TECHNISCHE
UNIVERSITÄT
DARMSTADT

SECURE DEVICE-TO-DEVICE COMMUNICATION FOR EMERGENCY RESPONSE

Vom Fachbereich Informatik
der Technische Universität Darmstadt
genehmigte

DISSERTATION

zur Erlangung des akademischen Grades
Doktor-Ingenieurin (Dr.-Ing.)

von

FLOR MARÍA ÁLVAREZ ZURITA, M. SC.

Erstreferent: Prof. Dr.-Ing. Matthias Hollick
Korreferent: Prof. Dr. Andreas Mauthe

Darmstadt 2020
Hochschulkennziffer D17

Flor María Álvarez Zurita, *Secure Device-to-Device Communication for Emergency Response*, Dissertation, Technische Universität Darmstadt, 2020.

Fachgebiet Sichere Mobile Netze
Fachbereich Informatik
Technische Universität Darmstadt
Jahr der Veröffentlichung: 2020
Tag der mündlichen Prüfung: 21. Februar 2020
URN: urn:nbn:de:tuda-tuprints-114864

"It is impossible to live without
failing at something.
Unless you live so cautiously that
you might as well not have lived at all,
in which case, you fail by default."
– J.K. Rowling.

Dedicated to the loving memory of my parents. Although they are no longer in this world, I still feel their presence in every step I follow. I also want to dedicate this work to my family and friends in Ecuador. The distance and time have not diminished the love and appreciation I have for all of you.

Especialmente dedicado a Jonilu y Tobi.

ABSTRACT

Mobile devices have the potential to make a significant impact during disasters. However, their practical impact is severely limited by the loss of access to mobile communication infrastructure: Precisely, when there is a surge in demand for communications from people in a disaster zone, this capacity for communications is severely curtailed. This loss of communications undermines the effectiveness of the many recent innovations in the use of smartphones and similar devices to mitigate the effects of disasters.

While various solutions have been proposed, e. g., by having handsets form wireless ad hoc networks, none are complete: Some are specific to certain mobile operating systems or operating system versions. Others result in unacceptably increased energy consumption, flattening the batteries of phones at a time when users need to conserve energy due to the loss of access to opportunities to recharge their mobile devices. Realistic user behaviour, including patterns of movement and communications, are also rarely addressed. Further, security is rarely considered in a comprehensive and satisfying manner, leaving users exposed to a variety of potential attacks.

Thus there is a compelling need to find more effective solutions for communications, energy management, and security of mobile devices operating in disaster conditions.

To address these shortcomings, this thesis provides a suite of comprehensive solutions that contribute to facilitate secure device-to-device communication for emergency response. This thesis works to solve these problems by: *(i)* Conducting a large-scale field-trial to understand and analyze civilians' behaviour during disaster scenarios; *(ii)* Proposing a practical, lightweight scheme for bootstrapping device-to-device security, that is tailored for local urban operations representative of disaster scenarios; *(iii)* Realizing novel energy management strategies for the neighbour discovery problem, which deliver significant energy savings in return for only a minimal reduction in neighbour discovery efficiency; *(iv)* The description of novel concepts for using devices in a smart city environment that remain functