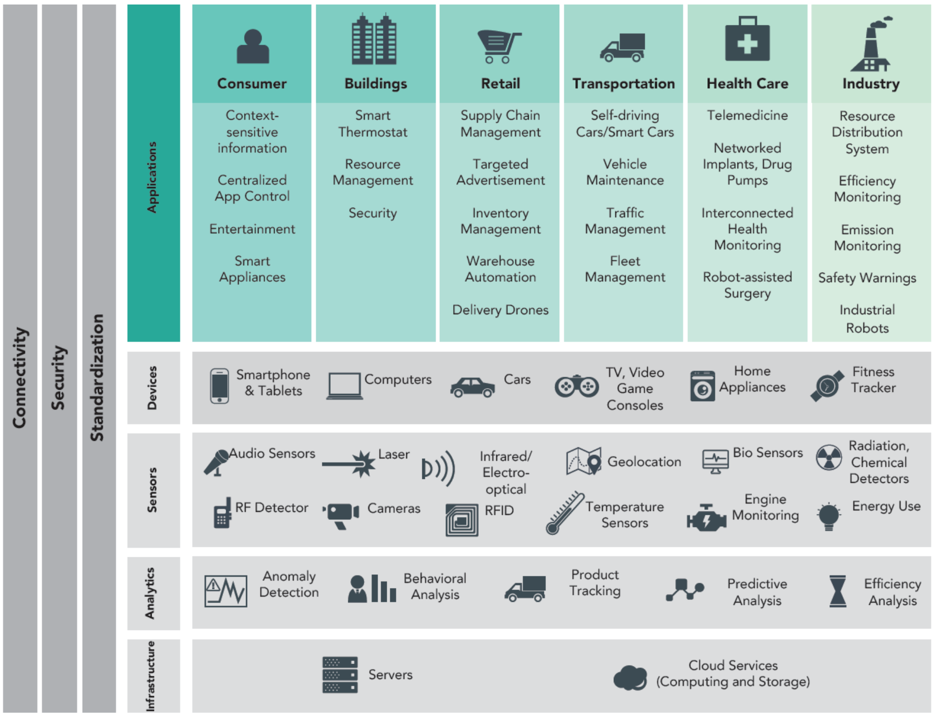


Figure 2.1: *Envisoned Domains and Applications for IoT [54]*

more innovative power sources such as solar panels, piezoelectric transducers etc.

3. Platform boards able to provide Input/Output (I/O) interfaces to integrate many other add-ons such as sensors, actuators, radio antennas etc.

4. Ability to be left unattended on the field of operations with Wireless Sensor Network (WSN) configurations for self management, recovery, fault-tolerance and interfacing external systems.

As shown in figure 2.1, traditional physical IoT devices such as the *Sensor* layer has diversified to include more potential devices such as engine monitoring and management systems in cars, radiation and chemical detection sensors, sensors for detecting audio inputs, laser scanners etc. But apart from the traditional physical IoT devices, there are other aspects for ICT that have developed. Concepts such as Smart Phones, Smart Homes, Smart Watches, connected vehicles, Smart Robots etc. have added a new dimension of application and deployment for IoT technologies. These "Smart devices" use the embedded sensors such as a Smart Home system using a temperature sensor for monitoring ambient home temperature.

As a result, new form of IoT devices have penetrated into everyday people's lives and have enabled for a "Smarter Society" supported by digitization and connectivity. IoT is no longer limited to laboratory and experimental environments but has been applied to commercial and large scale implementations. Concepts such as Industry 4.0 has incorporated IoT as an integral component for future digitization and automation of the traditional analog machines and has been one of the key pushers for such innovation [56]. Information Technology (IT) is being merged with Operational Technology (OT) systems to create a seamless ICT layer opaque to changes and upgrades to underlying components.

Due to the massive amount of data generated by these IoT devices, analysis and action based on data has also becomes more complex. Analytics based on IoT device inputs such as anomaly detection based on sensor readings, tracking and locating supply chain inventories, analysis of Smart Home user behavior has gained more inroads. There is a huge need for on-demand computing services where applications, storage and processing power can be readily accessed since all capabilities are not available at the source. *Cloud computing* is such a concept in modern ICT infrastructure set-up which provides these resources with minimal to no user intervention. It provides an abstraction to end-users needing services related to data storage, servers, networking, software etc. which the users does not house themselves. Users access these services or functionalities with remote access to central cloud hosting them [57]. As a result, we see today cloud technologies being used on every layer of Enterprise Architecture (EA) and Enterprise Integration (EI) with support for existing or predicted inflow of IoT data. Just creation of data at the device end is no more the goal of IoT-computing but to make sense of the data is what is driving the trend today. Data Science tracks in industry and academia are getting pushed for data management, visualisation and prediction. Cloud computing has now diverted from being centralised in nature to being distributed to the edge [58]. Edge computing as we know of it today, caters to this "as close to the source" analysis of data and dissemination of analytics rather than pushing all the data to a centralised cloud [59]. Domains in supply chain, manufacturing, retail, healthcare are using IoT enabled operations for predicting trends and events, adding value to the legacy services. IoT has become more like "Smart Objects" which is enabling "Smart Operations" aided by advances in automation and Artificial Intelligence (AI) technologies. IoT terminology has taken up many forms due to advances in its applications and characteristics such as Internet of Medical Things (IoMT), Industrial IoT (IIoT), Internet of Battlefield Things (IoBT), Ocean of Things etc. All of these new advancements are further supported by efforts in standardisation for IoT technologies such as standards for connectivity and data exchange, security and privacy, infrastructure set-up etc. [60]

All of these standardisation measures come with their goals and limitations w.r.t Quality of Service (QoS) and Quality of Information (QoI) for IoT devices. Different applications have different service requirements related to performance, delay and latency, reliability, scalability, safety and security [61]. Especially for IoT devices which are deployed in many critical applications, such demands dictate how and where these IoT technologies can be used. Similarly, QoI requirements decide the timeliness, accuracy, appropriateness and completeness of information. The trust level of an information delivered from an IoT device device decides how and where it can be put to use [62]. For example, in the healthcare domain, a patient's stats need to be delivered reliably and with lowest delay. At the same time, it needs to be ensured that the quality and preciseness of the data is maintained since a patient's life depends on it. So, a standard appropriate to the health application use-case is needed which can guarantee such QoS and QoI requirements.

IoT technologies, thus are maturing to support and innovate the IoT ecosystem and the range of new application requirements. The following sub-sections (2.1.1, 2.1.2 and 2.1.3) describe some of these aspects.

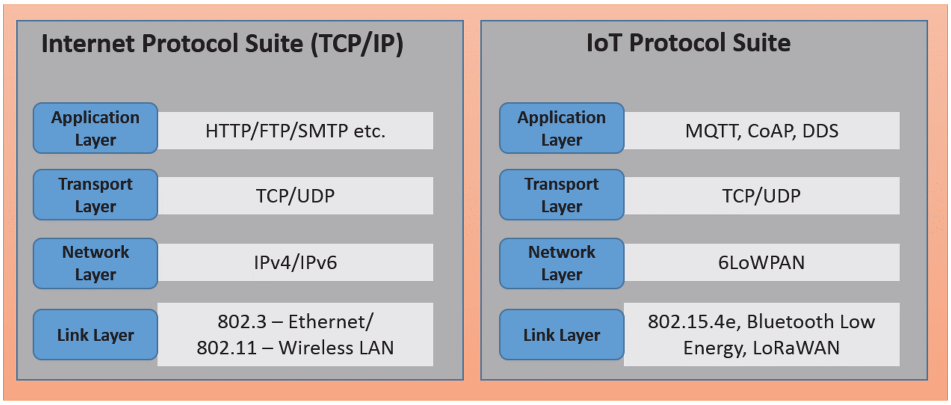
2.1.1 Protocols

IoT devices come with their special needs. While they offer compact, flexible, reliable and low power consumption computing, these requirements cause issues with the traditional communication and data exchange protocols.

As mentioned earlier, the physical device layer concept of IoT started initially with WSNs and mesh networks with focus on Machine-to-Machine (M2M) communication. Under this concept, isolated islands of IoT devices connected explicitly to each other provided the use case and requirements for developing IoT specific protocols. But with time, the application areas for IoT diversified leading to special requirements for IoT protocols. Some of these requirements are [63]:

1. Moving to decentralized from centralized deployments.
2. Low power consumption of the physical devices means that the devices have to process lesser data and induce lower overheads while communicating.
3. Minimal delay between message reception and acknowledgement.
4. Ability to handle lost and delayed packets in transmission.
5. Support for routing over wireless and wired connections.
6. Support for asynchronous communication.
7. Support for existing protocols such as Ethernet, Hypertext Transfer Protocol (HTTP), HTTP Secured (HTTPs), Transmission Control Protocol (TCP) and the Internet Protocol (IP), User Datagram Protocol (UDP) etc.
8. Ability to communicate using existing radio protocols such as WiFi, Cellular (2G, 3G, 4G) networks, Bluetooth, Infrared, Near Field Communication (NFC) etc.
9. Support for data exchange patterns such as request/response, publish/subscribe etc.
10. Support for tiny Microcontrollers (MCUs) to high performance systems.
11. Support for network and data security mechanisms such as encryption, authentication and authorization, access control, Public Key Infrastructure (PKI), Cryptographic security protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) etc.

Based on these requirements, either new IoT protocols were conceived or else, changes were made to the existing protocols to make them suitable for IoT applications [63]. Different standards to meet IoT's needs are offered by standardisation organisations such the



Internet Protocol Suite (TCP/IP)

Application Layer	HTTP/FTP/SMTP etc.
Transport Layer	TCP/UDP
Network Layer	IPv4/IPv6
Link Layer	802.3 – Ethernet/ 802.11 – Wireless LAN

IoT Protocol Suite

Application Layer	MQTT, CoAP, DDS
Transport Layer	TCP/UDP
Network Layer	6LoWPAN
Link Layer	802.15.4e, Bluetooth Low Energy, LoRaWAN

Figure 2.2: *Mapping of IP to IoT Protocols*

Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), and the International Telecommunication Union (ITU). Figure 2.2 shows some of these popularly used IoT protocols w.r.t to the existing TCP/IP protocol suite. Most of the IoT devices support the full range of TCP/IP suite apart from the specialized use of IoT specific protocols. Below is a brief description for some of these IoT protocols relevant to the context of the thesis work:

1. Application Layer Protocols:

   - Message Queuing Telemetry Transport (MQTT) is a lightweight publish/subscribe messaging protocol having a small code footprint and requiring low network bandwidth [64]. It uses either a broker based mechanism or a client/server mechanism to facilitate exchanging messages between clients (publishers and subscribers). Messages are labelled and organised by topics to which clients publish and subscribe to. It can run using both TCP/IP and UDP protocols.
   - Constrained Application Protocol (CoAP) is a client-server document transfer protocol like HTTP supporting both request-response and publish-subscribe mechanisms for multicast, low overhead communications [65]. CoAP can run on most devices that support UDP and supports UDP security features to protect information.
   - Advanced Message Queuing Protocol (AMQP) is a TCP based publish-subscribe message exchange protocol [66]. It uses a broker in the middle for relying in-

formation between the clients. But it is not is not reliable for lower bandwidths and does not support discovery mechanisms.

- Data Distribution Service (DDS) publish-subscribe data-centric middleware protocol [67]. It uses topics to exchange information between the clients but with no broker or mediator in between. All data rests on wire supported by multiple Quality-of-Service (QoS) profiles over TCP/IP and UDP.

2. Network Layer Protocols:

    - 6 Low Power Wireless Personal Area Network (6LoWPAN) is a low-power radio communication standard for devices that support IEEE 802.15.4 radios [68]. Using encapsulation and header compression mechanisms, IPV6 packets can be efficiently sent in small IEEE 802.15.4 frames. It is highly interoperable with communication platforms using Ethernet, WiFi, sub 1 GHz Industrial, Scientific, and Medical (ISM) radio channels, Bluetooth Smart etc. making it operate independently over the underlying physical layer.

3. Link Layer Protocols:

    - 802.15.4 is a IEEE radio technology operating on unlicensed, international frequency band supporting low data rates, low complexity and low power consumption [69]. It belongs to the class of Low-rate Wireless Personal Area Networks (LR-WPANs) and forms the basis for LoRaWAN. It is used for applications where remote, unattended sensors need to operate on battery power, possibly for years.
    - Bluetooth Low Energy is a derivation from traditional Bluetooth radio technology enabling low power consumption Personal Area Networks (PAN) while maintaining similar range to traditional Bluetooth [70]. Bluetooth mesh profiles use this radio technology to communicate with other Bluetooth Low Energy devices.
    - Long Range Wide Area Network (LoRaWAN): It is a radio technology that uses the licence-free ISM sub-GHz bands [71]. It enables long-range but with low data rate transmission using the spread spectrum modulation techniques derived from Chirp Spread Spectrum (CSS) technology [72]. Communication

features include bi-directional communication, end-to-end security, mobility and localization services.

These protocols at different layers of the existing IP stack enable integrators and service providers to exploit the “physical IoT world” of devices and marry them to the existing ICT domain. Backward compatibility and ability of the IoT protocols to co-exist with existing IP protocols provide the flexibility to use appropriate IoT protocols for required business domains. Especially, provided the fact that most of these protocols have been built over the existing IP protocols such as IPV6, enables standardisation agencies to leverage the advantages of the existing stack and use them further with co-existence of the new IoT protocols.

The main challenge with such a great variety of IoT protocols is: *“which protocol is the best fit for the application scenarios”*. The answer to such a question requires investigation of the protocols for their properties such as performance, reliability, bandwidth consumption, range etc. for the individual layer of application. The thesis can provided an insight into which IoT protocols are considered for HADR applications and how to federate between them.

The following subsection 2.1.2 further describes the architectural concepts which try to leverage the potential of IoT technologies.

2.1.2 Architectures

In order to support this new dimension of IoT devices, corresponding architectures were built to incorporate the IoT domain into the existing ICT domain. It meant adding more abstraction and middleware layers to interface the existing backend and Internet-enabled technologies. They incorporate the adaption to new characteristics, requirements, and constraints from stakeholders and applications involving the IoT ecosystem [73, 74]. It can be co-related to the protocol suite shown in figure 2.2 where different protocols provide different levels of functionality catering to the need of the individual applications. Apart from the protocols, the application constructs for the IoT domain is also different such as:

1. Use of IoT protocol specific APIs.

2. Use of middleware technologies to interface the legacy applications and technologies.

3. Adjusting business models and corresponding QoS and QoI expectations.

4. Adapting to the security, privacy and access control issues that come with use of IoT devices and their constraints of processing power and unreliable connectivity.

5. Providing service abstraction layers through Service-Oriented Architecture (SOA) approaches [75]. SOA provides service descriptions or meta-data with which service consumers and service providers consume or provide the service. These loosely coupled, self-contained and self-descriptive services act like black boxes to end users which the users should not be concerned about. It makes the domain accessibility through APIs more flexible to the end users since the end users should not be bothered about the end devices but instead should be ingesting analysed and required data.

6. Enabling distributed data management to address the needs of application-specific models.

7. Taking computing to the edge i.e. remote and close to the end device computing instead of just using centralised computing strategies such as the ones used for traditional cloud computing.

8. Providing a layered approach for IoT data and physical device access through the abstraction services.

9. Incorporating interoperability solutions as a core approach to make the service end points extensible and future-proof.

10. Emphasis on using open standards rather than using proprietary standards since the IoT technologies are still maturing and there is still along way ahead for stable solutions to be put in place.

11. Network management approaches such as Software-defined Networking (SDN) to separate the network control plane from the forwarding plane. Such approaches enable dynamic, automated provisioning of network configuration to improve network performance and monitoring [76].

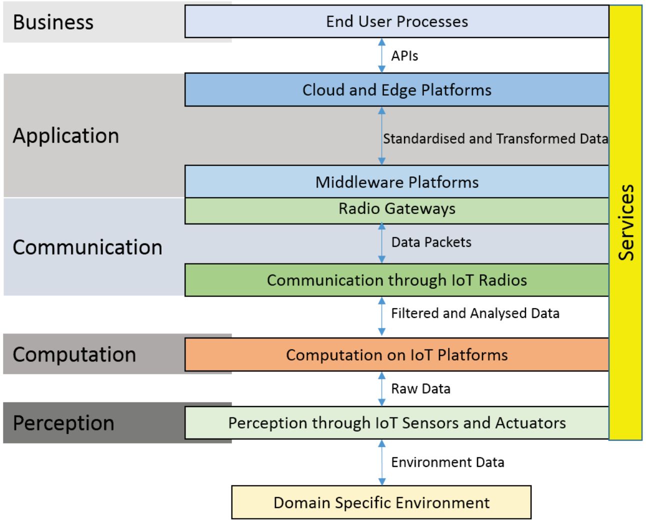

Business
End User Processes
APIs
Application
Cloud and Edge Platforms
Standardised and Transformed Data
Middleware Platforms
Radio Gateways
Communication
Data Packets
Communication through IoT Radios
Filtered and Analysed Data
Computation
Computation on IoT Platforms
Raw Data
Perception
Perception through IoT Sensors and Actuators
Environment Data
Domain Specific Environment
Services

Figure 2.3: *Basic Representation of IoT Architecture Concepts [77, 78]*

Figure 2.3 shows the basic representation of architectural concepts for IoT deployment. Its components are:

1. **Perception**: This is the lowest layer of the hierarchy where all the sensing and actuation end of IoT resides interacting with the domain specific environment. It creates the raw data based on its sensing and control feedback.

2. **Computation**: This represents the computation end where all the IoT platforms such as MCUs reside. These platforms either host on-board perception devices or else collect them from independent sources creating meaning of the collected raw data through filtering and analysis.

3. **Communication**: After the data is ready, it needs to be sent out using the communication layer. These radios can be on the IoT platform itself on other connected communication devices. These IoT radios then further are connected to a more stable backend network such the conventional broadband or cellular networks to connect to the Internet and push the data higher up.

4. **Application**: This layer represents the place where the consumed data is transformed for end user usage. The middleware platforms transform the data from the

IoT devices into a format that is standardised or is based on existing API functionality. The Cloud and Edge platforms then can implement various business use cases doing operations related to machine learning, predictive analysis etc. [59]

5. **Services**: Another underlying concept for any IoT architecture is the concept of exposing IoT deployment components as services [79, 80]. Concepts of SOA has been around since long and with IoT, the idea of distributed computing with "microservices" has come into fore [81]. IoT is being used "as-a-service" to magnify the cost and efficiency benefits. The concept is synonym to Cloud models such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) where each of the IoT layers can be exposed for the business models to be used as services.
6. **Business**: Business layer represents where the demand and requirements come from. To the end user, what matters is the end result what can be seen and accessed. The end user processes decide what the requirements for the a business model is and accordingly the lower layers adapt. For example, a cloud application can consume large chunks of hourly data from a electric grid. But in the end, the user might only be interested in a predictive analysis of what the next years' consumption might be. So, accordingly, based on cost, performance and other economics estimates the lower layers have to be adapted to suit into that specific business goal.

As seen from these components, the "IoT Architecture Stack" provides a range of possibilities for the IoT domain. Each layer can be used independently or in conjunction with the existing or legacy ICT domain components. "Services" being the driver of ICT deployments, enables leveraging such an IoT architecture for integration for any given use-case or domain. As of today, multiple such architectures from multiple standardisation organisations and companies exist, making it difficult to adopt just one for all assumed HADR use-cases. An insight into issues for using existing IoT architectures for the HADR context is provided in section 2.5. Further, subsection 2.1.3 below describes an application area where IoT is used, relevant to the HADR context.

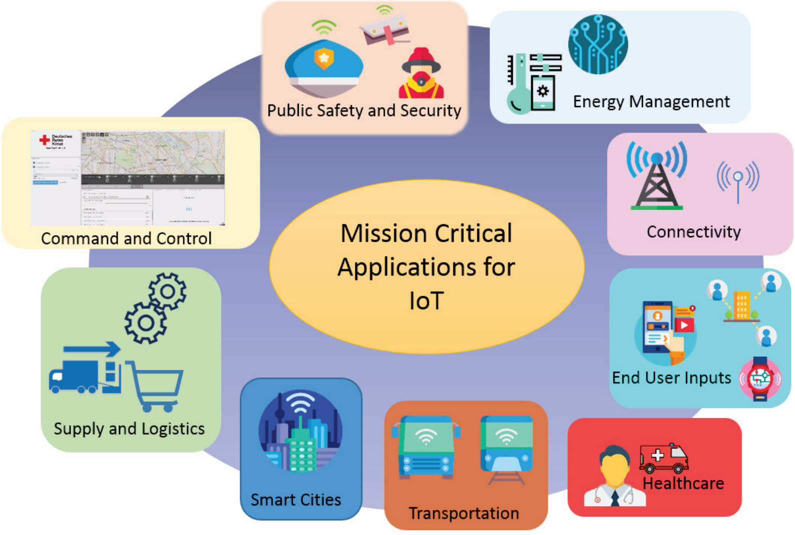


Figure 2.4: *Mission Critical Applications for IoT*

2.1.3 Applications in Critical Domains

As discussed, the growing trend of IoT lies with data-driven applications enabled by embedded automation and intelligent adaptive systems. Supported by the growing ecosystem of standardised IoT solutions, large-scale industry driven deployment has added to its reliability and proven efficacy. The result can be seen reflected in the applications which are mission critical i.e. which require a continuous and reliable functioning for a business functionality to be successful [82]. If mission-critical applications experience even a brief delay or downtime, the range of undesirable consequences are likely to be critical. A mission-critical app's failure to function may bring damages in big financial terms or else, as for the case in the thesis, loss in human lives. Programs such as IoBT from the US Army has shown the path and intent of IoT use in such mission critical applications [83]. Figure 2.4 shows the domains of interest classified for mission critical applications relevant to the context of the thesis.

One critical component of IoT application in mission critical domains is the safety and security of the applications in the corresponding domains. Mechanisms are needed to establish trust for individual assets and support resilience of participating systems especially where ICT domain can comprise interconnection to legacy systems [84]. Maintaining integrity of the data exchanges over the IoT connectivity along with ensuring trusted data and information provenance need to be supported at system inception. Any incursion of incorrect and malicious data can severely harm the continuity and effectiveness of an operation. IoT assets need to be tested, verified and validated for use corresponding to the critical domain needs which are dynamic and adversarial in nature.

In an event of emergency, such IoT-based critical applications need to function reliably. Especially when applied to domains of *Public Safety and Security*, the applications need to ensure correct SA to the HADR responders while reducing costs, ensuring security and integrity, and increasing operation efficiency. C2 systems display the overall scenario with reports collected by these applications along with the human operators. Based on these C2 SA data, the decision makers need to take the appropriate calls how to deal with the issue in hand. Actuation and operational protocols get activated based on the type of the event reported. Accordingly, correct responders are sent on site.

An example is: when a fire needs to be controlled in an area. The buildings with fire alarm sensors report fire and dangerous gas emissions which are then sent across to the C2 systems through appropriate *connectivity* mediums such as a Long Term Evolution (LTE) or a WiFi network. The report is corroborated with inputs from the cameras mounted in buildings and streets. The decision makers actuate a fire response using the C2 system, sending the police and firefighting units to the area. Following which the *healthcare* responders are also sent to assist the victims seeking medical attention. IoT devices help the workers serve affected people by engaging IoT devices to monitor vitals of the injured, offloading the workload of the health workers. If a large scale devastation has occurred then the appropriate *supply and logistics* need to be sent the area who can be tracked in real-time using the IoT Global Positioning System (GPS) sensors. *End users' inputs* are provided using users' IoT (Smart) devices such as Smartphones reporting trapped and injured people. *Transportation* services based on automated response systems evacuate and move the people to safer areas while using IoT based systems such as cameras and PANs, to track and monitor the evacuation. The grid has to then step in for *energy management* in the affected area by restoring electricity in affected areas by using IoT sensors and also diverting electricity to areas of rehabilitation.

Although the above example shows a particular scenario, it shows the potential and possible opportunities that IoT can be useful for. Some of the underlying challenges related to use of IoT in mission critical applications stems from the age and maturity of IoT technologies. IoT is still relatively new in the ICT landscape as compared to legacy technologies used for mission critical applications. Although there is a huge surge in commercial adoption, using IoT for critical applications by defence, security and HADR agencies needs quite a lot of assessment related to standardisation, performance, reliability, safety and security. So, there is still a gap for establishing trustworthiness of IoT use. But considering that IoT technologies are becoming more reliable, affordable and standardised, such mission critical applications are looking at a more inclusive adoption of IoT.

The below subsection 2.2 describes another such domain of IoT application relevant to the HADR context.

2.2 Smart Cities

In 1.1, the issue with modern population moving towards dense, packed urban areas which would create issues in the coming future was presented. Smart City initiatives intend to address this future problem by involving public and private body “partnerships” and “collaboration” through “Digital ICT platforms”. These collaborations and partnerships with all bodies involved in a city’s functioning tries to bridge the gap between the actual expectations and available amenities. This digitalisation involves connecting and improving infrastructures, both digital and analog, from all organisations alike, under a single framework for a city. The analog infrastructures refer to the existing assets and services from the city which are yet to be connected to the city’s ICT domain.

The Smart City concepts again within its domain involves concepts such as [85]:

1. **Smart Living**: Enabled by the “Smart Devices” such as Smart Homes, Smart Phones, Smart Watches, this idea tries improving lives of people. Technology interaction is the core component which combines sensing with physical action to aid behavior analysis, data analytics, security etc. One such example is home lighting solutions which monitor the lights in a house and associate that with motion detection sensors to switch on or off lights, helping to save energy.

2. **Smart Mobility**: It involves connecting and digitisation of public and private transport infrastructure for increasing energy efficiency, low-emissions, safe, comfortable and cheap mobility. Apart from that, it also includes services for car and ride sharing, walking, biking, roadside assistance etc. It envisions a future with "Zero Emissions, Zero Accidents, Zero Ownership" [86].

3. **Smart Governance**: It aims at providing transparent, cooperative and democratic governance function which is "made for the people, made by the people, and answerable to the people" [87]. It relies on interconnected smart objects and cyber-physical systems for delivering efficient and effective performance of public tasks. "E-governance" is also a term used in this regard which provides electronic access to government tools and dissemination of information.

4. **Smart Parking**: One of the major issues in urban structures is the issue of parking. People move around with their cars for flexibility and sometimes this is rather a pain due to unavailability of parking spaces in urban premises. Smart Parking uses ICT assets such as parking sensors, vehicle GPS and distributed cloud based data management to inform car owners for available parking spaces in connected parking locations. This reduces hassles for parking while saving fuel and time.

5. **Smart Energy and Smart Grid**: It basically entails the smart use and distribution of energy from and within grids, and between grids to the end users. Smart Meters at homes enable energy saving by monitoring energy utilization, providing heuristics to owners and to the energy providers helping them to plan their energy supply and utilization. Likewise, Smart Grids aim at electronic power conditioning, controlling production and distribution of electricity by using various monitoring sensors and systems at the grid level. The future electricity needs are migrating towards renewables and the Smart grids aided by the Smart Devices aims to deliver a reliable and secure electricity infrastructure.

6. **Smart Buildings**: Legacy infrastructure such as the existing buildings can either be retrofitted, or else new buildings constructed with sensors to provide building management services such as monitoring the structural health of buildings, ensuring safety of its dwellers. Centralized monitoring and command stations can provide information in real-time enabling the authorities to take appropriate action in

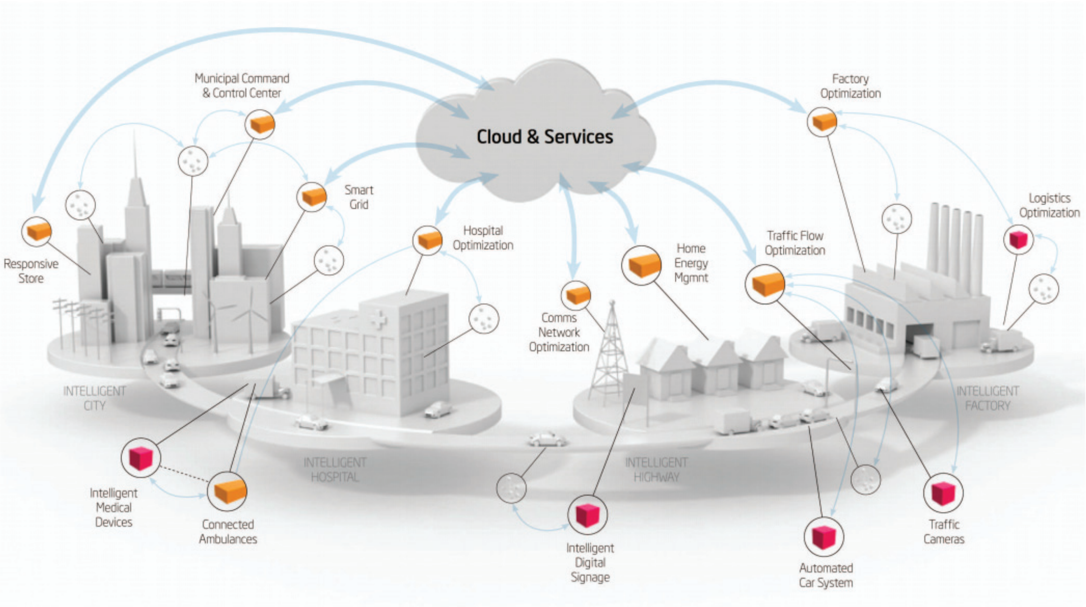


Figure 2.5: *Smart City with IoT Integration [5]*

real-time for events concerning the building. Examples include, gas and air quality sensors which monitor ambient air quality and raise alarms in case of gas leakage.

7. **Smart Manufacturing**: It means the interfacing of OT to IT systems to aid manufacturing processes with features such as high levels of adaptability for rapid design changes, flexible digitalized technical workforce training, on-demand production and distribution load changes, making production efficient and increasing recyclable asset use. As mentioned earlier, Industry 4.0 is such as measure that uses standardised and interoperable systems that can scale dynamically aided by intelligent automation, secure operations, and networked sensors.

As seen in these concepts, the role of ICT is huge. One of the major contributors and enablers of these ICT usage has been application of IoT. Figure 2.5 shows this scenario where a city enabled by IoT technologies embraces ICT into its everyday operations and needs.

A big part of this IoT enabled ICT framework involves intelligent networks of connected smart objects that transmit data using IoT radio technologies to and from, the edge and the cloud. These cloud and edge applications receive, analyze, manage and predict in real-time to help government, private industries, and citizens make better decisions and improve quality of the city operations. The enabling technologies and concepts for Smart City ICT deployments is further discussed in 2.2.1.

2.2.1 Aspects of Smart City ICT Deployment

A Smart City ICT deployment, in real world cases as seen till now such as in Singapore, pilot projects within the Horizon2020 Program of the European Union showcase how Smart City ICT potential can be leveraged [88, 89]. The approaches in this regards can of two types:

1. Form rules, regulations, use-cases and build the ICT deployment around it, as seen in Singapore. There was an agreement formed between the various civic agencies based on certain guidelines and initially physically integrated ICT platform was avoided. Integrated assets were the end physical devices or a data consumption and sharing platform which the potential end users could access. Although this process is slow, it makes sure that the resulting ICT deployment is usable and scalable considering the city's current and future needs.

2. Another option is the other way round as seen in EU projects such as in Satander, Spain [90], where one of the very first Smart City projects was executed. Under EU H2020 projects, various use cases in various domains were identified such as healthcare, transport, living etc. ICT deployments were tested as pilots for the individual use-cases. The expectation was that it would lead to future waypoints guiding these ICT deployments based on use-cases and domains. Although, this potential was and is exploited in many cities across Europe, there have been issues within it [91, 92]. This has lead to multiple silos where each use-case, domain and city has its own way of operating the Smart City concept. There have been multiple architectures, data models, technology formulations, deployment constraints, data silos introduced by the various organisations operating within the Smart City landscape. As a result, there is a lack of integrated discovery option for Smart City ICT resources such as data, physical assets, critical information etc. Along with it, rising security

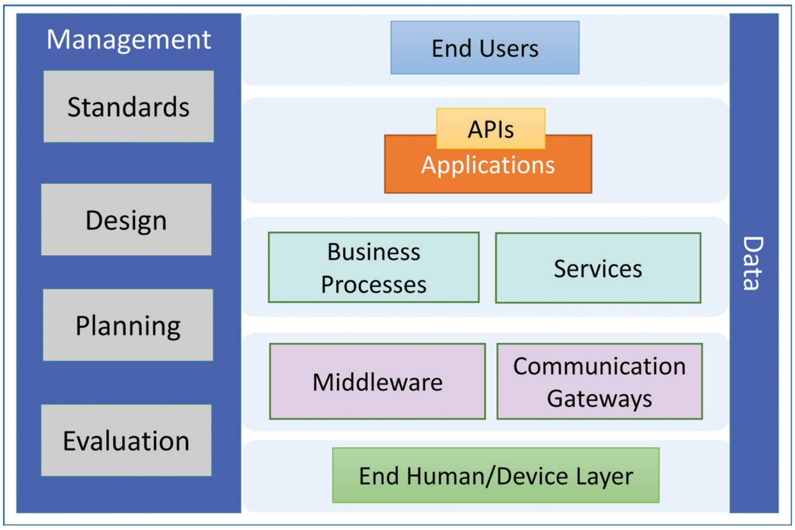


Figure 2.6: *Smart City ICT Architecture Components*

and privacy issues is a big concern. But on the other hand, due to these cumulative efforts, there has been a big push from industry and the economic perspectives of future smart cities has strengthened.

There are various architectural concepts related to the organisation and therefore the way technology is used in cities. Figure 2.6 shows a generic representation of the components of a Smart City ICT Architecture [93, 94, 95]:

1. **Management**: Management functions form the base of any Smart City ICT deployment. As discussed earlier about the examples of Singapore and Europe, first the right requirements and the corresponding action plan has to be laid out. Some of these include how to plan and design the inclusion of existing business processes and components from civic or industry bodies. **"Open standards and interoperability"** serve as the fundamental requirements to enable integration of city's existing infrastructure and new ICT usage. This entails planning and evaluation of multiple technologies and platforms available in the market, and then trying to analyse how to fit in the city's requirements to the tools and techniques available. Of course, a city might also want to go "Rambo" and design and implement an ICT deployment from scratch!!

2. **End Human/Device Layer**: As presented for IoT architecture, the end physical device layer forms the base on top of which any ICT function executes. But in contrast to just the independent devices for IoT, this layer for Smart Cities might also include humans who serve as sources of sensing, actuation and feedback for the ICT components. An example is from the hospital where the end human medical professional provides input to the ICT system through an interfacing physical device. In addition, this layer also contains existing analog physical devices such as traffic lights which are retrofitted with an interfacing communication gateway to be able to interact with the central ICT deployment.

3. **Middleware and Communication Gateways**: Interfacing the physical/human layer to the ICT system requires mapping and/or transforming the raw input received to a more standardised, understandable and consumable format that is recognised by the ICT platforms. The Middleware layer is responsible for service management, provisioning and providing interconnection to the system database. It processes information, performs ubiquitous computations, and makes decisions based on business processes. Examples such as edge or fog computing platforms consume raw data from heterogeneous data sources, analyse and filter them and finally expose the necessary data to the higher layers such as the central cloud. These edge computing platforms might also incorporate on-board multiple radio technologies such as LoRaWAN, low-energy Bluetooth to consume data from the end users transmitting using these radio technologies. Further these edge nodes can send data back directly to the end users through the same radio channels. Or else, they can use a stable backend radio link such as WiFi or wired Ethernet to send data reliably back to cloud endpoints.

4. **Business Processes and Services**: Any decision making is based on the business process dictated during the planning phase. How and what data or assets can be reported or exposed, and what corresponding processing is needed, is based on these business processes. These might include considerations such as business models i.e. economic aspects involved, security and privacy, roles and responsibilities of the involved actors. Based on these decisions, the corresponding services can be formulated to be exposed or utilized by the applications on the higher layer. Services might include concepts such as AI-based predictive decision making, automation,

machine learning, data mining, blockchain etc.

5. **Applications and APIs**: This layer contains the visible component of the whole ICT deployment what end users directly interact with. Smart Cities generally use dashboards, C2 systems and mobile information platforms for control and visualisation of all the data received from the lower layers. These applications expose the data they learn about, to the end users' platforms using APIs. Ideally Smart City services provide API dictionaries through interactive linked data services using the SOA approach. Users can access the application components and thus the data using these APIs.

6. **End Users**: These represent the humans and machines who consume the data through the applications. These in a Smart City environment include users from the government, citizens as well as private industries. The management functions decide the requirements of the end users and accordingly design the ICT functions to provide the information needed. For the scope of the thesis, the end users of these deployed ICT can be civic bodies such as the city administration, police, firefighters, city engineering and repair agencies, hospitals and medic services. Extending it further involves national organisations such as military, para-military and also the non-government organisations such as Red Cross. These agencies can consume the data from the service APIs displayed through dashboards, personalized mobile applications and C2 applications.

7. **Data**: As mentioned for IoT, data is of prime importance in the whole ICT deployment. Data is exposed through the services and the corresponding APIs. Ingestion, exchange, storage and management can be associated with all the layers of the ICT. Semantics and Ontologies of data and the related APIs decide how to collect, store and distribute the data consumed at various levels. Each level has got it its own requirement leading to a different process of handling the data exchanged at that level. Concepts such as Big Data is used to manage all the data in the ecosystem through:

   - Application Repositories to store applications.
   - Model Repositories to store city models, such as a traffic model, sensor network model etc.

- Data Repositories to store the data collected from the end points such as IoT platforms, citizens and the associated applications.

These architectural components in a Smart City ecosystem enable the various processes of a city function to come together with the goal of providing effective citizen services and governance. Although, as discussed, a Smart City provides for much more than just governance but increases end user interaction and participation in a city's functioning. Using technology for service and data provisioning, lays the ground work for future HADR operations where these individual components can be accessed through services based on regulations and user policies.

Current state of various Smart City architectures floated around the world suggest again a fractured common mandated approach to Smart City architectures. Business processes and economics decide which city adopts which architecture. Although some standardisation organisations and self-organised forums have tried to push and organise some standardised architectures, still there is a long way to go before they can converge [96, 97]. But considering the scope of HADR what the agencies are interested in is: "Services". Standardised data from the API end points are the need based on SOA approaches.

Subsection 2.3 further elaborates the underlays of HADR operations with focus on urban scenarios.

2.3 HADR Agencies' Operations

Disaster rescue and relief work is generally done by the city's civic agencies such as the police, firefighters, city engineering and repair agencies, hospitals and medic services in co-ordination with the city administration. There are procedures and protocols to be followed for the type and scale of the disaster emergency. Based on the administrative boundaries, these can be shared between municipalities, cities, states upto nations. These administrative formations can interact with each other based on their need and capacity to deliver. An example in this regard is the German emergency and disaster management system where civil defense and civil protection is the task of the 16 states in the country [98]. Further down, the municipalities and districts are responsible for the organisation of

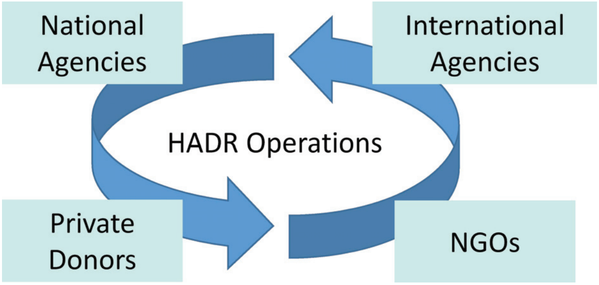


Figure 2.7: *Stakeholders in HADR Operations [99]*

disaster and rescue services. Apart from that there are multiple national government organisations such as Technisches Hilfswerk (THW/Federal Technical Support Service) and NGOs such as Deutsches Rotes Kreuz (DRK/German Red Cross) involved in such situations. The THW provides the engineering and repair services, while the DRK provides medical assistance services. These organisations employ either full-time professionals or part-time volunteers who are trained for such actions. The German constitution allows to call in the federal armed forces when needed to support the disaster relief organisations. Figure 2.7 shows these interactions of the stakeholders in HADR operations.

Some of the actions for HADR operations include [100, 101]:

1. Search and rescue of victims.
2. Evacuation and relocation of the affected population.
3. Setting up relocation and settlement centres for accommodation of the affected population.
4. Providing logistics operations for food, water, medical supplies and other essential equipment.
5. Engineering and construction work to repair/rebuild affected infrastructure.
6. Removing and sanitizing hazardous materials and dangerous infrastructure.
7. Deconflicting areas, ensuring public order and safety.
8. Setting up interactions and action items with other local/national/international organisations.

9. Initiating and organising post-disaster relocation and sustenance operations.

Based on the exigency and scale of the disaster, different levels of C2 protocols apply [102, 103]. In cases where the situation can be handled locally, the existing command centres are used with the respective operators working with the agency defined protocols. But in cases, where there is a requirement of multiple agencies working together, there is a cross-interaction between the various agency operators and the used C2 systems to gather a better SA picture and accordingly exchange information. Generally, a shared operations command post is set-up where the agency operators work together taking care of coordinated action reporting and interacting with the ground assets. A lot of the interactions for coordination and control operations are in most cases still very manual i.e. a lot of information exchange happens with manual human interactions. There is always "man-in-the-middle" operations model where a specialized operator is responsible for taking analog commands and report items for logging and disseminating the necessary action items. There is always the argument that a human operator is always more reliable or trustworthy than machines [104, 105].

A prime example of such a HADR operations deployment is the Civil-Military Co-operation (CIMIC) concept in the NATO domain [102]. This concept tries to bridge the gap between the national and international HADR agencies with militaries from the NATO nations collaborating and cooperating together to help out in case of conflicts and disasters. Further, these NATO bodies interact with the local authorities, civilian populations and other participating NGOs. Examples include the efforts during the Haiti and Nepal earthquakes, Kosovo and Chad conflicts. Traditionally, in such scenarios, the CIMIC operators interact with the civilians and local bodies on behalf of the NATO commander. Protocols for Area of Operations (AOO) are set-up after assessment of the ground situation and planning for required mission objectives. The end goal of such plan of action is to bring the AOO to a sustainable end-state from where the local bodies can take over and carry out the normal operations of the AOO.

2.3.1 Multi-agency Cooperation and Interoperability

According to Research and Development (RAND) Corporation, Interoperability is defined as:
The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together. [106]

Based on the discussion presented in 1.1 and 2.3, it can be inferred that in the coming future, the need for multi-agency HADR operations would increase in number, capacity and needs. Already many new initiatives are going around in the world to support such future actions. Protocols to enable interoperability exist at some levels, but are mainly based on manual human interventions. But as the scale of the HADR operations evolve and expand, always involving a manual human operator might not provide the required effectiveness and pace.

As the requirements for inclusion of digitisation and automating many services from the HADR agencies increase, new concepts for interoperability based on ICT usage is also coming into fore. And within this drive with increasing ICT dependence, IoT technologies are getting incorporated more towards such deployments. The NATO-147 group looked towards this idea of leveraging IoT and Smart City ICT for HADR operations. The following NATO-176 group is discovering federation mechanisms for extending the interoperability concept [107].

Federated Mission Networking (FMN) is another such initiative for ensuring interoperability and operational effectiveness of the NATO forces [108, 109]. It spans much more than just creating interoperable ICT frameworks for the allied countries. It also provides methods for creating better operational communication and training processes. The goal is that there should be common understanding for operational protocols irrespective of the domain and administrative boundaries of the allied forces. An aspect of FMN and CIMIC is the inclusion of civilian assets through the organisational end-points. These can be either human operators or else API based ICT service end-points. Further, FMN also tries to address the issue of integrating the legacy systems from the NATO domain such as existing C2 systems, analog tactical radios etc. using SOA approaches. SOA approaches are mainly based on exposing the service end points using Web Services for Network-enabled Capabilities (NEC) operations [110].

2.3.2 Smart City Safety and Disaster Recovery

To envision the deployment of Smart ICT and design HADR frameworks around it, needs attention to the interoperability aspects of the Smart City services. There have been initiatives towards it such as designing separate services for public safety, security and disaster preparedness. Examples such as Smartresilience [111], Infrastress [112] show an approach in this regard. But still there is a void in the automated service discovery and integration aspects. While open standards and open data technologies help to simplify the discovery problem, they also create issues with them w.r.t their flexibility and extensibility. Often resulting standards from many initiatives get shelved as prototypes and pilots, or else become proprietary providing limited, to no access for essential services needed during HADR operations. An example of such shelving is the platform for smart cities designed during the Sentilo project. It included a cross-platform infrastructure and data management service with which information could be shared between heterogeneous systems while integrating legacy applications. It leveraged open source components to integrate data from IoT technologies from heterogeneous device manufacturers. But since 2017, after the project timeline finished, there has been no followup or add-ons on that project.

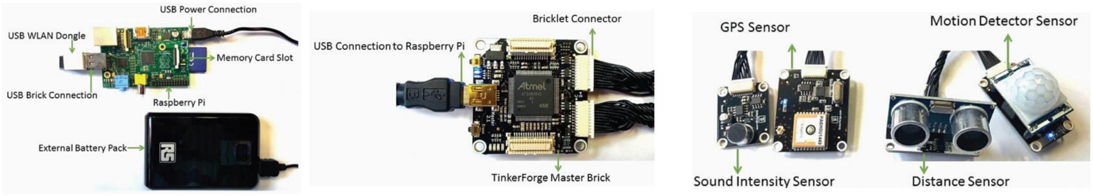
Multiple such Smart City architectures and platforms are floating around with multiple silos between the cities. Even within a city there are multiple providers of Smart City data which follow their own architectures and deployment mechanisms. Following each and every architecture and integrating those individual components of architecture is not the correct approach for disaster recovery operations. Rather what is needed is the access to those end point or Application Programming Interfaces (APIs) to be more exact. Cities or data providers might want to expose limited data based on their QoI, QoS, security and privacy, and business model considerations. In such cases, having a directory of APIs exposed and accessing those end points is the way to go ahead. This would minimise integration efforts, and overload of quantity and quality of data.

On the same lines, there are multiple Semantic and Data Ontology specifications which describe the data once they have been accessed through the APIs. Examples such as Ontologies from Microsoft Azure, Amazon Web Services (AWS), FIWARE, European Telecommunication Standards Institute (ETSI), Smart Appliances REFerence (SAREF) etc. describe their own way of describing the data accessed using their respective service layers [113]. It creates a huge issue while trying to connect to each of these services and mapping the semantics of the data to the HADR service end-point functionalities. From the IEEE point, the IEEE Smart Cities Working group [114] and IEEE P1951.1 [115] working group are trying to address these issues. It intends to propose reference frameworks and mechanisms to overcome these silos of operations.

2.4 Background Work related to HADR Operations

Work with IoT and HADR operations in Smart City environments has been going since quite some now which provided the problem areas and further research directions leading to the thesis conception. Back in 2016, we showed how cheap COTS IoT devices can be integrated into the existing functional military C2 information systems using open source standards. Figure 2.8 shows the IoT set-up used for sensing on the ground and using the sensed data to provide SA for Intelligence, Surveillance, and Reconnaissance (ISR) operations [116]. It used Representational State Transfer (REST) based web services to exchange data with the Multilateral Interoperability Programme (MIP) based C2 system [117, 118]. The raw data sensed from the sensors was mapped and transformed into MIP Information Model (MIM) data format. Figure 2.9 shows this display with the sensed and mapped MIM data. It showed that IoT devices based on open standards can be used for military ICT deployment.

In 2017 at Oulu, Finland, as part of IST-147 initiative, we demonstrated the utilization of IoT in urban military operations. The use-case set was the safe passage of a military convoy between two end-points [5]. The use-case added the dimension of adding SA data leveraged from sensors and cameras installed by the Finnish Transport Agency (FTA). The data from the publicly installed sensors and those installed by the military were fused to provide real-time SA data through the Android Tactical Assault Kit (ATAK) C2



(a) Raspberry Pi with External Battery Power (b) TinkerForge Master Brick (b) TinkerForge Bricklets (Sensors)

Figure 2.8: *Using IoT Platforms and Sensors for ISR Operations*

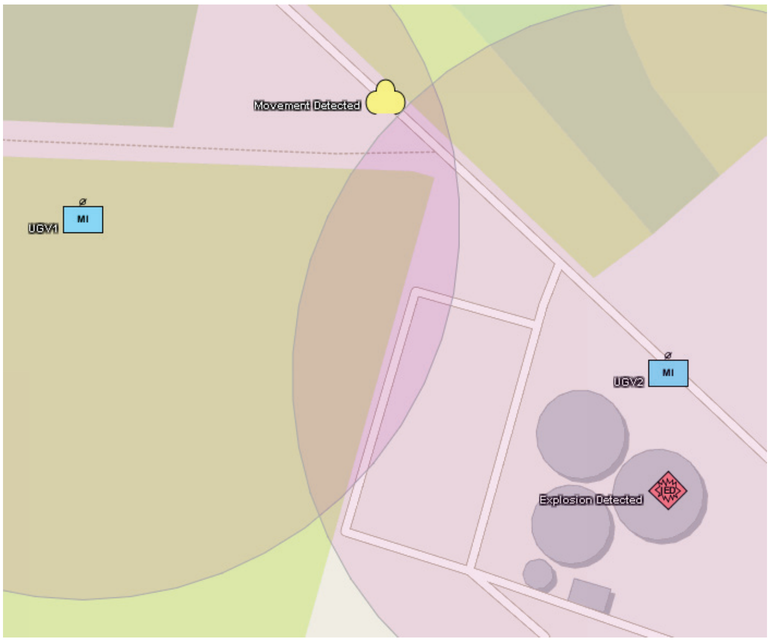


Figure 2.9: *Display of Sensed ISR data on MIP C2 System*

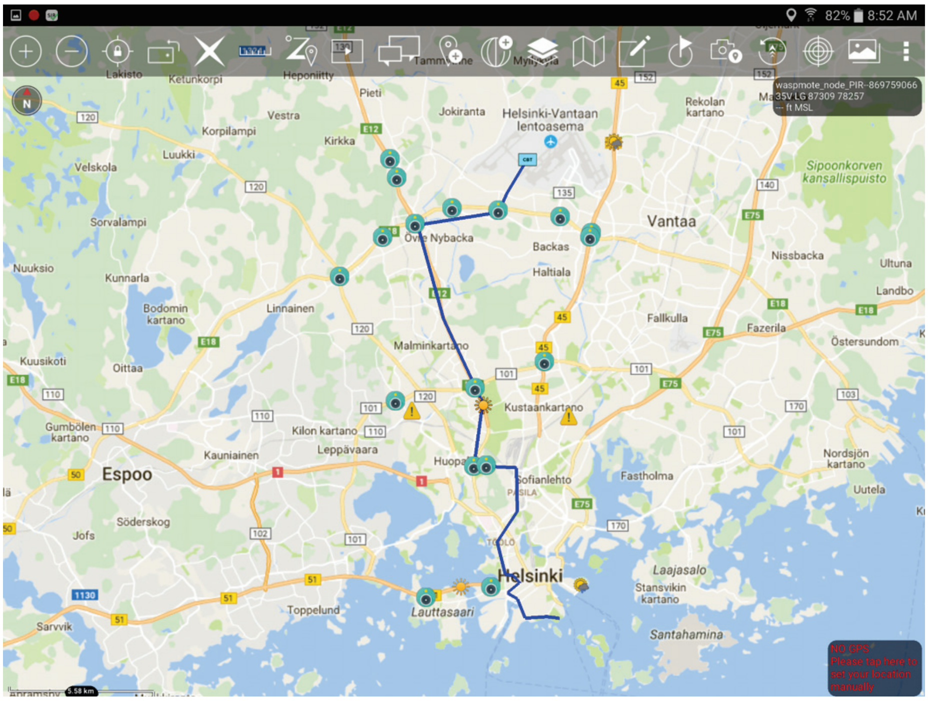


Figure 2.10: *C2 Status on ATAK*

application [119]. In addition, it demonstrated the interoperability between the military and public data exchanges. The military IoT data was described using NATO Generic Vehicle Architecture's (NGVA's) data models [120] and while from the FTA's side, OpenAPI Specification (OAS) [121] was used. Both the data were then sent using Web Service Description Language (WSDL) in Extensible Markup Language (XML) data formats [122]. It also integrated the United States Army Research Lab's (ARL) Sieve Process Forward (SPF) middleware to consume, filter, analyse and disseminate data using Value of Information (VoI) based metrics [59]. All these operational data was relayed through a mobile cloud running on the mobile Tactical Operations Center (TOC) running on one of the convoy vehicles. Figure 2.10 shows an instance of the SA displayed on the ATAK interface. It lists the cameras accessed from the FTA (as green icons) which can be triggered to access the video and the yellow icons show the alert events reported by the IoT platforms.

During the IST-147's working tenure MQTT was identified as the protocol to be used IoT data exchanges due to its lower complexity of implementation and lower transport

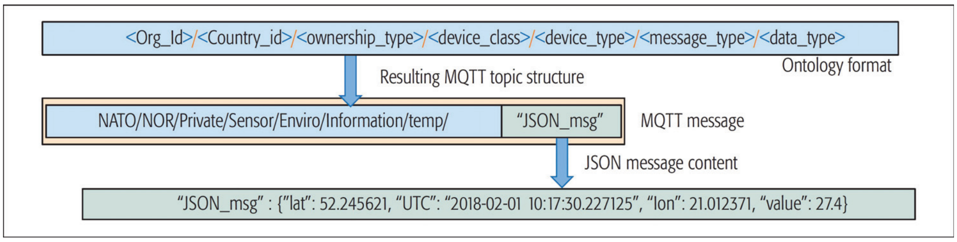
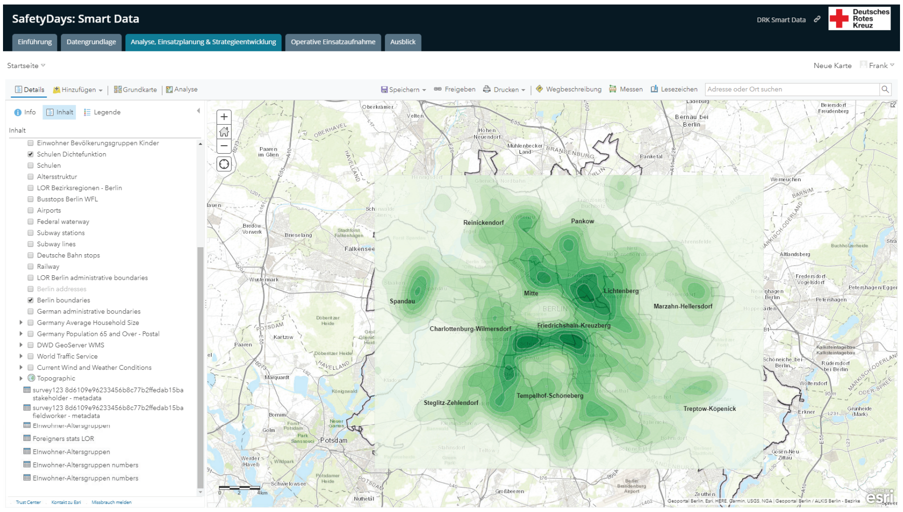

<Org_Id>/<Country_id>/<ownership_type>/<device_class>/<device_type>/<message_type>/<data_type>
Ontology format
Resulting MQTT topic structure
NATO/NOR/Private/Sensor/Enviro/Information/temp/
"JSON_msg"
MQTT message
JSON message content
"JSON_msg" : {"lat": 52.245621, "UTC": "2018-02-01 10:17:30.227125", "lon": 21.012371, "value": 27.4}

Figure 2.11: *Ontology Format for MQTT-based JSON-formatted Data Exchange*

overheads. For tactical radio networks, where bandwidth is expensive, MQTT was found to be a better choice than more complex Web-Service (WS) Notification protocol. All the data exchanged through MQTT was done using JavaScript Object Notation (JSON) which is a lightweight data-interchange format [123]. In 2018 at Warsaw, Poland, the IST-147 did a live demonstration showing multi-nation interoperability for IoT and legacy technologies [124]. After considering multiple specifications for describing IoT data such as SensorML, Base Ontology, (SAREF) ontology, IoT-O, Spitfire, IoT-lite Ontology, a simple representation for IoT capabilities was formulated for MQTT's topic based data exchange [125]. The topics were presented in JSON format to leverage its light-weight nature and REST web services were used to expose the end points accessible by the coalition partners. Figure 2.11 shows the format used along with a sample data describing a sensor.

This experimentation also demonstrated the complex data exchange while ensuring interoperability between the interacting partners. Data from the various agencies in Warsaw like the public transport agencies, data feeds from weather companies providing web service endpoints for the weather sensors, camera feeds from city administration from Points-of-Interest (PoI) etc. was consumed to show SA data. This SA data was fused with other available military-IoT SA data. Also, concepts of storing data to cloud (to AWS) and local processing on Edge Nodes using the SPF middleware were demonstrated to show the Smart City HADR ops scenario.

To showcase how NGO organisations can act during a HADR operation, in 2019 during the Safety Days event, we collaborated with the German Red Cross to demonstrate evacuation of affected population in the city of Berlin, Germany [126]. We developed both web and mobile applications accessible using REST web services over the ArcGIS frame-



Inhalt

- □ Einwohner Bevölkerungsgruppen Kinder
- ☑ Schulen Dichtefunktion
- □ Schulen
- □ Altersstruktur
- □ LOR Bezirksregionen - Berlin
- □ Busstops Berlin WFL
- □ Airports
- □ Federal waterway
- □ Subway stations
- □ Subway lines
- □ Deutsche Bahn stops
- □ Railway
- □ LOR Berlin administrative boundaries
- □ Berlin addresses
- ☑ Berlin boundaries
- □ German administrative boundaries
- □ Germany Average Household Size
- □ Germany Population 65 and Over - Postal
- □ DWD GeoServer WMS
- □ World Traffic Service
- □ Current Wind and Weather Conditions
- Topographic
- survey123 8d6109e96233456b8c77b2ffedab15ba stakeholder - metadata
- survey123 8d6109e96233456b8c77b2ffedab15ba fieldworker - metadata
- EInwohner-Altersgruppen
- Foreigners stats LOR
- EInwohner-Altersgruppen
- EInwohner-Altersgruppen numbers
- EInwohner-Altersgruppen numbers

Figure 2.12: *Heat Map showing Areas of Schools with Immediate Evacuation Needs*

work [127]. The apps could be used both by the operators of DRK as well as the civilians. We demonstrated how critical infrastructures could be identified along with PoIs during the HADR operations such as hospitals, ambulance locations, schools, kindergartens, bus, rail and air stops, pharmacies etc. where people could seek help. We added routing for civilians through the apps so that they could be pointed to the PoIs. The DRK responders could also use the app to locate and plan their evacuation based on ground reports as well as pre-aggregated and analysed data. Figure 2.12 shows the heat map on the ArcGIS map showing the areas with schools which need evacuation based on the analysis of the DRK operators. The operators here choose the density function created using ArcGIS tools to aggregate at-risk school areas over the administrative boundaries of Berlin.

2.5 Lessons Learned for Further Research

The section 2.4 showed that it is possible to connect to Smart City assets while using IoT technologies as a core component. It showed the way forward for the domain for HADR agencies to adopt IoT as an enabler for the future HADR ops while interfacing the legacy applications and devices. Using open standards that enable interoperability between different data sources and consumers is an important aspect for finding resources and consuming services through end-points. For this purpose, the concept of gateways and middleware components built into the HADR ICT infrastructure was found to be the only way for allowing space for existing and future integration with heterogeneous systems.

But there were multiple issues found with approaches currently used for Smart Cities/urban constructs for providing their services to be used. The work done at Helsinki, Warsaw and Berlin showed that there are multiple agencies and therefore multiple sources of data that are essentially needed during a HADR operation. Ideally in such case, a central API dictionary from a city provider would be needed which the agencies can connect to. But its not realistic all the time. So, an ICT architecture is needed for the agencies to deploy quickly at a disaster site and have the components. This architecture should address issues related to discovery, connecting to various end devices directly and to filtered/analysed data through city services. So, following the IoT and ICT landscape for discovering widely used architectures based on best practices is needed. Further, during the demonstrations, only one IoT protocol was considered for experimentation, but in real-world there can be many providers using their own IoT protocol suitable for their use-cases. So, the architectures also need to put that into consideration.

Another aspect discovered during the operations was w.r.t actuation i.e. if we have the event which triggers an action, how can IoT be leveraged for delivering those actions. In such scenarios, robots and unmanned devices are of potential use where there is limited time and space, and always direct human interaction with the scene is not possible as the first course of action. Further, if such IoT assets are available, then how to federate such actions between the participating C2 systems operated by the HADR agencies. Federation of various IoT and Smart City assets between the agencies is important since one agency or one agency's asset might not always be "at the right time, at the right place". So exchanging SA information between the agencies' C2 systems for the operators to take due course of actions is the way forward for multi-agency cooperation. It was also found to be worth investigating the security and privacy aspects of IoT devices when being used in the military domain. As the world of IoT expands, its accessibility to agencies is going to increase. So, measuring and finding out the security and privacy aspects while using IoT assets is necessary for future integration.

Finally, humans on the ground are effective sources of information, be it agencies' responders or the civilian population. These human sources of information complement and provide confirmation to the information gathered from the ICT assets. In the end, it will always boil down to the operators and end humans to act upon the information. Although, with AI and automation, many tasks are going to be offloaded from operators but still gathering human inputs from the ground is critical to success of an operation. So, concepts and approaches from this human interaction with the ICT systems was another use-case found to be useful for investigation. The following chapter 3 describes the contributions in the thesis with regards to the issues discussed for HADR operations.

3 Summary of Scientific Research Contributions and Published Papers

"The secret of change is to focus all of your energy, not on fighting the old, but building on the new."

- Socrates (470-399 BC), Philosopher

The second part of the dissertation consists of summary of scientific research contributions made through the thesis. Then the summary of the publications contributed during the thesis in peer-reviewed international conferences, magazines or books is discussed. The author of this thesis is the principal contributor and first author of papers A, C, D, E, F, H and I, joint first author of book chapter B. He is the fourth author of paper G. The papers address the problem areas and the corresponding goals envisioned. They are closely thematically interrelated and try to solve a broader issue of interoperability for HADR operations.

3.1 Scientific Research Contributions

As discussed in Chapter 2, the core research problem lies with the heterogeneity and diverse nature of ICT technologies emerging from IoT and Smart City domains. HADR responder agencies, city administrations and private deployments use a vast array of assets, both hardware and software. These assets are deployed based on the operational, business and economic considerations. Different technologies suit the needs of the respective organisations what they feel is adequate for their needs, either for short or long run. As a result, there are silos of technology assets and data which are not interoperable with each other.

As discussed in Chapter 1, the trend of evolving disaster phenomenon shows that humanity would see more of such disasters. Chapter 2 introduced and suggested how modern ICT assets can increase the effectiveness of HADR operations. But considering the current state of ICT deployments, when HADR situations arise and these ICT assets need to be integrated under the same umbrella, there would be chaos and unavailability of intended ICT resources. The research in this thesis has tries to formulate and envision ways to enable ICT assets to be interoperable in HADR situations.

As presented in Figure 1.6, the thesis goes step by step, investigating the problem areas from an interoperability perspective for HADR operations. Paper in 3.2 described the problem areas, scope and objectives of the PhD work. It described what would be the scientific approach for analysing the problem areas and the corresponding outcomes which would address the problem areas identified. The scientific, technological and social impact of the thesis were also underlined considering the fact that HADR operations in the coming future would directly affect the society.

One of the major issues for interoperability between Smart City and IoT systems, is the heterogeneous architectures for deployment of the ICT assets. Technologies, business processes and economic aspects dictate how an architecture for deployment is laid out and thus how the different ICT components interact. The book chapter in 3.3 presents a survey of the widely standardised and adopted IoT architectures. It identifies various horizontal and vertical components, their related functions for IoT deployments and their corresponding interactions in Smart Cities. It details how they interact and thus how these various functions can be interfaced by the HADR agencies in a real-time environment.

Based on the proposed high level architecture proposed in 3.3, paper in 3.4 presented the applied concept in a real-world demonstration. It presented various components involved in a HADR scenario based on their military applications. The paper described a live demonstration and joint experiment involving heterogeneous assets from various nations and their interoperability with Smart City assets from the city of Warsaw, Poland. Various tiers of ICT assets and the involved technologies for interoperbility is detailed along with the identified problem areas. Interaction involving various IoT and legacy protocols at the device layer and top-layer interaction using web services is described. The basis of this interaction is a shared common Ontology approach which was derived from state-of-the-art Ontologies from the IoT space. The Ontology allowed various service layer instructions to be exchanged between HADR agencies and Smart City components.

Further, one of the major problems identified for integration of IoT with HADR systems such as from the military is their security, privacy, and dependability (SPD) aspects.

HADR assets needs to be robust, reliable and trustworthy. Without these features, such IoT devices even with all their advantages related to cost, size and availability, would not be usable for HADR agencies. The paper in 3.5 looked at this issue from an integrator's point-of-view (POV) and showed how the SPD aspects can be evaluated in a real-world integration of HADR assets. The paper then showed a Verification and Validation (V&V) process for IoT integration based on SPD constraints. This process would enable HADR systems' integrators to objectively look at the SPD aspects of IoT systems to tailor the V&V processes.

For HADR operations being effective, it is inevitable to bring in the assets from the ground i.e. the citizens into the operations perspective. Citizen participation through use of smart devices where citizens contribute their SA data, passively or actively is rapidly getting adopted in Smart Cities. Governments and HADR agencies can not actively cover every nook and corner of the cities or have an accurate SA picture of the densely populated cities. The paper in 3.6 discusses the Crowdsourcing and Crowdsensing concepts for HADR operations. It demonstrates the applicability and effectiveness of these concepts through applied use of smart devices and distributed ICT technologies from the civilian and HADR agency domains. Further, it discusses upcoming ICT solutions to further enhance the citizens' participation in urban areas.

The use of human resources and direct physical interaction with HADR assets with operators is not always possible. There are times when situations do not allow for direct physical human intervention. These situations require deploying remote, manned or unmanned sensor and actuators platforms to gain SA data from the ground. Robots operated in land, air and water form the higher tier of HADR operations providing operators enhanced capabilities. The paper in 3.7 discusses the interoperability issue with robots in HADR situations with focus on IoT-based UAVs. As the adoption of robots in ICT industry has increased, so is the number of platforms provided by manufacturers. A HADR agency can not possibly have all interfaces to all available robot platforms. The paper discusses the concept of interoperability based on Robot Operating System (ROS). ROS is a widely used platform for robotic devices based on which manufacturers provide their custom robotic implementations. It proposes a system architecture for ROS-based interoperable platform and shows a real-world application of architecture through a IoT-based UAV. The applied system shows how interoperability between various HADR agencies and Smart City systems can be achieved when they might need to share their ROS-based robotic platforms.

Another aspect related to interoperability of HADR systems is their discovery. Even if a technically capable HADR asset is available, the current state of things suggests that many of these assets can not be actively discovered and thus can not be used in real-time. The paper in 3.8 discusses a solution for discovery: Multi-domain Asynchronous Gateway Of Things (MARGOT). It targets the discovery issue by proposing a distributed architecture of gateways. The interoperability is based on data exchange through IoT protocols and the ontology proposed in 3.4. The gateway concept allows flow of queries and information over an extended network using query forwarding policies, providing data replication policies and permissions. Discovery agents are proposed for the workflow which are pluggable entities in the MARGOT sphere enabling discovery and management of resources using a wide range of discovery protocols. The architecture proposed was implemented and experiments were conducted with existing Smart City assets to show the MARGOT platform in action.

While MARGOT addressed discovery issues for Smart City assets, a comprehensive deployment architecture is needed for the HADR response forces to quickly deploy on the ground and start interacting with multitude of ICT assets from the agencies and urban installations. The paper in 3.9 proposes such a deployment architecture for Mobile Tactical Operation Centres (MTOCs). The concept presented discusses the various aspects of HADR operations in urban areas and what factors should be considered while designing an architecture for MTOCs. The goal of the architecture is to enable the coalition disaster recovery agencies to co-operate with each other while leveraging existing Smart City assets.

Finally the paper in 3.10 presents the use of MQTT for enabling federation and interoperability in a distributed HADR scenario. As identified in 4.4, MQTT is an industry-wide accepted protocol for IoT exchange and the military domain is also planning to adopt it. The MQTT version 5.0 is the latest version of the protocol which presents many new features essential for driving HADR operations in unpredictable and resource-constrained environments. The paper presents a federation architecture and shows a reference implementation for HADR operations. The ICT assets handled within the reference implementation show how HADR agencies can interoperably use their traditional assets such as vehicles, UAVs and C2 systems with the urban ICT assets. SA data gathered from Smart City services and crowdsourcing platforms are fused and federated between the HADR operators to showcase an operational use-case.

The following subsections describe the papers resulting from the thesis in more detail along with the research questions and goals they address.

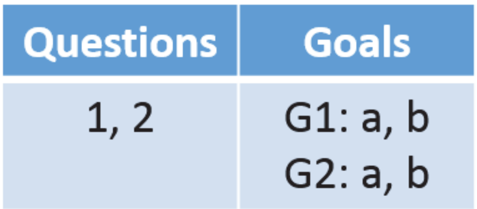
3.2 Paper A: Interoperability for Disaster Relief Operations in Smart City Environments

Manas Pradhan, "Interoperability for Disaster Relief Operations in Smart City Environments," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 711-714.

The thesis journey starts with Paper A which provides an overview of the research problems and intended objectives needed to overcome interoperability issues for HADR operations in Smart City environments. It takes inputs from the work done from the IST-147 group work and work done at Fraunhofer for interoperability of military ICT systems. The objectives and the entailed scientific work for the target PhD topic based on inputs is presented. It describes the approach for the PhD work i.e. what surveys and use-cases need to be considered for formulating the research waypoints based on which the further goals would be targeted. The scientific, technological and social impacts are then mentioned to show the real-world impact of the PhD goals. Based on the "Engineering Method", it finally lists the Integration Framework and the Implementation System deliverables which would conclude and validate the PhD work.

Figure 3.1 shows mapping of the research questions mentioned in 1.3.1 and the corresponding goals mentioned in 1.3.2 with the below description:

- Question 1: What are the different methods and architectures for ICT deployment that can be used by HADR agencies?



Questions	Goals
1, 2	G1: a, b G2: a, b

Figure 3.1: *Mapping Paper A to Research Questions and Goals*

  - G1 (a): Overview of deployed technologies and its corresponding components from HADR agencies and Smart Cities.
  - G1 (b): Overview of hierarchy and nature of interaction between the ICT components and what is lacking.

- Question 2: What are the hindrances faced by the HADR agencies when being deployed in real-time environments?
  - G2 (a): List service interaction methods within and between the HADR agencies, their shortcomings and possible mitigation strategies.
  - G2 (b): List service interaction methods between the HADR agencies and the cities, the shortcomings and possible mitigation strategies.

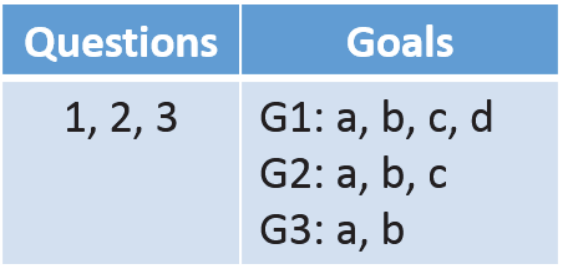
3.3 Book Chapter B: Architectural Considerations

Christoph Fuchs, Manas Pradhan, Niranjan Suri, Mauro Tortonesi, and Frank T. Johnsen. Architectural Considerations. In Niranjan Suri, Konrad Wrona, and Zbigniew Zielinski, editors, Military applications of Internet of Things, chapter 3. Springer, 2021.

In section 2, the use-case for considering various ICT deployments and their architectural considerations were mentioned. For scenarios involving IoT technologies in Smart City environments, to alleviate issues mentioned in 1.1, requires investigation into state-of-the-art and widely used IoT architectures. Book Chapter B undertakes this problem case and presents various architectural considerations from the civilian and the military domains. It presents various common interactions in the architectures as well as, what is important w.r.t interoperability with existing HADR agencies (military) ICT architectural concepts. It discusses how the Smart City ICT deployment is laid out and how the military IoT frameworks could access these Smart City assets/services. It discusses the idea of "services" and their accessibility in Smart City environments. As mentioned in 1.1, incorporating or designing a HADR agency ICT architecture based on just one/or multiple existing Smart City architectures is not realistic. Instead what is needed is accessibility to service end points. In this regard, the paper describes the various end-point connection constructs and then how to describe and discover services accessible through the end-points.

Figure 3.2 shows mapping of the research questions mentioned in 1.3.1 and the corresponding goals mentioned in 1.3.2 with the below description:

- Question 1: What are the different methods and architectures for ICT deployment that can be used by HADR agencies?
  - G1 (a): Lists the IoT architectures and standardisation efforts.
  - G1 (b): Describes the architecture assessment corresponding to military ICT system deployment and provides integration frameworks based on open standards.
  - G1 (c): Presents the Smart City service access methods to further and complement the HADR agencies' operations.
  - G1 (d): Proposes a generic architecture for HADR operations.
- Question 2: What are the hindrances faced by the HADR agencies when being deployed in real-time environments?
  - G2 (a): Lists service interaction methods between the components of military ICT deployment.
  - G2 (b): Lists service interaction methods between the HADR agencies and the cities, and proposes service access and interaction mechanisms.
  - G2 (c): Identifies and defines connection points between the Smart City and HADR agency ICT assets.



Questions	Goals
1, 2, 3	G1: a, b, c, d G2: a, b, c G3: a, b

Figure 3.2: *Mapping Book Chapter B to Research Questions and Goals*

- Question 3: How can concepts of IoT and Smart Cities be utilized to further the goal of HADR operations?
  - G3 (a): Lists service interaction methods based on open standard IoT technologies for data exchange, existing usability and applicability, service discovery and access.
  - G3 (b): Analyses methods to leverage Smart City services.

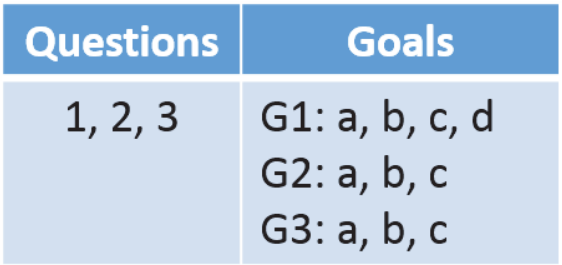
3.4 Paper C: Toward an architecture and data model to enable interoperability between federated mission networks and IoT-enabled smart city environments

Manas Pradhan, Niranjan Suri, Christoph Fuchs, Trude H. Bloebaum and Michal Marks, "Toward an Architecture and Data Model to Enable Interoperability between Federated Mission Networks and IoT-Enabled Smart City Environments," in IEEE Communications Magazine, vol. 56, no. 10, pp. 163-169, October 2018.

Use of IoT for mission critical operations, especially for HADR operations, requires multiple agencies to work together as described in 1.1. Such situations require a common federation mechanism and commonly understood data models that each agency similarly interprets. This paper explores the deployment of IoT in Smart City environments to showcase use of federated mission networks in real-time applications. It discusses the various contexts and architectures for deployment in HADR situations including the challenges with existing techniques for such operations. The various components and actors in such a federated architecture is then described. Following on, it proposes and describes a functioning federated exchange between heterogeneous platforms based on heterogeneous data exchange mechanisms through a shared Ontology structure. This approach involves systems from both civilian and military agencies functioning together to build a common SA to show waypoints for future IoT enabled HADR operations.

Figure 3.3 shows mapping of the research questions mentioned in 1.3.1 and the corresponding goals mentioned in 1.3.2 with the below description:

- Question 1: What are the different methods and architectures for ICT deployment that can be used by HADR agencies?
  - G1 (a): Lists the architectures and standards from IoT and existing military perspectives.
  - G1 (b): Describes the issues and bottlenecks related to federated deployment of HADR agencies.
  - G1 (c): Presents the Smart City service access methods to further and complement the HADR agencies' operations.
  - G1 (d): Proposes a generic architecture for involving military and civilian systems.
- Question 2: What are the hindrances faced by the HADR agencies when being deployed in real-time environments?
  - G2 (a): Lists service interaction methods between the components of military ICT deployment.
  - G2 (b): Lists service interaction methods between the HADR agencies and the cities, and proposes service access and interaction mechanisms.
  - G2 (c): Identifies and defines connection points between the Smart City and HADR agency ICT assets.
  - G2 (d): Discusses an implementation based on the architecture envisioned and its application in real demonstration scenario.



Questions	Goals
1, 2, 3	G1: a, b, c, d G2: a, b, c G3: a, b, c

Figure 3.3: *Mapping Paper C to Research Questions and Goals*

- Question 3: How can concepts of IoT and Smart Cities be utilized to further the goal of HADR operations?
  - G3 (a): Lists service interaction methods based on open standard IoT technologies for data exchange, existing usability and applicability, service discovery and access.
  - G3 (b): Analyses methods to leverage Smart City services especially with related to use of MQTT for exchanging Smart City and IoT data.
  - G3 (C): Discusses the implementation and demonstration from Warsaw Poland.

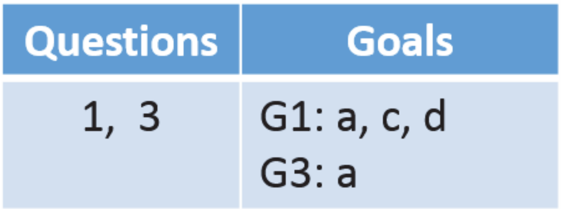
3.5 Paper D: Security, Privacy, and Dependability Evaluation in Verification and Validation Life Cycles for Military IoT Systems

Manas Pradhan and Josef Noll, "Security, Privacy, and Dependability Evaluation in Verification and Validation Life Cycles for Military IoT Systems," in IEEE Communications Magazine, vol. 58, no. 8, pp. 14-20, August 2020.

SPD of any ICT component is necessary to determine their use for critical operations such as with HADR agencies operations. Situations with component failure and untrustworthiness can disrupt the critical and time-intensive operations. Military applications of IoT also targets such use-cases where long term, reliable and secured usage for the military assets is necessary. This paper presented the use of IoT use-case from the background work of IST-147 and 176 groups i.e. if and how IoT can be used for military deployments. It used the SPD evaluation methodology based on the multi-metric approach developed under the European Security in Health Data Exchange (SHIELD) activity, the nSHIELD project. It used the relevance of the method while arguing the other relevant state-of-the-art approaches in the military domain. Based on a real-life implementation involving IoT platform robots and military vehicle interaction, it presented use-cases and validated the approaches for use-case implementation using the SPD multi-metric evaluation. Finally, it presented a V&V process to include the SPD Evaluation. The process aims at V&V of IoT assets so that their use can be proven before being integrated into the military domain. The concepts from this paper can be applied to IoT assets both from the military as well as Smart City domain. Smart Cities have IoT assets and any direct access to such devices from the HADR agency's domain would need such V&V processes. This is needed to make sure that the ICT operations from the HADR agencies' viewpoint is not compromised.

Figure 3.4 shows mapping of the research questions mentioned in 1.3.1 and the corresponding goals mentioned in 1.3.2 with the below description:

- Question 1: What are the different methods and architectures for ICT deployment that can be used by HADR agencies?
  - G1 (a): Describes real-life use of robotic assets based on IoT and how they interact with other military (HADR agency) systems. It also describes a V&V process used for military vehicles to integrate sub-systems from heterogeneous manufacturers.
  - G1 (c): Presents a method for SPD evaluation based on multi-metrics for security and privacy features for IoT-deployments.
  - G1 (d): Proposes a V&V process that can be used for future integration of IoT assets.
- Question 3: How can concepts of IoT and Smart Cities be utilized to further the goal of HADR operations?
  - G3 (a): Explores IoT deployments for military use-cases and identifies methods for incorporating the IoT assets using the V&V processes.



Questions	Goals
1, 3	G1: a, c, d G3: a

Figure 3.4: *Mapping Paper D to Research Questions and Goals*

3.6 Paper E: Leveraging Crowdsourcing and Crowdsensing Data for HADR Operations in a Smart City Environment

Manas Pradhan, Frank T. Johnsen, Mauro Tortonesi and Sabine Delaitre, "Leveraging Crowdsourcing and Crowdsensing Data for HADR Operations in a Smart City Environment," in IEEE Internet of Things Magazine, vol. 2, no. 2, pp. 26-31, June 2019.

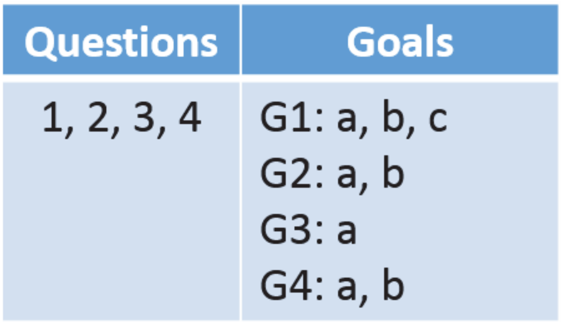
In sub-section 1.1, the problem with future cities was presented i.e. the inflow of humans in large numbers. This is a burden, but at the same time it can be used to the advantage, if ICT technologies can leverage this enormous amount of ground level intelligence and SA data. HADR situations demand immediate actions, and its not possible to deploy assets entirely by HADR agencies. They need to interact with the existing ground "human" assets. In Section 2, the idea of Smart Cities deploying citizen-centric ICT technologies was described. One such aspect usable for HADR agencies is the concept of "Crowdsourcing and Crowdsensing". This paper describes how Crowdsourcing and Crowdsensing be leveraged for HADR operations to assist and complement the actions of HADR agencies. It surveys and describes various real-life implemented projects using these concepts and many other upcoming initiatives from the civilian, NGO and military sectors. How and where these projects were used to assist affected human populations or HADR operators are described as use-cases. Further, it mentions the takeaways from the projects, the outstanding issues and possible solutions, and the future research directions.

Figure 3.5 shows mapping of the research questions mentioned in 1.3.1 and the corresponding goals mentioned in 1.3.2 with the below description:

- Question 1: What are the different methods and architectures for ICT deployment that can be used by HADR agencies?

  - G1 (a): Describes real-life projects and experimentations using ICT tools and in particular mobile devices to gather end user SA data.
  - G1 (b): Lists the issues related to interoperability, privacy and security, trust and connectivity.
  - G1 (c): Presents various services available for Crowdsourcing and Crowdsensing in the described projects.

- Question 2: What are the hindrances faced by the HADR agencies when being deployed in real-time environments?
  - G2 (a): List service interaction methods for the deployed ICT assets.
  - G2 (b): Lists shortcomings and proposes mitigation through future research directions.
- Question 3: How can concepts of IoT and Smart Cities be utilized to further the goal of HADR operations?
  - G3 (a): Explores IoT deployments in Smart Cities and HADR agencies domain and how they are used to assist public safety and security.
- Question 4: How can the end users from cities or citizens and agencies' human assets be brought into the HADR operations scenario?
  - G4 (a): Presents the SMART experiment with the Norwegian home guard and how the Communication Application with Geographical Element Data (CAGED) application used in interaction with the Bring Your Own Device (BYOD) concept.
  - G4(b): Presents projects such as the Public Safety Management by Wellness Telecom, Management of Networked IoT Wearables Very Large-Scale Demonstration of Cultural and Societal Application (MONICA), CrowdFlower and Mission 4636 initiative during Haiti Earthquakes. The ICT aspects of the projects in urban and disaster scenarios provide the insights into how Smart Cities tailor and exploit end user data and services.



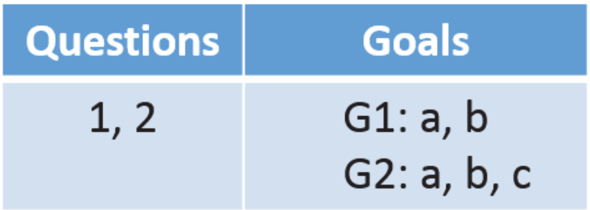
Questions	Goals
1, 2, 3, 4	G1: a, b, c G2: a, b G3: a G4: a, b

Figure 3.5: *Mapping Paper E to Research Questions and Goals*

3.7 Paper F: Enabling Interoperability for ROS-based Robotic Devices for Smart City HADR Operations

Manas Pradhan and Sushma Devaramani, "Enabling Interoperability for ROS-based Robotic Devices for Smart City HADR Operations," MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, 2019, pp. 1-6

Section 2 mentioned the need for actuation, especially with manned and unmanned robots for HADR operations since access to a human operator is not always possible. The paper F describes this use-case while discussing why its not always possible to access these robotic devices from a single integrated platform. It describes how ROS-based robotic assets work and what is needed to integrate COTS ROS-enabled devices on a generic HADR platform. The platform needs to be based on open standards, able to be deployed by various agencies using varied Operating Systems (OS) and controllers for their C2 activities. It provides insight into the related work for enabling interoperability for military robotic devices using NATO standards. Finally, an architecture and platform is proposed and implemented as a PoC to show how interoperability can be achieved for ROS-based robotic platforms. For the PoC, a COTS drone was used along with array of controllers. The PoC also included a C2 application developed using open VAADIN framework and Openstreet Maps. The drone can be controlled interchangeably using the C2 application or the physical controller operating at physically separate locations. Exchange of JSON-formatted status and control messages is achieved over web services using the Ontology format presented in figure 2.11.



Questions	Goals
1, 2	G1: a, b G2: a, b, c

Figure 3.6: *Mapping Paper F to Research Questions and Goals*

Figure 3.6 shows mapping of the research questions mentioned in 1.3.1 and the corresponding goals mentioned in 1.3.2 with the below description:

- Question 1: What are the different methods and architectures for ICT deployment that can be used by HADR agencies?
  - G1 (a): Describes existing robotic interoperability approaches such as NGVA to Robotics and Autonomous Systems Ground (RAS-G) Interoperability Profiles (IOPs) bridge to establish interoperability between military vehicles and robots.
  - G1 (b): Lists the issues related to interoperability and actuation in HADR environments identified during the IST-147 working tenure.
- Question 2: What are the hindrances faced by the HADR agencies when being deployed in real-time environments?
  - G2 (a): Lists service interaction methods for the deployed ICT assets.
  - G2 (b): Lists shortcomings and proposes architecture for a generic ROS based interoperability platform.
  - G2 (c): Demonstrates the architecture implementation through PoC applied as on-field experiment involving COTS IoT drone.

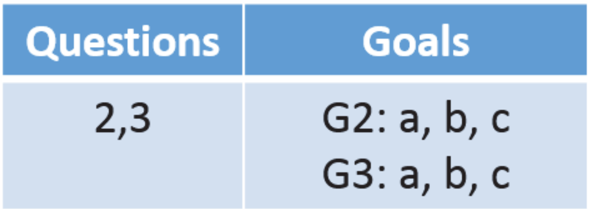
3.8 Paper G: MARGOT: Dynamic IoT Resource Discovery for HADR Environments

Lorenzo Campioni, Rita Lenzi, Filippo Poltronieri, Manas Pradhan, Mauro Tortonesi, Cesare Stefanelli and Niranjan Suri, "MARGOT: Dynamic IoT Resource Discovery for HADR Environments," MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, 2019, pp. 809-814.

Service discovery and federation is an important aspect for future HADR operations where the service API end-points can be connected to gather SA data and enhance it. MARGOT is a solution described in paper G for resource discovery in Smart City environments that implements a distributed and federated architecture and supports a wide range of discovery protocols. It uses IoT data exchange protocols: MQTT and CoAP to enable discovery of services through Discovery Agents (DAs). These DAs discover and register services/assets, store them in a federated database where all stakeholders running MARGOT agents register their services. This enables agents to quickly learn about a service in a crowded and contested ICT environment, where network connectivity and service reliabilities are detrimental for successful HADR operations. The paper describes a experiment performed using Extensible Ad-hoc Networking Emulator (EMANE) where multiple MARGOT nodes were tested in a emulated network environment. The nodes represented the federation, discovery and connectivity with consumed data from a Cloud service: 511ny.org. This 511ny service provided information about public traffic camera, road events, publicly mounted sensors in New York City. The results of the experimentation are presented describing the latencies in discovery using the MQTT, CoAP and HTTP protocols.

Figure 3.7 shows mapping of the research questions mentioned in 1.3.1 and the corresponding goals mentioned in 1.3.2 with the below description:

- Question 2: What are the hindrances faced by the HADR agencies when being deployed in real-time environments?
  - G2 (a): Describes the service interaction needs for the deployed ICT: IoT and IoBT assets.



Questions	Goals
2,3	G2: a, b, c G3: a, b, c

Figure 3.7: *Mapping Paper G to Research Questions and Goals*

- G2 (b): Presents shortcomings and proposes architecture for a distributed architecture of gateways capable of re-routing queries and information over an extended network using query forwarding policies and to provide data replication policies and permissions.
- G2 (c): Demonstrates the architecture implementation through PoC applied to the emulated network experiment based on EMANE for federation and discovery of services in Smart City environments .

- Question 3: How can concepts of IoT and Smart Cities be utilized to further the goal of HADR operations?
  - G3 (a): Describes the MQTT and CoAP based IoT assets' access in a distributed and federated environment.
  - G3 (b): Uses the 511NY deployed Smart City assets in New York and presents methods to access and federate services offered.
  - G3 (c): Implements and demonstrates the PoC involving the MARGOT nodes while interacting with the Smart City assets.

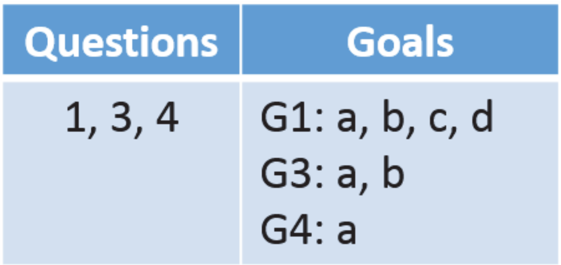
3.9 Paper H: Deployment Architecture for Accessing Smart City and Coalition Assets for Multi-Agency HADR Operations

Manas Pradhan, Christoph Fuchs and Josef Noll, "Deployment Architecture for Accessing Smart City and Coalition Assets for Multi-Agency HADR Operations," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2020, pp. 1-6

HADR agencies need to deploy quickly in the Area of Operations (AOO) to bring in fast and effective relief. Success of future HADR ops involving ICT components needs to be accordingly envisioned to ensure quality SA. This has to be done while sharing of SA data with other participating disaster recovery agencies. Paper G describes such a deployment architecture for MTOCs which can be readily deployed on a mobile set-up carrying ICT assets. It presents the motivation for such fast deployment, existing approaches for Smart Cities and the issues related to it. The components for the fast deployment and operation requires features which can take care of existing issues with connecting and utilizing data/services from Smart Cities and other HADR agencies. Such features include components for security/access control associated with decision making components, discovery of assets and correspondingly routing of requests for the access of assets, and finally storing the registered asset information in a database. All these components need to be generically mapped to an API/platform broker for services and a protocol broker. These brokers take care of translating requests and data exchange based on asset type and request. The MTOC deployment architecture lists and details these components and provides their workflow in the architecture.

Figure 3.8 shows mapping of the research questions mentioned in 1.3.1 and the corresponding goals mentioned in 1.3.2 with the below description:

- Question 1: What are the different methods and architectures for ICT deployment that can be used by HADR agencies?
  - G1 (a): Describes existing use-cases and approaches for HADR responses.
  - G1 (b): Lists the hierarchy and nature of interaction between the ICT components for a rapid deployment of MTOC.
  - G1 (C): Describes the services and actions for individual components of the MTOC architecture.
  - G1 (d): Presents an architecture for MTOC which can be readily deployed in a HADR operation.
- Question 3: How can concepts of IoT and Smart Cities be utilized to further the goal of HADR operations?



Questions	Goals
1, 3, 4	G1: a, b, c, d G3: a, b G4: a

Figure 3.8: *Mapping Paper H to Research Questions and Goals*

- G3 (a): Describes the protocol and API/platform brokers to interface the IoT and Smart City assets.
- G3 (b): Describes the components responsible for asset discovery, registration, storage and access considering the heterogeneous deployment of assets by multiple service providers.

- Question 4: How can the end users from cities or citizens and agencies' human assets be brought into the HADR operations scenario?
  - G4 (a): Presents the method of access of the Crowdsourcing and Crowdsensing assets from the MTOC.

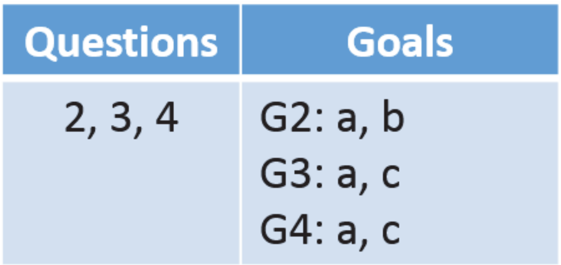
3.10 Paper I: Federation based on MQTT for Urban HADR Operations

Manas Pradhan, "Federation based on MQTT for Urban HADR Operations," in IEEE Communications Magazine, vol. 59, no. 2, February 2021.

IoT protocols are constantly evolving to support new, missing features or correcting existing voids for large-scale acceptance by the industry. The IST-147 proposed using MQTT as the IoT protocol of choice for IoT operations in the NATO domain. This paper I presents the federation of services between C2 systems based on MQTT version 5.0 which is the newest MQTT standard released by Organization for the Advancement of Structured Information Standards (OASIS). The version offers new and improved features with new operating models over older versions 3.0 and 3.1. The PoC implementation based on version 5.0 is used to show federation of HADR services. Backward compatibility for various features of MQTT versions is also shown. The use-case presented in the PoC implementation is based on the current COVID-19 situation where Crowdsourced data from various private and public sources are pushed onto the RiskLayer service [128]. The RiskLayer service offers fine-grained data about latest COVID situations in districts, states and municipalities across Germany. The implementation also shows federation and fusing of SA data on multiple C2 systems (both proprietary and open) representing different HADR agencies. Also, the PoC uses transport APIs to show the real-time road events/conditions across Germany representing another Smart City service which can be leveraged to form precise SA and exchanging them across agencies.

Figure 3.9 shows mapping of the research questions mentioned in 1.3.1 and the corresponding goals mentioned in 1.3.2 with the below description:

- Question 2: What are the hindrances faced by the HADR agencies when being deployed in real-time environments?
  - G2 (a): Describes existing use-cases and approaches for HADR responses w.r.t federation and accessing heterogeneous agency assets.
  - G2 (b): Proposes distributed architecture for federation based on open IoT standards and presents a real-use case implementation using military and open-source C2 systems.
- Question 3: How can concepts of IoT and Smart Cities be utilized to further the goal of HADR operations?
  - G3 (a): Describes the MQTT V 5.0 protocol and its new features for federated data exchange mechanisms for HADR ops usability and applicability.
  - G3 (C): Shows PoC implementation where agency C2 systems consume and federate data from Smart City transport services.
- Question 4: How can the end users from cities or citizens and agencies' human assets be brought into the HADR operations scenario?



Questions	Goals
2, 3, 4	G2: a, b G3: a, c G4: a, c

Figure 3.9: *Mapping Paper I to Research Questions and Goals*

- G4 (a): Presents the RiskLayer COVID Crowdsourced data service.
- G4 (C): Presents PoC where Germany's real-time COVID data is fused with the transport data to form precise SA for addressing emergency situations in an experimental environment. The emergency response is then initiated by using actuation on the federated C2 systems.

4 Conclusion

“The stakes are very high in how we construct the future of the Internet, ... Do we want a winner-takes-all scenario for whichever company ultimately creates that particular piece of intellectual property that maximizes interoperability (across systems) or do we want to create a commons”

- Michael Tiemann, Vice President
Open Source Affairs, Red Hat

This chapter concludes *Part I* of the thesis. It gives a summary of the research and highlights the key contributions of the thesis. It provides some considerations for ethics and finally concludes with suggestions for future research.

4.1 Summary of the Research

The overall goal of this research was to find out methods and possibilities for establishing interoperability between heterogeneous ICT systems for HADR Operations in Smart City Environments. From this overall goal, several research questions were identified that resulted in specific research objectives achieved including:

1. Analysis of interactions with existing IoT and Smart City deployment architectures, and investigating how to deploy ICT assets and associated mechanisms for HADR operations based on the envisioned architectures:
    - Analysed various standards for IoT and Smart City deployment and formulated ICT deployment architectures from HADR agencies’ perspective.
    - Conceptualized architectures based on open standards for allowing interoperable operations of IoT and Smart City services.
    - Proposed an Ontology for federated data exchange based on existing open standard IoT Ontologies.

- Used the corresponding data model from the Ontology designed for exchanging IoT and Smart City data from a HADR perspective.
- Showed interoperability between heterogeneous data sources using heterogeneous data exchange methods.
- Showed the interoperable interaction of various legacy and IoT assets in PoC implementations while exchanging SA data with HADR agencies.

2. Crowdsourcing and Crowdsensing concepts for integration and utilizing end-user/human ground asset data to aid the HADR agencies:

   - Surveyed and analysed real-life projects dealing with Crowdsourcing and Crowdsensing for public safety and security, and application by HADR agencies.
   - Proposed methods for use of the concepts in HADR operations to gain end-user SA data.
   - Demonstrated end-user Crowdsourced data integration for PoC HADR scenarios involving multiple agencies, C2 systems and combining Smart City services.

3. Analysing security and privacy evaluation methods, and proposing V&V processes for future IoT asset usage.

   - Provided a real-life working use-case of an IoT asset interacting with a core HADR ICT asset (a C2 system) communicating over radio links.
   - Applied the SPD methodology to showcase the multi-metric measurement for IoT assets for critical operations.
   - Used the V&V process used for NGVA standard and introduced SPD methods in the V&V process.
   - The V&V process when coupled with SPD methodology provides an approach for secure operation and integration of IoT assets for the HADR agencies.

4. Implementation and experimentation of generic platforms for robotic device usage across heterogeneous ICT set-ups.

   - Provided use-cases and motivation for generic platform development for robotic devices based on ROS.

- Developed and demonstrated a generic platform for interoperability for ROS-based robotic devices using open standards and frameworks.
- Demonstrated using PoCs how to enable federation for robotic devices using standard Ontologies over heterogeneous controllers and operating platforms.

5. Experimentation and implementation showing Smart City asset discovery and federation using IoT protocols:
    - Analysed methods for accessing Smart city services based on available Smart City data and service providers.
    - Established interoperability and federation based on IoT protocols for sharing and storing Smart City data.
    - Showed how to register, store and distribute discovery asset data between heterogeneous agents on the field.
    - Demonstrated using PoCs how discovery works in real-life and how the discovery can aid HADR services.
6. Showing use of MQTT for a full-scale federation scenario including operational C2 systems and Smart City services:
    - Analysed various IoT protocols and established MQTT as the IoT protocol to go for a federated IoT data exchange between HADR agencies.
    - Discussed the advantages for MQTT's features based on version 5.0 and applied them to achieve federation.
    - Applied the concepts to a PoC implementation to showcase a HADR operation that uses MQTT and exchanges SA data between heterogeneous agency and civilian assets.

The IMRAD method was used for writing the dissertation, as well as for each of the individual papers for problem identification and resolution. Scientific methods based on theories and hands-on experiences were used for describing and identifying individual problem areas and correspondingly providing solution approaches. It involved study and analysis of real-life and state-of-the-art approaches to solve those issues. Finally, based on the proposed solution approaches, PoC implementations were provided to showcase the usability and applicability to the problem areas.

The outcome of the research has been published in conference proceedings, international magazines and as a book chapter; three have been published in magazines, four in international conference proceedings and one as a chapter in a book publication. Concepts, results and future research directions related to the thesis work was presented as a talk in the yearly German national technology forum [129]. Some of the concepts and implementation for Smart City data integration for military HADR systems have already been included and demonstrated for a national project [130].

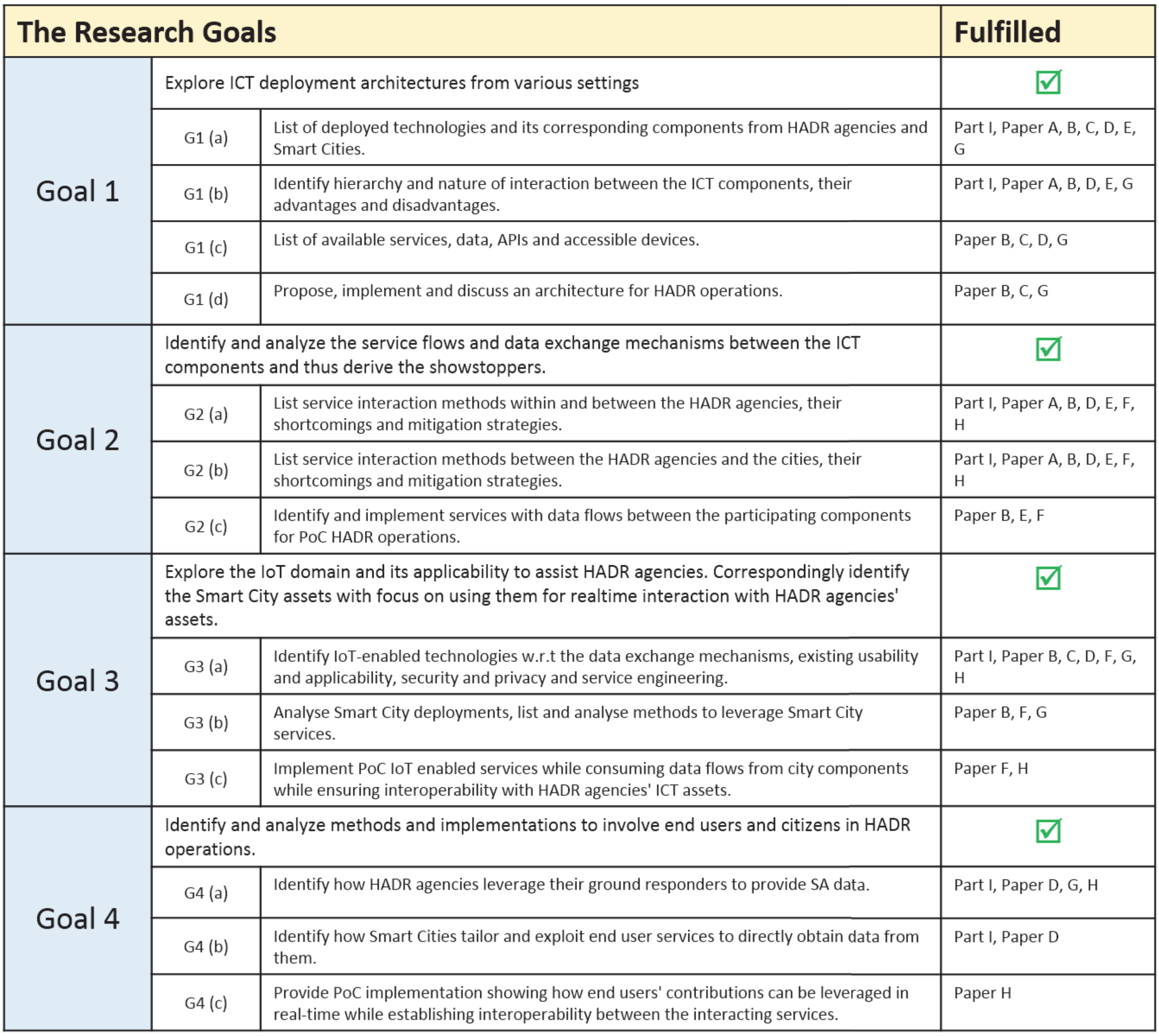
The research goals, which were presented and discussed in Section 1.3.2, have been addressed. How the goals, with sub-goals, have been fulfilled is outlined in Table 4.1.

In addition to addressing the defined research goals, applicability and relevance for have been provided in terms of interoperability solutions, advise and consultancy to real-world HADR operators [131], participating research groups of NATO [132] and the German Armed Forces (Bundeswehr) [133] during the research period.

4.2 Takeaways from the Thesis Results

The primary concepts dealt in the research lie with use of open standards and proposing generic methods of ICT operation that can be adopted by any HADR agency. For any kind of HADR operation that needs interaction with other Ontologies, requires that the ICT stack deployed follows and adopts standards that are open and evolving. Any kind of implementation that uses a closed system operation model will cause issues for the coming future. Especially, considering IoT and Smart Cities, the standards and protocols are still evolving and not standardised in a broader sense. Any kind of implementation from a HADR agency that is based on proprietary solutions will limit future proofing the usage.

From a HADR perspective, from the various PoCs for HADR use-cases implemented in



The Research Goals			Fulfilled
Goal 1	Explore ICT deployment architectures from various settings		☑
	G1 (a)	List of deployed technologies and its corresponding components from HADR agencies and Smart Cities.	Part I, Paper A, B, C, D, E, G
	G1 (b)	Identify hierarchy and nature of interaction between the ICT components, their advantages and disadvantages.	Part I, Paper A, B, D, E, G
	G1 (c)	List of available services, data, APIs and accessible devices.	Paper B, C, D, G
	G1 (d)	Propose, implement and discuss an architecture for HADR operations.	Paper B, C, G
Goal 2	Identify and analyze the service flows and data exchange mechanisms between the ICT components and thus derive the showstoppers.		☑
	G2 (a)	List service interaction methods within and between the HADR agencies, their shortcomings and mitigation strategies.	Part I, Paper A, B, D, E, F, H
	G2 (b)	List service interaction methods between the HADR agencies and the cities, their shortcomings and mitigation strategies.	Part I, Paper A, B, D, E, F, H
	G2 (c)	Identify and implement services with data flows between the participating components for PoC HADR operations.	Paper B, E, F
Goal 3	Explore the IoT domain and its applicability to assist HADR agencies. Correspondingly identify the Smart City assets with focus on using them for realtime interaction with HADR agencies' assets.		☑
	G3 (a)	Identify IoT-enabled technologies w.r.t the data exchange mechanisms, existing usability and applicability, security and privacy and service engineering.	Part I, Paper B, C, D, F, G, H
	G3 (b)	Analyse Smart City deployments, list and analyse methods to leverage Smart City services.	Paper B, F, G
	G3 (c)	Implement PoC IoT enabled services while consuming data flows from city components while ensuring interoperability with HADR agencies' ICT assets.	Paper F, H
Goal 4	Identify and analyze methods and implementations to involve end users and citizens in HADR operations.		☑
	G4 (a)	Identify how HADR agencies leverage their ground responders to provide SA data.	Part I, Paper D, G, H
	G4 (b)	Identify how Smart Cities tailor and exploit end user services to directly obtain data from them.	Part I, Paper D
	G4 (c)	Provide PoC implementation showing how end users' contributions can be leveraged in real-time while establishing interoperability between the interacting services.	Paper H

Table 4.1: *The fulfillment of the Research Goals and Sub-goals (the expected measurable outcome).*

the thesis, all of them had to adopt to the local Smart City services. There is no standard way of accessing the Smart City services and in the coming future, this would still be an issue. So, a flexible architecture for deployment as presented in the thesis is needed. Such an architecture supports heterogeneous open standards for web services, protocols for IoT and Smart Cities, and physical device use. Further, for the architectural considerations, there will always be concerns for safety and security of the HADR ICT deployment. Not every aspect of HADR ICT deployment, such as data models, Ontologies, service interfaces etc. can be made public. Instead, there always needs to be service interfaces or API dictionaries available with key mechanisms that will allow external entities access to those services.

Further, the concept of *Gateways* and *Middleware* solutions for any modern ICT deployment is mandatory. Every ICT model should allow for scalability and extensibility through use of gateways. Not every organisation would be self-sufficient containing every functionality that it needs, and the same rests for HADR agencies. Not all agencies will have everything individually, that they need immediately in aggravated circumstances during disasters. With cloud and edge services becoming a norm for industry, access to services have become more flexible and accessible. Organisations can access what they don't have, be it applications, infrastructure or software on per-use-basis. They don't need to own anything but use as they need from these multitude of service providers. The future ICT development should be based on using the SOA concepts so that focus should be on services and APIs that can be either exposed to others, or allow to be ingested from others. This would make ICT deployments more economic and flexible, supporting big and small organisations leverage their core business models.

IoT is still very much ingrained with the physical concept of devices. Standards for such physical characteristics have been evolving and are expected to become more structured in the coming years. As a result, the *COTS* concept will push the industry further. These standards will enable easier adoption and integration by the technology users, be it private or industrial. Labels for such devices are soon expected to be rolled out enabling users to get *certified for purpose* devices. Concepts of SPD and V&V as discussed in the thesis will gain traction for such integration and certification.

Along the lines of physical devices, the thesis dealt with creating generic platform implementations based on ROS which simplifies the use of robotic devices. As robots gain more intelligence i.e. more capabilities are added for automation, such platforms are unavoidable. The focus for any robotic interaction should be on creating new functionalities based on existing platform capabilities and not on adding integration of any new robot standards. System manufacturers can provide their platforms based on ROS, and the end users using the developed gateway mechanisms in the thesis can concentrate on generating add-on intelligence for their robots. Especially for HADR agencies, such generic platforms will add value to their operational effectiveness by using robotic assets from other participating agencies using such generic robotic platforms. They can supplement and complement the joint ISR capabilities by sharing their robotic devices and services.

Finally, end users will always form the core of business models of companies, and the same applies for HADR agencies. So the concepts of Crowdsourcing and Crowdsensing presented in the thesis show the waypoints of how HADR agencies can leverage the huge potential of Smart Devices to gain precise, real-time and on-demand SA data.

4.3 Ethical considerations of the Results

HADR operations require access to very precise data and intelligence as close to the ground as possible. It means that many times there is an operational requirement to gather data from people's personal devices. Apart from the necessary data, there is always the concern and possibility that the security and privacy of individual citizens would be breached. A similar use-case was encountered at the IST-147 group's experimentation at Warsaw where for the PoC demonstration, we accessed a Smart Home data from a private individual in Warsaw. Although, there was an established agreement with the user and the user could monitor and change what data is accessible from the Smart Home device, in many cases its not the case. Many users do not know how to handle their IT systems and thus this creates a big loophole which could possibly be exploited nefariously. Further, many city platforms have security and economic concerns about the data which they provide to 3rd parties which also is an ethical showstopper. What and how the data can be accessed, what can be analysed from it, if and how the data is stored and shared with other HADR agencies is still not defined under a unified process.

These concerns often lead to disruptions on the ground while accessing the data from the cities and individuals. Although many times, the intentions are right, loopholes in laws, security and privacy components of ICT systems always keep the service providers skeptical of providing access to their assets. Currently, there are initiatives like that from European Defence Agency (EDA) to formalise data protection and privacy requirements for European citzens [134]. Similarly, General Data Protection Regulation (GDPR) from the European Union also provides a framework and rules for protecting citizens' data [135]. Still its a long way ahead, how to approach such issues and handle it.

4.4 Suggestions for Further Research

This thesis showed the possibilities and applications for interoperability for Smart City HADR operations. But still most of the research is at conceptual and experimental level with relatively controlled assumptions and parameters. Based on the content handled in the thesis the following areas were identified for further research:

- The PoC demonstrations used a simple Ontology format used for data exchange and the data consumed through the middleware was transformed to this format to enable interoperability of data. But the discovery of Smart City service end-points based on this Ontology is practically not possible. There are plethora of data models and Ontologies floating around in the Smart City space and there is no established Ontology which can be directly mapped to. The IST-176 and IEEE groups that i am working with is currently looking into this issue. From the NATO IST-176 group's viewpoint, the idea is to create a new IoT Ontology specification to handle future IoT asset needs. The resulting Ontology would be introduced a part of the new FMN specification. From the IEEE viewpoint, we are currently looking into best practices and available Ontologies from various organisations and nations to provide recommendations for discovery of Smart City services.
- Robotic platforms in the recent years have evolved with new standards introduced. Currently, we are looking into ROS2 which is new version of ROS [136]. The idea is to extend the generic platform built for ROS, to include ROS2 exchanges. It would enable a single ROS platform for older and the newer ROS-based devices.

- We are trying to extend the EMANE network emulator to include IoT radio emulation characteristics which can be used for lab experimentation. Currently EMANE supports limited tactical radio links which might not be usable for IoT radios. For this, we are looking to available tools for IoT radio emulation and finding ways to integrate or reuse those tools.

- The thesis showed the multi-C2 system federation. Currently, at Fraunhofer we are in process of building an integrated testbed for the NATO nations where they could access virtual testbed environments and deploy their C2 applications to test out interoperability. The goal is find out what are the showstoppers and solve those issues before doing on-field experiments.

- Anglova Scenario was developed by the NATO IST-124 group to simulate field environments involving agency assets [137]. It handles various formations of agency asset deployment and then test them over EMANE radio links. It allows to emulate movement of troops and exchange of data from the deployed ICT assets. Currently, there is no defined HADR scenario (vignette) modelled. The future plan is to model a HADR scenario with cooperation and inputs from HADR agencies and test out various ICT deployment formations and tactics. Further, we are using ML techniques to analyse and choose Smart City resources based on predetermined parameters which can provide appropriate SA information when requested.

This thesis has contributed with publications in international magazines, conference proceedings, book and talks. The research goals defined in Part 1 have been achieved. The results in this thesis have practical relevance and provide a pathway for upcoming HADR operations strategies. This research has also laid the groundwork for future extension of the FMN spirals and IEEE standardisation efforts for Smart Cities.

References

[1] Luciana B Sollaci and Mauricio G Pereira. The introduction, methods, results, and discussion (imrad) structure: a fifty-year survey. *Journal of the medical library association*, 92(3):364, 2004.

[2] Stephan Haller, Stamatis Karnouskos, and Christoph Schroth. The internet of things in an enterprise context. In *Future Internet Symposium*, pages 14–28. Springer, 2008.

[3] Vito Albino, Umberto Berardi, and Rosa Maria Dangelico. Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of urban technology*, 22(1):3–21, 2015.

[4] Hafedh Chourabi, Taewoo Nam, Shawn Walker, J Ramon Gil-Garcia, Sehl Mellouli, Karine Nahon, Theresa A Pardo, and Hans Jochen Scholl. Understanding smart cities: An integrative framework. In *2012 45th Hawaii international conference on system sciences*, pages 2289–2297. IEEE, 2012.

[5] Frank T Johnsen, Zbigniew Zieliński, Konrad Wrona, Niranjan Suri, Christoph Fuchs, Manas Pradhan, Janusz Furtak, Bogdan Vasilache, Vincenzo Pellegrini, Michał Dyk, et al. Application of iot in military operations in a smart city. In *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, pages 1–8. IEEE, 2018.

[6] Niranjan Suri, Zbigniew Zielinski, Mauro Tortonesi, Christoph Fuchs, Manas Pradhan, Konrad Wrona, Janusz Furtak, Dragos Bogdan Vasilache, Michael Street, Vincenzo Pellegrini, et al. Exploiting smart city iot for disaster recovery operations. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pages 458–463. IEEE, 2018.

[7] Zaheer Allam and Peter Newman. Redefining the smart city: Culture, metabolism and governance. *Smart Cities*, 1(1):4–25, 2018.

[8] Herbert E Huppert and R Stephen J Sparks. Extreme natural hazards: population growth, globalization and environmental change. *Philosophical Transactions of the*

Royal Society A: Mathematical, Physical and Engineering Sciences, 364(1845):1875–1888, 2006.

[9] Hannah Ritchie and Max Roser. Urbanization - our world in data. `https://ourworldindata.org/urbanization`, 11 2019. (Accessed on 01/14/2021).

[10] Jeff Desjardins. Mapped: The world's fastest growing cities. `https://www.visualcapitalist.com/mapped-the-worlds-fastest-growing-cities/`, 11 2015. (Accessed on 01/14/2021).

[11] Hannah Ritchie and Max Roser. Natural disasters - our world in data. `https://ourworldindata.org/natural-disasters`, 11 2019. (Accessed on 01/14/2021).

[12] Niall McCarthy. The natural disasters that inflict the most economic damage. `https://www.statista.com/chart/4114/the-natural-disasters-that-inflict-the-most-economic-damage/`, 12 2015. (Accessed on 01/14/2021).

[13] J Edward Taylor and Philip L Martin. Human capital: Migration and rural population change. *Handbook of agricultural economics*, 1:457–511, 2001.

[14] Anita J Gagnon, Meg Zimbeck, Jennifer Zeitlin, Roam Collaboration, et al. Migration to western industrialised countries and perinatal health: a systematic review. *Social science & medicine*, 69(6):934–946, 2009.

[15] Barney Cohen. Urban growth in developing countries: a review of current trends and a caution regarding existing forecasts. *World development*, 32(1):23–51, 2004.

[16] United Nations Department of Economic and Social Affairs. 68% of the world population projected to live in urban areas by 2050, says un. `https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html`, 05 2018. (Accessed on 12/29/2020).

[17] Stephen Devereux. *Famine in the twentieth century.* IDS, 2000.

[18] William Donner and Havidán Rodríguez. Population composition, migration and inequality: The influence of demographic changes on disaster risk and vulnerability. *Social forces*, 87(2):1089–1114, 2008.

[19] Maarten K Van Aalst. The impacts of climate change on the risk of natural disasters. *Disasters*, 30(1):5–18, 2006.

[20] Ole Magnus Theisen, Helge Holtermann, and Halvard Buhaug. Climate wars? assessing the claim that drought breeds conflict. *International Security*, 36(3):79–106, 2012.

[21] Ronak B Patel and Thomas F Burke. Urbanization—an emerging humanitarian disaster. *New England Journal of Medicine*, 361(8):741–743, 2009.

[22] A Spinelli and G Pellino. COVID-19 pandemic: perspectives on an unfolding crisis. *The British journal of surgery*, 2020.

[23] Halvard Buhaug and Henrik Urdal. An urbanization bomb? population growth and social disorder in cities. *Global environmental change*, 23(1):1–10, 2013.

[24] European Commission. Developments and forecasts on continuing urbanisation. `https://knowledge4policy.ec.europa.eu/foresight/topic/continuing-urbanisation/developments-and-forecasts-on-continuing-urbanisation_en`. (Accessed on 12/30/2020).

[25] World Health Organization et al. *Health risk assessment from the nuclear accident after the 2011 Great East Japan earthquake and tsunami, based on a preliminary dose estimation.* World Health Organization, 2013.

[26] Sandro Schroeder. German city of aachen offers iodine tablets amid nuclear fears. `https://www.dw.com/en/german-city-of-aachen-offers-iodine-tablets-amid-nuclear-fears/a-40318504`, 09 2017. (Accessed on 12/29/2020).

[27] Edward Broughton. The bhopal disaster and its aftermath: a review. *Environmental Health*, 4(1):1–6, 2005.

[28] Andrea Caragliu, Chiara Del Bo, and Peter Nijkamp. Smart cities in europe. *Journal of urban technology*, 18(2):65–82, 2011.

[29] Lawrence J Vale and Thomas J Campanella. *The resilient city: How modern cities recover from disaster.* Oxford University Press, 2005.

[30] Raven Marie Cretney. Local responses to disaster. *Disaster Prevention and Management*, 2016.

[31] Kamal Birdi, Kerry Griffiths, Christine Turgoose, Victòria Alsina, Daniela Andrei, Adriana Băban, P Saskia Bayerl, Fabio Bisogni, Sofia Chirică, Pietro Costanzo, et al. Factors influencing cross-border knowledge sharing by police organisations: an integration of ten european case studies. *Police Practice and Research*, pages 1–20, 2020.

[32] Jan Terpstra. Police, local government, and citizens as participants in local security networks. *Police practice and research: An international journal*, 9(3):213–225, 2008.

[33] Salvatore Loreto and Simon Pietro Romano. Real-time communications in the web: Issues, achievements, and ongoing standardization efforts. *IEEE Internet Computing*, 16(5):68–73, 2012.

[34] Joseph Farrell and Garth Saloner. *Economic issues in standardization.* Franklin Classics, 2018.

[35] Stefan Timmermans and Steven Epstein. A world of standards but not a standard world: Toward a sociology of standards and standardization. *Annual review of Sociology*, 36:69–89, 2010.

[36] Peter J. Denning, Douglas E Comer, David Gries, Michael C. Mulder, Allen Tucker, A. Joe Turner, and Paul R Young. Computing as a discipline. *Computer*, 22(2):63–70, 1989.

[37] Robert L Glass, Venkataraman Ramesh, and Iris Vessey. An analysis of research in computing disciplines. *Communications of the ACM*, 47(6):89–94, 2004.

[38] Robert L Glass. A structure-based critique of contemporary computing research. *Journal of Systems and Software*, 28(1):3–7, 1995.

[39] Marilyn M Rawnsley. Ontology, epistemology, and methodology: A clarification. *Nursing Science Quarterly*, 11(1):2–4, 1998.

[40] Ricardo de Almeida Falbo, Giancarlo Guizzardi, and Katia Cristina Duarte. An ontological approach to domain engineering. In *Proceedings of the 14th international conference on Software engineering and knowledge engineering*, pages 351–358, 2002.

[41] Gregory N Hearn and Marcus Foth. Action research in the design of new media and ict systems. In *Topical issues in communications and media research*, pages 79–94. Nova Science, 2005.

[42] Kathryn Herr and Gary L Anderson. The continuum of positionality in action research. *The action research dissertation: A guide for students and faculty*, pages 29–48, 2005.

[43] James D McKeen, Michael H Zack, and Satyendra Singh. Knowledge management and organizational performance: An exploratory survey. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, volume 7, pages 152b–152b. IEEE, 2006.

[44] Yasir Rashid, Ammar Rashid, Muhammad Akib Warraich, Sana Sameen Sabir, and Ansar Waseem. Case study method: A step-by-step guide for business researchers. *International Journal of Qualitative Methods*, 18:1609406919862424, 2019.

[45] David Peters, Taghreed Adam, Olakunle Alonge, Irene Agyepong, and Nhan Tran. Implementation research: What it is and how to do it. *BMJ (Clinical research ed.)*, 347:f6753, 11 2013.

[46] Mike Allen. *The SAGE encyclopedia of communication research methods.* Sage Publications, 2017.

[47] CARNEGIE MELLON UNIVERSITRY. The" only" coke machine on the internet, 2018.

[48] Mark Wiser. The computer for the 21st century. *Scientific american*, 265(3):66–75, 1991.

[49] Friedemann Mattern and Christian Floerkemeier. *From the Internet of Computers to the Internet of Things*, pages 242–259. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[50] Peter Corcoran. The internet of things: why now, and what's next? *IEEE consumer electronics magazine*, 5(1):63–68, 2015.

[51] Gérald Santucci. The internet of things: Between the revolution of the internet and the metamorphosis of objects. *Vision and Challenges for Realising the Internet of Things*, pages 11–24, 2010.

[52] Kevin Ashton et al. That 'internet of things' thing. *RFID journal*, 22(7):97–114, 2009.

[53] Manas Pradhan, Fahrettin Gökgöz, Nico Bau, and Daniel Ota. Approach towards application of commercial off-the-shelf internet of things devices in the military domain. In *2016 IEEE 3rd world forum on internet of things (WF-IoT)*, pages 245–250. IEEE, 2016.

[54] Denise E Zheng and William A Carter. *Leveraging the internet of things for a more efficient and effective military*. Rowman & Littlefield, 2015.

[55] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[56] Martin Wollschlaeger, Thilo Sauter, and Juergen Jasperneite. The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. *IEEE industrial electronics magazine*, 11(1):17–27, 2017.

[57] Brian Hayes. Cloud computing, 2008.

[58] Jianli Pan and James McElhannon. Future edge cloud and edge computing for internet of things applications. *IEEE Internet of Things Journal*, 5(1):439–449, 2017.

[59] Mauro Tortonesi, James Michaelis, Alessandro Morelli, Niranjan Suri, and Michael A Baker. SPF: An SDN-based middleware solution to mitigate the IoT information explosion. In *2016 IEEE Symposium on Computers and Communication (ISCC)*, pages 435–442. IEEE, 2016.

[60] Emmanuel Darmois, Omar Elloumi, Patrick Guillemin, and Philippe Moretto. IoT standards–state-of-the-art analysis. *Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds*, pages 978–87, 2012.

[61] Gary White, Vivek Nallur, and Siobhán Clarke. Quality of service approaches in IoT: A systematic mapping. *Journal of Systems and Software*, 132:186–203, 2017.

[62] Hamza Baqa, Nguyen Binh Truong, Noel Crespi, Gyu Myoung Lee, and Franck Le Gall. Quality of Information as an indicator of Trust in the Internet of Things. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pages 204–211. IEEE, 2018.

[63] Anna Triantafyllou, Panagiotis Sarigiannidis, and Thomas D Lagkas. Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends. *Wireless communications and mobile computing*, 2018, 2018.

[64] OASIS. MQTT Version 5.0. `https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html`. (Accessed on 01/13/2021).

[65] RFC 7252 - The Constrained Application Protocol (CoAP). `https://tools.ietf.org/html/rfc7252`. (Accessed on 01/13/2021).

[66] ISO/IEC. ISO - ISO/IEC 19464:2014 - Information technology — Advanced Message Queuing Protocol (AMQP) v1.0 specification. `https://www.iso.org/standard/64955.html`. (Accessed on 01/13/2021).

[67] DDS Foundation. DDS Resources. `https://www.dds-foundation.org/dds-resources/`. (Accessed on 01/13/2021).

[68] RFC 4919: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. `https://www.rfc-editor.org/rfc/rfc4919.html`. (Accessed on 01/13/2021).

[69] IEEE Std 802.15.4-2011, IEEE Standard for Local and metropolitan area networks—Part 15.4: Low-Rate Wireless Personal Area Networks (WPANs). `http://ecee.colorado.edu/~liue/teaching/comm_standards/2015S_zigbee/802.15.4-2011.pdf`. (Accessed on 01/13/2021).

[70] Carles Gomez, Joaquim Oller, and Josep Paradells. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors*, 12(9):11734–11753, 2012.

[71] LoRa Alliance. LoRaWAN® Specification v1.1 — LoRa Alliance®. `https://lora-alliance.org/resource-hub/lorawanr-specification-v11`. (Accessed on 01/13/2021).

[72] Brecht Reynders and Sofie Pollin. Chirp spread spectrum as a modulation technique for long range communication. In *2016 Symposium on Communications and Vehicular Technologies (SCVT)*, pages 1–5. IEEE, 2016.

[73] Ivan Zyrianoff, Alexandre Heideker, Dener Silva, João Kleinschmidt, Juha-Pekka Soininen, Tullio Salmon Cinotti, and Carlos Kamienski. Architecting and deploying IoT smart applications: A performance–oriented approach. *Sensors*, 20(1):84, 2020.

[74] Ibrar Yaqoob, Ejaz Ahmed, Ibrahim Abaker Targio Hashem, Abdelmuttlib Ibrahim Abdalla Ahmed, Abdullah Gani, Muhammad Imran, and Mohsen Guizani. Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. *IEEE wireless communications*, 24(3):10–16, 2017.

[75] Ali Arsanjani. Service-oriented modeling and architecture. *IBM developer works*, 1:15, 2004.

[76] Keith Kirkpatrick. Software-defined networking. *Communications of the ACM*, 56(9):16–19, 2013.

[77] Liliana Antao, Rui Pinto, Joao Reis, and Gil Gonçalves. Requirements for testing and validating the industrial internet of things. In *2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pages 110–115. IEEE, 2018.

[78] Xuyang Liu, KH Lam, Ke Zhu, Chao Zheng, Xu Li, Yimeng Du, Chunhua Liu, and Philip WT Pong. Overview of spintronic sensors with internet of things for smart living. *IEEE Transactions on Magnetics*, 55(11):1–22, 2019.

[79] Tian Wang, Guangxue Zhang, Anfeng Liu, Md Zakirul Alam Bhuiyan, and Qun Jin. A secure iot service architecture with an efficient balance dynamics based on cloud and edge computing. *IEEE Internet of Things Journal*, 6(3):4831–4843, 2018.

[80] In Lee. The internet of things for enterprises: An ecosystem, architecture, and iot service business model. *Internet of Things*, 7:100078, 2019.

[81] Long Sun, Yan Li, and Raheel Ahmed Memon. An open IoT framework based on microservices architecture. *China Communications*, 14(2):154–162, 2017.

[82] Paula Fraga-Lamas, Tiago M Fernández-Caramés, Manuel Suárez-Albela, Luis Castedo, and Miguel González-López. A review on internet of things for defense and public safety. *Sensors*, 16(10):1644, 2016.

[83] Stephen Russell and Tarek Abdelzaher. The internet of battlefield things: the next generation of command, control, communications and intelligence (C3I) decision-making. In *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*, pages 737–742. IEEE, 2018.

[84] Ioannis Agadakos, Gabriela F Ciocarlie, Bogdan Copos, Jemin George, Nandi Leslie, and James Michaelis. Security for resilient iobt systems: emerging research directions. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 1–6. IEEE, 2019.

[85] Radovan Novotnỳ, Radek Kuchta, and Jaroslav Kadlec. Smart city concept, applications and services. *J. Telecommun. Syst. Manag*, 3(1), 2014.

[86] Lukas Neckermann. *The mobility revolution: zero emissions, zero accidents, zero ownership*. Troubador Publishing Ltd, 2015.

[87] Harlow W Sheidley. The webster-hayne debate: Recasting new england's sectionalism. *The New England Quarterly*, 67(1):5–29, 1994.

[88] Sang Keon Lee, Heeseo Rain Kwon, H Cho, J Kim, and D Lee. International case studies of smart cities singapore. *Inter-American Development Bank*, 2016.

[89] Paolo Cardullo and Rob Kitchin. Smart urbanism and smart citizenship: The neoliberal logic of 'citizen-focused'smart cities in europe. *Environment and Planning C: Politics and Space*, 37(5):813–830, 2019.

[90] Bin Cheng, Salvatore Longo, Flavio Cirillo, Martin Bauer, and Ernoe Kovacs. Building a big data platform for smart cities: Experience and lessons from santander. In *2015 IEEE International Congress on Big Data*, pages 592–599. IEEE, 2015.

[91] Patrick TI Lam and Ruiqu Ma. Potential pitfalls in the development of smart cities and mitigation measures: An exploratory study. *Cities*, 91:146–156, 2019.

[92] Jiska Engelbert, Liesbet van Zoonen, and Fadi Hirzalla. Excluding citizens from the european smart city: The discourse practices of pursuing and granting smartness. *Technological Forecasting and Social Change*, 142:347–353, 2019.

[93] Abdelfatteh Haidine, Sanae El Hassani, Abdelhak Aqqal, and Asmaa El Hannani. The role of communication technologies in building future smart cities. *Smart Cities Technologies*, 1:1–24, 2016.

[94] Eduardo Felipe Zambom Santana, Ana Paula Chaves, Marco Aurelio Gerosa, Fabio Kon, and Dejan S Milojicic. Software platforms for smart cities: Concepts, requirements, challenges, and a unified reference architecture. *ACM Computing Surveys (Csur)*, 50(6):1–37, 2017.

[95] NEC Corporation. The Solution: CCOC the thinking platform. `https://es.nec.com/es_ES/solutions_services/smartcity/en/solution/index.html`. (Accessed on 01/06/2021).

[96] Paul Wilson. State of smart cities in uk and beyond. *IET Smart Cities*, 1(1):19–22, 2019.

[97] Rob Kitchin, Claudio Coletta, Leighton Evans, Liam Heaphy, and Darach MacDonncha. Smart cities, epistemic communities, advocacy coalitions and the'last mile'problem. *It-Information Technology*, 59(6):275–284, 2017.

[98] B Domres, HH Schauwecker, K Rohrmann, G Roller, GW Maier, and A Manger. The german approach to emergency/disaster management. *Medicinski arhiv*, 54(4):201–203, 2000.

[99] Wisinee Wisetjindawat, Hideyuki Ito, Motohiro Fujita, and Hideshima Eizo. Planning disaster relief operations. *Procedia-Social and Behavioral Sciences*, 125:412–421, 2014.

[100] Aruna Apte, C. Greenfield, K. Yoho, and C. Ingram. An analysis of united states navy disaster relief operations, 2012.

[101] Wen K Chan. Operational Effectiveness of Smartphones and Apps for Humanitarian Aid and Disaster Relief (HADR) Operations–A Systems Engineering Study. Technical report, NAVAL POSTGRADUATE SCHOOL MONTEREY CA DEPT OF SYSTEMS ENGINEERING, 2012.

[102] CIMIC Field Handbook. Civil-Military Cooperation Centre of Excellence (2016).

[103] Wrona Konrad, Pradhan Manas, Mauro Tortonesi, Suri Niranjan, et al. Civil-Military Collaboration in Smart Environments under Adversarial Conditions. In *The First International Workshop on Internet of Things for Adversarial Environments (in conjunction with IEEE INFOCOM 2019)*, pages 1–6. IEEE, 2019.

[104] Erik P Blasch, Richard Breton, and Pierre Valin. Using the c-ooda model for cimic analysis. In *Proceedings of the 2011 IEEE National Aerospace and Electronics Conference (NAECON)*, pages 130–138. IEEE, 2011.

[105] David Peabody. The challenges of doing good work: The development of Canadian forces CIMIC capability and NGOs. *Journal of military and strategic studies*, 8(3), 2006.

[106] Myron Hura, Gary McLeod, Eric Larson, James Schneider, and Daniel Gonzales. Interoperability: A continuing challenge in coalition air operations. Technical report, Rand Corp Santa Monica Ca, 2000.

[107] Konrad Wrona, Mauro Tortonesi, Michał Marks, and Niranjan Suri. Leveraging and fusing civil and military sensors to support disaster relief operations in smart environments. In *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*, pages 790–797. IEEE, 2019.

[108] Marianne R Brannsten, Frank T Johnsen, Trude H Bloebaum, and Ketil Lund. Toward federated mission networking in the tactical domain. *IEEE Communications Magazine*, 53(10):52–58, 2015.

[109] NATO ACT. Federated Mission Networking. `https://www.act.nato.int/activities/fmn`. (Accessed on 01/07/2021).

[110] Ketil Lund, Anders Eggen, Dinko Hadzic, Trude Hafsoe, and Frank T Johnsen. Using web services to realize service oriented architecture in military communication networks. *IEEE communications magazine*, 45(10):47–53, 2007.

[111] Smartresilience. http://smartresilience.eu-vri.eu/. (Accessed on 01/07/2021).

[112] Infrastress. Critical infrastructure. https://www.infrastress.eu/. (Accessed on 01/07/2021).

[113] Antonio J Jara, Martin Serrano, Andrea Gómez, David Fernández, Germán Molina, Yann Bocchi, and Ramon Alcarria. Smart cities semantics and data models. In *International Conference on Information Theoretic Security*, pages 77–85. Springer, 2018.

[114] IEEE. IEEE IoT Initiative Smart Cities Working Group. https://cmte.ieee.org/comsoc-iotisc/. (Accessed on 01/14/2021).

[115] IEEE. P1951.1 - Standard for Smart City Component Systems Discovery and Semantic Exchange of Objectives. https://standards.ieee.org/project/1951_1.html. (Accessed on 01/14/2021).

[116] Carl Rhodes, Jeff Hagen, and Mark Westergren. *A strategies-to-tasks framework for planning and executing intelligence, surveillance, and reconnaissance (ISR) operations*, volume 434. Rand Corporation, 2007.

[117] Mark Masse. *REST API Design Rulebook: Designing Consistent RESTful Web Service Interfaces.* " O'Reilly Media, Inc.", 2011.

[118] Michael Gerz. Multilateral Interoperability Programme MIP Test Reference System. Technical report, FRAUNHOFER SOCIETY WACHTBERG (GERMANY) FRAUNHOFER INST FOR COMMUNICATION ..., 2009.

[119] Kyle Usbeck, Matthew Gillen, Joseph Loyall, Andrew Gronosky, Joshua Sterling, Ralph Kohler, Kelly Hanlon, Andrew Scally, Richard Newkirk, and David Canestrare. improving situation awareness with the Android Team Awareness Kit (ATAK). In *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security, Defense, and Law Enforcement XIV*, volume 9456, page 94560R. International Society for Optics and Photonics, 2015.

[120] NATO. www.natogva.org. https://www.natogva.org/. (Accessed on 01/17/2021).

[121] Openapi specification - version 3.0.3 — swagger. https://swagger.io/specification/. (Accessed on 01/17/2021).

[122] Web service definition language (wsdl). https://www.w3.org/TR/wsdl.html. (Accessed on 01/17/2021).

[123] Json. https://www.json.org/json-en.html. (Accessed on 01/17/2021).

[124] Manas Pradhan, Niranjan Suri, Christoph Fuchs, Trude Hafsoe Bloebaum, and Michal Marks. Toward an architecture and data model to enable interoperability between federated mission networks and iot-enabled smart city environments. *IEEE Communications Magazine*, 56(10):163–169, 2018.

[125] Frank T Johnsen, Trude Hafsøe Bloebaum, Marianne Rustad Brannsten, and Ketil Lund. Using open standards for utilizing iot sensors in a smart city scenario. In *International Command and Control Research and Technology Symposium (ICCRTS)*, 2018.

[126] safety days 2019 – Informationstechnologie trifft zivile Gefahrenabwehr. https://www.safetydays.de/. (Accessed on 01/07/2021).

[127] ArcGIS. About arcgis — mapping & analytics platform. https://www.esri.com/en-us/arcgis/about-arcgis/overview. (Accessed on 01/07/2021).

[128] Risklayer. http://www.risklayer.com/en/. (Accessed on 01/10/2021).

[129] AFCEA_ZuT-Forum. https://www.afcea.de/fileadmin/user_upload/Sonderveranstaltungen/Zukunfts-u._Techn.Forum/AFCEA_ZuT-Forum_-_Agenda.pdf. (Accessed on 01/10/2021).

[130] LEVIDA. https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/FraunhoferSolutionDays2020/FKIE_Projektfolder_LEVIDA_DE.pdf. (Accessed on 01/10/2021).

[131] Home - DRK e.V. https://www.drk.de/en/. (Accessed on 01/10/2021).

[132] Federated interoperability of military C2 and IoT systems. https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=564. (Accessed on 01/10/2021).

[133] Homepage - bundeswehr. https://www.bundeswehr.de/en/. (Accessed on 01/10/2021).

[134] Data protection. https://www.eda.europa.eu/Aboutus/how-we-work/data-protection. (Accessed on 01/10/2021).

[135] Paul Voigt and Axel Von dem Bussche. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 10:3152676, 2017.

[136] ROS 2 Overview. https://index.ros.org/doc/ros2/. (Accessed on 01/10/2021).

[137] Anglova. https://anglova.net/. (Accessed on 01/11/2021).

PART II: Scientific contributions

Paper A: Interoperability for Disaster Relief Operations in Smart City Environments

Manas Pradhan

In proceedings of the
5th World Forum on Internet of Things (WF-IoT), 2019
doi: 10.1109/WF-IoT.2019.8767169.

Book Chapter B: Architectural Considerations

Manas Pradhan, Christoph Fuchs, Niranjan Suri, Mauro Tortonesi and Frank T. Johnsen

Chapter from Springer Book:
Military applications of Internet of Things
Under Publication, Draft Version as of 01/02/2021.

Paper C: Toward an architecture and data model to enable interoperability between federated mission networks and IoT-enabled smart city environments

Manas Pradhan, Niranjan Suri, Christoph Fuchs, Trude Hafsoe Bloebaum and Michal Marks

In
IEEE Communications Magazine, vol. 56, no. 10, 2018
doi: 10.1109/MCOM.2018.1800305.

Paper D: Security, Privacy, and Dependability Evaluation in Verification and Validation Life Cycles for Military IoT Systems

Manas Pradhan and Josef Noll

In
IEEE Communications Magazine, vol. 58, no. 8, 2020
doi: 10.1109/MCOM.001.2000342.

Paper E: Leveraging Crowdsourcing and Crowdsensing Data for HADR Operations in a Smart City Environment

Manas Pradhan, Frank T. Johnsen, Mauto Tortonesi and Sabine Delaitre

In
IEEE Internet of Things Magazine, vol. 2, no. 2, 2019
doi: 10.1109/IOTM.001.1900013.

Paper F: Enabling Interoperability for ROS-based Robotic Devices for Smart City HADR Operations

Manas Pradhan and Sushma Devaramani

In proceedings of the
IEEE Military Communications Conference (MILCOM), 2019
doi: 10.1109/IOTM.001.1900013.

Paper G: MARGOT Dynamic IoT Resource Discovery for HADR Environments

Lorenzo Campioni, Rita Lenzi, Filippo Poltronieri, Manas Pradhan, Mauro Tortonesi, Cesare Stefanelli and Niranjan Suri

In proceedings of the
IEEE Military Communications Conference (MILCOM), 2019
doi: 10.1109/MILCOM47813.2019.9021092.

Paper H: Deployment Architecture for Accessing IoT and Legacy Assets in a Smart City Environment for Coalition HADR Operations

Manas Pradhan, Christoph Fuchs and Josef Noll

In proceedings of the
6th World Forum on Internet of Things (WF-IoT), 2020
doi: 10.1109/WF-IoT48130.2020.9221431.

Paper I: Federation based on MQTT for Urban HADR Operations

Manas Pradhan

In proceedings of the
IEEE Communications Magazine, vol. 59, no. 2, 2021

Federation based on MQTT for Urban HADR Operations

Manas Pradhan

Abstract—Today's age of Information and Communications Technologies (ICTs) in urban areas revolve around the application of Internet-of-Things (IoT) and application of IoT in Smart City constructs. IoT has enabled cheap and yet reliable ubiquitous computing for modern day ICT needs. As a result, the military community is actively looking into application of IoT for its operational needs. Federation and interoperability becomes complex for IoT implementation in the huge jungle of protocols and technologies available for IoT. This problem becomes critical in Humanitarian Assistance and Disaster Recovery (HADR) Operations where multiple agencies need to collaborate to bring quick and effective relief to disaster struck areas. Message Query Telemetry Transport (MQTT) is such an IoT-based protocol that is widely adopted in the industry for lightweight yet reliable messaging. This paper tries to provide an insight into federation based on MQTT with a prototype implementation between military and civilian ICT systems. This federation concept would enable lightweight, vendor-agnostic and interoperable message exchange while using existing information sources and preventing stove-piped systems.

Index Terms—Internet of Things, MQTT, Federation, Interoperability, HADR, Civil-military Co-operation, Smart Cities

1 Introduction

Humanitarian Assistance and Disaster Recovery (HADR) Operations in the modern-day context requires multiple agencies, from the military and the civilian domains to act together [1]. Especially in urban scenarios, where the concentration of humans makes it a very complex and challenging environment, a single emergency responder agency often does not suffice to have the required recovery impact [2]. As the modern human demographics turn towards cities, the cities are equipping themselves with modern Information and Communications Technologies (ICTs) to serve this high influx and concentration of population. Smart City concept is a step in this direction aiming to provide better governance, participation, economic possibilities, sustainable development etc. for its citizens. Internet-of-Things (IoT) has been one of the biggest enablers of the Smart City concept by providing the necessary ubiquitous and participative computing for the urban ICT needs.

IoT-based innovations in sensors, actuators, computing platforms etc. have led to their mass acceptance in the civilian and industry domains. Concepts in industry such as Industry 4.0 has shown the wide proliferation of IoT systems on the shop floor, distribution and logistics, manufacturing, computing and analytics. In the consumer industry, Smart Phones, Smart Homes, personal computing and analytics etc. have shown the path ahead for the IoT-driven market. As a result, over the years the technologies have matured for large-scale acceptance coupled with cheap production while being reliable for long-term usage. In urban settlements, networks such as 4G, 5G, Wireless Local Area Networks (WLAN), Personal Area Networks (PAN) and Low-power Wide-Area Networks (LPWAN) have provided the backend network support to realise this idea of a connected world and thus the potential of IoT in everyday lives.

For HADR operations, such IoT based innovations can be leveraged to assist the emergency responders to assist and complement their recovery efforts. Especially, considering the Smart City domain where the ICT technologies tend to be more connected and organised, the ICT assets of HADR agencies can reuse the existing cities' capabilities. The quick reaction times required from responders leads to missing capabilities, which requires collaboration with the assets available on the ground. In the North Atlantic Treaty Organization (NATO) context, Civil-Military Co-operation (CIMIC) is such a concept which tries to address this gap of bridging the civilian ground (both human and technology) assets with the military assets [3]. Further on, the specialized NATO response force (NRF) and Very High Readiness Joint Task Force (VJTF) concepts further strengthen the use-case for urban environments. These specialized operational forces need to be deployed in just a few days, at short notice, to respond to adversarial situations affecting periphery of the Alliance [4].

The IST-147 Research Task Group on Military Applications of IoT, in this corresponding direction of adoption and integration of IoT in the military domain was formed in 2016. It investigated into the emerging IoT technologies and found favorable use of COTS IoT assets for complementing the military ICT assets. With a joint experiment in 2018 with multiple NATO nations, the group showed how IoT and ICT assets from multiple nations and civilian domain can integrated in an urban HADR operation [5]. But the experiment left some open questions such as:

1) How can the multiple Command and Control (C2) systems federate with each other?
2) How can an IoT protocol be leveraged for federation between the coalition partners?
3) Which C2 systems and which interfaces from the C2 systems can be used for federation?
4) How to access the civilian data and at which granularity?

As a response to these questions, following IST-176 group was formulated to focus on federated interoperability of military C2 and IoT systems. This paper tries to provide an insight to enable this federation between the military C2 systems while interfacing the civilian ICT systems with the focus on IoT domain for future HADR operations.

The rest of the paper is organised as follows. Message Query Telemetry Transport (MQTT) protocol and the state-of-the-art related research is presented. Based on features of MQTT and latest advances in its research, a federation mechanism based on MQTT to enable multiple C2 systems' interoperability is described. The architecture and prototypical implementation to showcase the federation concept is then detailed to show how MQTT is used in a real-life use-case. Finally, the conclusion and the lessons learned is presented based on which the corresponding future work follows.

2 MQTT

MQTT is a lightweight publish/subscribe messaging transport protocol that was developed keeping the needs of IoT applications in context. It suits the needs of low-power and resource-constrained remote IoT devices and applications due to its minimal code footprint and network bandwidth utilization. It fits the unreliable nature of remote and overcrowded networks operating at the edge by allowing persistent sessions and varied Quality-of-Service (QoS) settings. Various flavors of MQTT available supported by its security features, portability and extensibility has allowed MQTT applications to be deployed on cloud, containers and into enterprise environments [6]. MQTT, in its core operates with a client-server mechanism i.e. centralized server is responsible for co-coordinating and mediating the exchange of messages between the end-point clients. All communication and exchange of messages is based on topics with the clients publish or subscribe to messages. From MQTT version 5.0 on, Earlier versions of MQTT 3.1.x used the term "broker" for the central entity responsible for message exchange between the publishers and subscribers. From MQTT 5.0 on, the term "broker" has been replaced with "server" due to the new features added and the new nature of interactions. Similarly, terms "publishers" and "subscribers" are replaced with "clients".

The NATO IST-147, IST-150 and IST-161 groups have extensively evaluated MQTT for its application in tactical and coalition operation environments [5], [7], [8]. The experiments have shown favorable results for application of MQTT for federated distributed environment settings. The following subsection 2.1 describes the state-of-the-art findings and the scope for further research.

2.1 State-of-the-Art

A comparison of Web Services (WS) Notification with MQTT was presented in [9]. WS-Notification is used as the NATO Messaging Core Service but it is not well suited to low capacity tactical networks due to its overheads. Tactical network features very closely resemble to IoT application environments, so protocols with lower overheads are always preferred in such settings. MQTT was found to offer similar functionalities as WS-Notification but with less overhead for disconnected intermittent connectivity and limited bandwidth (DIL) scenarios. But the paper showed that a centralized broker architecture which exists for WS-notification and MQTT is not a favorable set-up due to single point of failure.

In the joint experiment done by the NATO IST-147 group [5], such a centralized broker MQTT set-up was demonstrated while combining multiple coalition IoT assets and available city's ICT assets. It used a simple ontology with messages in Java Script Object Notation (JSON) format to achieve interoperability between the various data sources and the C2 applications. But it lacked a distributed inter-broker communication which would remove this single point of failure in case the central broker crashed.

In [7], MQTT with Blue Force Tracking (BTF) was presented with a federated multi-broker approach. But the implementation used again a central broker which was bridged to two other brokers. It meant that if the central broker broke down then the two bridged brokers can't communicate anymore. Furthering the idea of multi-brokers, [10] showed the evaluation of federation mechanism using multiple brokers. This paper leverages the concept extending it to application in urban HADR scenarios and exploiting some of the features provided by the federation mechanism for interoperability and flow control for Situational Awareness (SA) exchange between the HADR agencies.

2.2 MQTT V.3.x vs V.5

The implementation and prototype described in this paper leverages the new MQTT version 5.0 which replaces the Versions 3.1 and 3.0 [11]. The new version 5.0 has certain elements new both for server and client sides. These are described below which enables the deployment of a distributed masterless architecture and reducing traffic overheads:

1) Shared Subscriptions: With standard MQTT subscriptions i.e. prior to Version 5, each subscribing client received a copy of the message it subscribed to. So, if a subscription node failed then published messages were lost (QoS 0) or accumulated in the server (QoS 1, 2). The solution to this issue was to increase the subscribing nodes which resulted in large number of duplicate messages and thus lots of extra traffic. With shared subscriptions, clients that share the same subscription within a subscription group receive messages in an alternating fashion. This feature enables client load balancing since load of the same subscribed topic is distributed amongst all subscribing clients. In contested HADR and DIL environments, such mechanism allows for reducing traffic and distribution overheads.
2) Clean Start Mode: In earlier versions of MQTT, Clean Session mechanism was used by MQTT clients to have temporary connections to brokers or not subscribing to messages at all. The idea was to support offline or persistent sessions to handle connection interrupts. But the mechanism did not support the expiry of a persistent session i.e. the session never expired or deleted. With Clean Start mechanism, a session starts without using an existing session. This results in Simplified State Management i.e. the session data for a client is

discarded only when all the messages are exchanged and not because of a network failure. The expiry times for the session states can be set with Clean Start mode which allows the session state to be deleted by the server if the client does not connect within a certain time. This forces the client to reconnect to the server just to clean up session state. This reduces the server overload in DIL networks when multiple clients keep on appearing and disappearing from the network.

3) Flow Control: In a real-time environment for MQTT usage, clients and servers with different processing and connectivity levels interact and thus they have different tolerance levels for managing in-flight messages. A client can connect to multiple MQTT servers having different restrictions and management properties on the number of in-flight messages. With flow control, all involved parties do not need to negotiate in-flight windows beforehand. Dynamic message flow adjustment is used that involve heterogeneous systems and devices. It ensures that neither the server or the client overwhelm each other with message processing.
4) Bridging of Servers: Bridging of multiple servers for a distributed environment is indirectly supported in the MQTT 5.0. It calls for providing subscription options to allow for message bridge applications. It also includes an option to not send messages originating on local clients and options for retaining subscribed messages. The bridge implementations with earlier version supported a single server to be configured as bridge and all other servers acted as client servers connecting to the bridge as was used in [7]. With the new MQTT version, now multiple servers on the same hierarchy can be configured to have bridge between them.
5) Non-retransmission of MQTT messages: Earlier versions of MQTT allowed for retransmission of MQTT messages with QoS 1 and 2 in case the TCP connection broke down. In case the MQTT clients are overloaded with MQTT message processing, further duplicate or new MQTT messages deprecates its performance. With MQTT 5.0, servers and clients are not allowed to retransmit messages, but instead re-sending unacknowledged packets when the TCP connection was closed.
6) Use of zero-length string: For cases when data is published to a single topic, clients and servers can set a zero-length string in the publish message for the topic. It basically informs the client or server to use the previous topic instead of explicitly sending out the topic name. It furthers reduces the overhead in message exchange on the MQTT bus.

3 Federated HADR Operations

As described in [5], a HADR operation requires capabilities of multiple agencies to be federated. Apart from the agencies' assets, the existing assets from the cities such as the ICT assets and on ground-humans can be used to complement, bring effectiveness and precision to the operations. Concepts such as edge computing, crowdsourcing and crowdsensing further IoT enabled ICT operations [12]. In 3.1, an architecture is described to leverage these capabilities and the related implementation is described in 3.2.

3.1 Architecture

Figure 1 shows the architecture envisioned for an urban HADR operation where the federated MQTT servers provide SA data exchange between different parties. Here federation refers to the standardised and agreed ontology and thus the data exchange between the parties involved. The various components involved in the architecture are:

1) HADR Agencies' C2 Applications: HADR agencies such as the military use C2 applications to have the SA pictures of their assets, ground reports, task assignment etc. C2 applications from various agencies are designed for their use-case specific requirements. These applications support different types of operations and SA behaviour. APIs exposed by the applications are used to leverage their functionalities. Based on their interaction and use-cases, they can use either REST or SOAP based APIs to interact with their assets and external partners. Most of the HADR agencies use private APIs with API gateways such as defined in the CIMIC doctrine of NATO. For the case in-hand, we target applications based on IoT and in order to interact with IoT as well legacy assets. These APIs are bound to the MQTT clients which exchange data on behalf of the C2 application. These clients connect to the federated MQTT servers which can be associated on the same platform where the C2 application is running or at the headquarter (HQ) level.
2) HADR Agencies' ICT Applications: HADR agencies such as the military, police, fire fighters etc. have their ICT assets deployed on the ground for operations. These assets can be legacy assets such as tactical radios from the military and police, drones used for search and reconnaissance, sensors deployed at strategic areas etc. Due to the adoption of IoT, agencies are leaning towards use of IoT assets in their operations. Thus the ICT applications are getting redesigned or refactored to provide support for IoT asset integration. These ICT applications can either use APIs directly to expose their services or else bind their API functionalities to the MQTT clients. These MQTT clients can then interface the existing APIs to their topic structures and in turn connect to the federated MQTT servers provided by the agencies.
3) City ICT Applications: Cities have their own ICT infrastructures for management and governance. Their assets also include the legacy assets such as CCTV cameras, traffic sensors, network and cloud infrastructures etc. With the concept of Smart cities fast advancing cities are adopting IoT usage for their infrastructures. Concepts such as Smart Buildings which provide automated sensing and building management, Smart Traffic which provide dynamic traffic management etc. are getting revolutionized in cities. In turn, these assets expose their functionalities to the cities though their APIs. For our use-case:
   - The MQTT servers can be deployed directly by the cities which can exchange information with the other federated MQTT servers from the agencies.
   - The cities use MQTT clients to connect to the federated servers provided by the agencies.

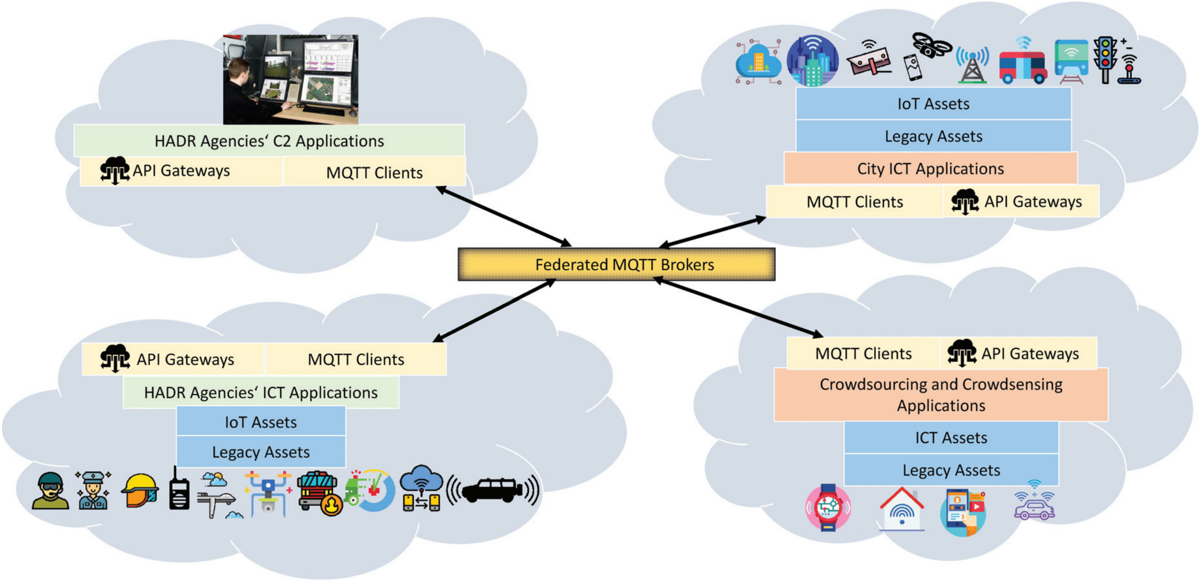


Fig. 1. Architecture for Federated MQTT-based SA Exchange for HADR Operations

- The agencies use MQTT applications which bind to the city APIs and exchange data with the servers.

4) Crowdsourcing and Crowdsensing Applications: End users and private entities are one of the biggest source of innovation in IoT. Concepts such as Smart Homes, Smart phones, Smart Watches, Smart vehicles etc. have reached out to all corners of the modern society. These crowdsourced and crowdsensed data would be the eyes of ears of the future HADR operations [12]. Citizens on the ground with their smart IoT objects can report ground SA faster and more effectively since agencies' assets are mostly overwhelmed in such operations. Many of these applications use MQTT clients to exchange data with their corresponding edge and cloud applications. This MQTT data can be directly wrapped with the interfacing MQTT topics to provide direct access to the end users' device reports. Else, the APIs from the service providers would be interfaced to the MQTT clients run by the agencies which in turn connect to the federated servers.

3.2 Implementation: Federated MQTT Brokers

The proof-of-concept (PoC) implementation for a federated MQTT server based interaction is presented in Figure 2. The term "broker" is used instead of "server" since the implementations used in the PoC presented use the term broker in theri documentation. The various components involved are:

1) C2 Application Instance 1 and 2: These C2 instances runs the Sitaware Frontline C2 application. Custom wrappers transform the data exchanged through the MQTT topics determined for interoperable data exchange. The MQTT clients used here as Mosquitto Version 5.0 clients which connect to VerneMQ brokers as in [10]. The brokers 1 and 2 are bridged to connect to each other to demonstrate the federation mechanism. In turn, broker 1 is bridged to broker 3.
2) C2 Application Instance 3: This C2 instance runs the custom developed C2 application as presented in [13]. The C2 application is based on opensource Vaadin framework and uses Openstreetmaps for showing SA data. The C2 application is bundled with an IoT-based drone controller to enable drone actuation operations. This C2 application is further interfaced with a HiveMQ Version 5.0 client and broker. The MQTT Client 5 in turn connects to broker 1 as the primary broker link and to broker 2 as the fallback broker in case broker 1 disconnects.
3) City Data Endpoint: This end point represents the city data services which are used for the HADR demonstration operations presented in 3.1. The city transport services API provides the latest SA data including the various types of events on the street network of Germany used here. Detailed traffic information regarding traffic jams and related incidents are pushed through this API. The minute details show attributes such as the location, road names, length, significance and type of delay, and distance. To represent the Crowdsourcing component in an urban HADR scenario, the ongoing COVID pandemic is used. Risklayer provides aggregated and verified crowdsourced cumulative data sets about the COVID situation in Germany [14]. Its parses through official and individual crowdsourced details such as numbers of new infections per day/week/month, deaths etc. per state, city, district and community. These details are updated daily and cross verified across multiple COVID data providers. Both: City Transport and COVID data sources expose their data sets through the determined MQTT topics and MQTT Version 5.0 publishing clients (3 and 4) which publish their data through the broker 3.

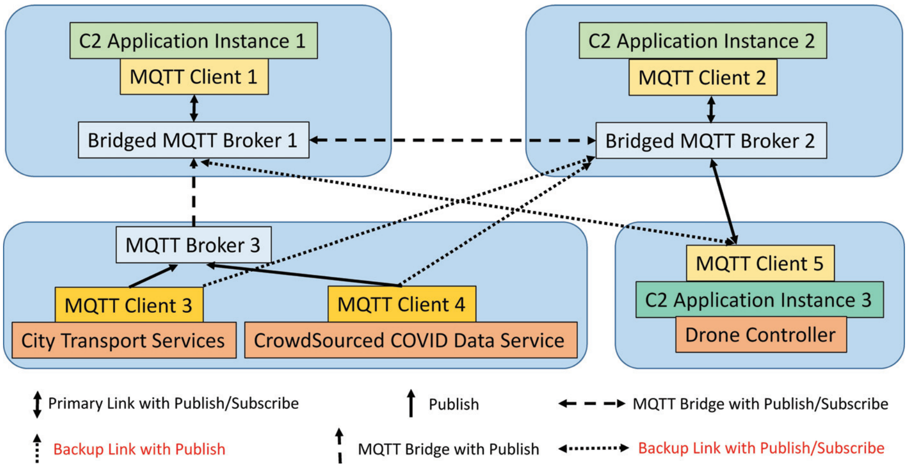


Fig. 2. Federation of C2 Systems based on MQTT-bridge for SA Exchange

3.2.1 Broker and Client Configuration

- Broker 1 and 2 are bridged to each other for all the topics both for publishing and subscription at their end points. It means that all the clients connected to broker 1 and 2 can publish and subscribe to the shared topics.
- Broker 1 is bridged to broker 3 for the topics but only for subscription. The clients 3 and 4 publish topics to the broker 3 which just forwards them to broker 1. But no topic data is sent back to the broker 3 and, clients 3 and 4.
- MQTT Clients 3 and 4 have a backup connection to broker 2 which would be used in case the link to broker 3 is lost. They can then publish their data to the bridged broker network.
- MQTT Client 5 is connected to broker 2 which publishes and subscribes to the topics determined in the network.
- All brokers require user ids and passwords for authorization.
- The brokers are configured to handle idle client connections and disconnect unresponsive ones in case they do not respond over a time interval.
- The clients too probe the brokers to check if the brokers are reachable and can publish/subscribe to their messages. In case such a check fails for a connection to a broker then they automatically switch over to the backup link to the next broker.
- Asynchronous messaging APIs are used in case of intermittent network disconnections. This enables the broker to store the messages destined for the clients for a predetermined time and deliver them if the client comes back online within the expiry timeframe.
- Topic filters are set at the bridged brokers to limit and regulate the topic data being sent out on the bridged network.

3.2.2 MQTT Topics

The MQTT topics form the base of interoperability and thus the basis for federation between the parties involved. In [5], we had demonstrated the use of simple Javascript Object Notation (JSON) based topic structures to exchange information between the coalition partners. Furthering that topic structure and using the ontology concepts defined for IoT-lite and IoT-O [15], the following describes an example topic structure and the JSON payload:

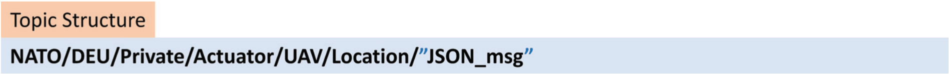
- Topic structure in figure 3 shows that a device of type actuator and sub-type drone is being held by Germany under the organisation header of NATO. The topic specifies that the topic intends to message of type "information" which in this case is the location of the drone.
- The JSON message in figure 4 contains the id of the drone "DEUDRONE1" at timestamp "2020-11-15 16:10:30.277125" and at location (50.618062, 7.12863).

As mentioned in 3.2.1, topic filters are used to limit the traffic on the brokers and thus on the clients. So, as presented in 2, the drone controller is connected to the MQTT client 5 which in turn connects to Bridged MQTT Broker 2. The topic data is directly sent over to all the subscribing parties. Or else filters are used to restrict which brokers and thus the clients are authorized to receive the location of the drone. This further helps to reduce unnecessary traffic overheads.

3.2.3 Working Use Case

The following scenario is envisioned as an example use-case to demonstrate this federation:

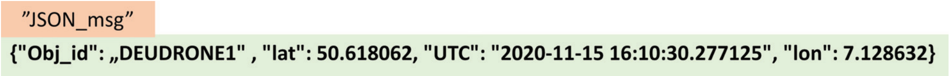
1) There is a COVID associated disaster situation in the city and the local agencies have summoned the HADR agencies to come and assist at a short notice.
2) The host country provides the city transport and COVID data service through its IoT-enabled edge computing applications and IoT radio networks.
3) The host country's NATO counterpart connects to the city infrastructure to receive the essential HADR related data provided by the city. MQTT Broker 3 connects to the Broker 1 for this purpose. The SA data is presented on the C2 Application Instance 1 running on an Armoured Personnel Carrier (APC) vehicle.
4) The invited coalition partner comes in with its assets and views the SA data on C2 application instance 2 running on a military ambulance vehicle. It establishes



Topic Structure

NATO/DEU/Private/Actuator/UAV/Location/"JSON_msg"

Fig. 3. Example of MQTT Topic Format



"JSON_msg"

{"Obj_id": „DEUDRONE1" , "lat": 50.618062, "UTC": "2020-11-15 16:10:30.277125", "lon": 7.128632}

Fig. 4. Example of JSON Message

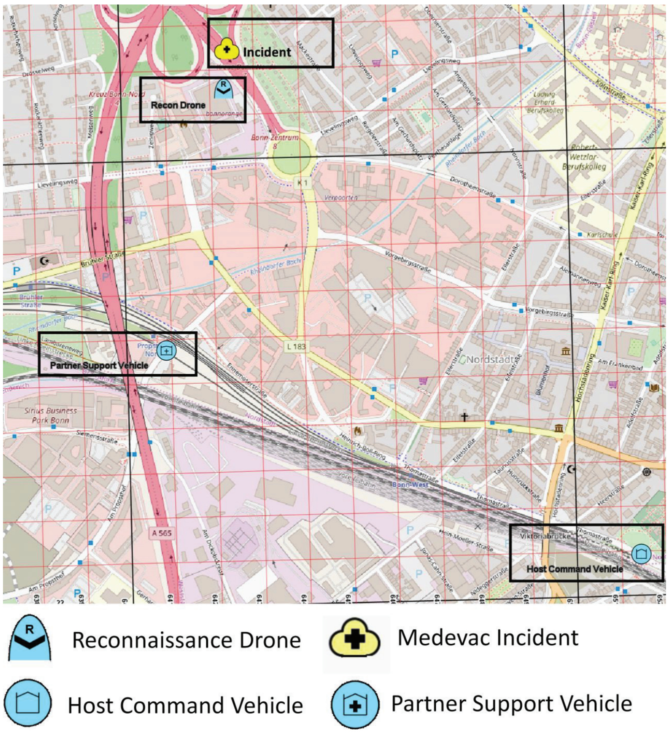


Fig. 5. C2 Status

a bridge to the host country's MQTT Broker 1 and uses pre-established topics and topic filters to exchange data. The city's MQTT Broker gets the invited partner's broker details through the host country's broker list published using MQTT topics and configures a back-up link to Broker 2.

5) A third party HADR agency such as a Non-Government Organisation (NGO) also joins the effort by providing an IoT-based drone. It has an open source based C2 application which in turns also is a drone controller running on a command vehicle. It connects directly to the Broker 2 and configures a back-up link to Broker 1.

The City Transport API used for this implementation reports fine-grained details of the incidents and their locations. Also, the COVID API reports the precise numbers for minute geographical territories. Based on this data, an incident is reported at a street periphery which needs immediate assistance:

1) The MQTT client 3 publishes this incident through the Broker 3 to the Broker 1. The C2 Application instance 1 shows the incident requiring immediate evacuation.
2) Since the Broker 1 is bridged to Broker 2, they share the topics and thus the incident is pushed to C2 Application Instance 2.
3) The vehicle from coalition partner is closer to the location of incident and thus moves to the incident location reporting its status through its shared location topic to C2 Application instance 1.
4) Coalition partner triggers a drone based surveillance of the location through the drone controller topics to provide imagery of the affected location.
5) The drone's location and imagery data (over http link [13]) is streamed to C2 Application Instance 1 and 2 along with the location of the coalition partner's vehicle. Figure 5 shows the location of the involved parties on the Sitware C2 application using the mil std. 2525b and 2525c symbols.

This working use case thus demonstrates the federation mechanism using MQTT bridging and the shared filtered topics in an emulated HADR operation .

4 Conclusion and Lessons Learned

This paper describes MQTT based bridging mechanism for federation between multiple MQTT brokers based on established ontology. It discusses the new features of MQTT which makes it even more favorable for military IoT exchange since the last versions of MQTT. It underlines the involvement of civilian and city reports as a supplement to the military Information Systems (ISs) for getting ground reports for an effective HADR operation in urban environments. It also shows how multiple C2 systems using the bridging concept, shared topics and topic filters can achieve federation and interoperability.

For the prototypical setting, the scenario plays fine but in actual scenarios, the approach might come with drawbacks. It was observed that whenever a MQTT 5.0 server tried to connect to a MQTT 3.0.x server using the MQTT 5.0 API, it returned an error saying that the protocol version is not supported. This would sure be an issue considering that many MQTT users might still be running older MQTT broker versions even though the federation through standard ontologies might exist. MQTT in its core, uses Transmission Control Protocol (TCP) based packets for MQTT data exchange. Although TCP ensures reliability, it always fairs worse in terms of latency and throughput when transmitting large and continuous data packets. Further, the bridging mechanism will always be a bottleneck w.r.t scalability of a federated system. Clustering of distributed and logically connected servers would be needed for a HADR scenario which might involve large number of connected clients creating huge amount of network traffic.

5 Future Work

As future work, we are setting up a federated testbed where the coalition partners can test out this federation mechanism and carry further measurements for application of MQTT brokers in tactical environments. The new spiral for FMN is also trying to underline the concept of CIMIC by incorporating civilian standards for data exchange for future civil-military collaboration. This proof-of-concept would be further developed to incorporate wrappers for military and civilian data exchange to provide a real-time emulation of CIMIC. The current implementation does not involve encrypting the MQTT transmission which will be extended in the future. Further, authentication and authorization mechanisms would be tested out supported by MQTT 5.0 enhancements. The concept of creating virtual distributed clusters would be tested to address the scalability issue of the bridging mechanism. Finally, serverless solutions based on UDP would be experimented to circumvent the fallacies of MQTT TCP packets.

References

[1] F. T. Johnsen, Z. Zieliński, K. Wrona, N. Suri, C. Fuchs, M. Pradhan, J. Furtak, B. Vasilache, V. Pellegrini, M. Dyk *et al.*, "Application of IoT in military operations in a smart city," in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE, 2018, pp. 1–8.

[2] N. Suri, Z. Zielinski, M. Tortonesi, C. Fuchs, M. Pradhan, K. Wrona, J. Furtak, D. B. Vasilache, M. Street, V. Pellegrini *et al.*, "Exploiting smart city IoT for disaster recovery operations," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. IEEE, 2018, pp. 458–463.

[3] K. Wrona, M. Pradhan, M. Tortonesi, S. Niranjan *et al.*, "Civil-military collaboration in smart environments under adversarial conditions," in *The First International Workshop on Internet of Things for Adversarial Environments (in conjunction with IEEE INFOCOM 2019)*. IEEE, 2019, pp. 1–6.

[4] C. Cucos, "Very high readiness joint task force-a new concept of NATO," in *International Scientific Conference "Strategies XXI"*, vol. 2. Bucharest: "Carol I" National Defence University, 2015, pp. 196–201.

[5] M. Pradhan, N. Suri, C. Fuchs, T. H. Bloebaum, and M. Marks, "Toward an architecture and data model to enable interoperability between federated mission networks and IoT-enabled smart city environments," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 163–169, 2018.

[6] C. Pahl, S. Helmer, L. Miori, J. Sanin, and B. Lee, "A container-based edge cloud paas architecture based on raspberry pi clusters," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. IEEE, 2016, pp. 117–124.

[7] M. Manso, B. Guerra, F. Freire, N. Jansen, K. Chan, A. Toth, T. H. Bloebaum, and F. T. Johnsen, "Mobile tactical forces: Experiments on multi-broker messaging middleware in a coalition setting," in *2019 24th International Command and Control Research and Technology Symposium (ICCRTS) proceedings*. ICCRTS, 2019.

[8] N. Suri, M. R. Breedy, K. M. Marcus, R. Fronteddu, E. Cramer, A. Morelli, L. Campioni, M. Provosty, C. Enders, M. Tortonesi *et al.*, "Experimental evaluation of group communications protocols for data dissemination at the tactical edge," in *2019 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE, 2019, pp. 1–8.

[9] F. T. Johnsen, L. Landmark, M. Hauge, E. Larsen, and Ø. Kure, "Publish/subscribe versus a content-based approach for information dissemination," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 2018, pp. 1–9.

[10] F. T. Johnsen, M. Manso, and N. Jansen, "Evaluation of message broker approaches for information exchange in disadvantaged tactical networks in a federated environment," in *2020 25th International Command and Control Research and Technology Symposium (ICCRTS) proceedings*. ICCRTS, 2020.

[11] A. Banks, E. Briggs, K. Borgendale, and R. Gupta, "Mqtt version 5.0," *OASIS Standard*, vol. 7, 2019.

[12] M. Pradhan, F. T. Johnsen, M. Tortonesi, and S. Delaitre, "Leveraging crowdsourcing and crowdsensing data for HADR operations in a smart city environment," *IEEE Internet of Things Magazine*, vol. 2, no. 2, pp. 26–31, 2019.

[13] M. Pradhan and S. Devaramani, "Enabling interoperability for ros-based robotic devices for smart city hadr operations," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. IEEE, 2019, pp. 1–6.

[14] S. Fuchs and J. I. Daniell, "„corona hotspots tagesaktuell & weltweit“," 2020.

[15] F. Sivrikaya, N. Ben-Sassi, X.-T. Dang, O. C. Görür, and C. Kuster, "Internet of smart city objects: A distributed framework for service discovery and composition," *IEEE Access*, vol. 7, pp. 14 434–14 454, 2019.

Manas Pradhan is a PhD fellow at the Department of Technology Systems, University of Oslo and the Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE, Germany. He received his Bachelor's degree in Computer Science and Engineering from the Institute of Technical Education & Research, Bhubaneswar, India, in 2009. He worked as a Software Engineer before commencing Masters in Media Informatics from RWTH Aachen University, Aachen, Germany. His research interests lie in the area of military interoperability, Internet-of-Things technologies and Smart Cities.

PART III: Appendices

V List of acronyms

Acronyms	**Full-form**
6LoWPAN	6 Low Power Wireless Personal Area Network
AMQP	Advanced Message Queuing Protocol
AOO	Area of Operations
API	Application Programming Interface
AR	Action Research
ARL	Army Research Labs
ATAK	Android Tactical Assault Kit
AWS	Amazon Web Services
BYOD	Bring Your Own Device
C2	Command and Control
CAGED	Communication Application with Geographical Element Data
CIMIC	Civil-Military Co-operation
CoAP	Constrained Application Protocol
COTS	Commercial-off-the-Shelf
COVID	Coronavirus
CRM	Computing Research Methods
CS	Case Study
CSIS	Center for Strategic and International Studies
CSS	Chirp Spread Spectrum
DA	Discovery Agent
DDS	Data Distribution Service
DRK	Deutsches Rotes Kreuz
EA	Enterprise Architecture
EMANE	Extensible Ad-hoc Networking Emulator
ES	Exploratory Survey
ETSI	European Telecommunication Standards Institute

EI	Enterprise Integration
EU	European Union
FE	Field Experiment
FMN	Federated Mission Networking
FTA	Finnish Transport Agency
GPS	Global Positioning System
GPU	Graphical Processing Unit
HADR	Humanitarian Assistance and Disaster Recovery
HTTP	Hypertext Transfer Protocol
HTTPs	HTTP Secured
IaaS	Infrastructure as a Service
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
I/O	Input/Output
IIoT	Industrial IoT
IMRAD	Introduction, Method, Results and Discussion
IP	Internet Protocol
IoBT	Internet of Battlefield Things
IoT	Internet of Things
IoMT	Internet of Medical Things
ISM	Industrial, Scientific, and Medical
IST	Information Systems Technology
IT	Information Technology
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
LoRaWAN	Long Range Wide Area Network
LR-WPAN	Low-rate Wireless Personal Area Networks
LTE	Long Term Evolution
M2M	Machine-to-Machine
MARGOT	Multi-domain Asynchronous Gateway Of Things
MCU	Microcontroller
MIM	Multilateral Interoperability Programme Information Model
MIP	Multilateral Interoperability Programme

MONICA	Management of Networked IoT Wearables Very Large-Scale Demonstration of Cultural and Societal Application
MQTT	Message Queuing Telemetry Transport
MTOC	Mobile Tactical Operation Centre
NEC	Network-enabled Capability
NFC	Near Field Communication
NGO	Non-government organisation
NATO	North Atlantic Treaty Organization
NGVA	NATO Generic Vehicle Architecture
OAS	OpenAPI Specification
OT	Operational Technology
PAN	Personal Area Networks
PKI	Public Key Infrastructure
PaaS	Platform as a Service
PoC	Proof-of-Concept
PoI	Points-of-Interest
QoI	Quality of Information
QoS	Quality of Service
RAS-G	Robotics and Autonomous Systems Ground
REST	Representational State Transfer
RFID	Radio-frequency Identification
ROS	Robot Operating System
RPL	Low-Power and Lossy Networks
RTG	Research Task Group
SA	Situation Awareness
SAREF	Smart Appliances REFerence
SDN	Software-defined Networking
SHIELD	European Security in Health Data Exchange
SOA	Service-Oriented Architecture
SPD	Security, Privacy, and Dependability
SPF	Sieve Process Forward
SSL	Secure Sockets Layer
STO	Science and Technology Organisation

TCP	Transmission Control Protocol
THW	Technisches Hilfswerk
TOC	Tactical Operations Center
TSCH	Time Slotted Channel Hopping
TLS	Transport Layer Security
ISR	Intelligence, Surveillance, and Reconnaissance
WSDL	Web Service Description Language
WSN	Wireless Sensor Network
WWW	World Wide Web
UDP	User Datagram Protocol
UN	United Nations
US	United States
V&V	Verification and Validation
VoI	Value of Information
XML	Extensible Markup Language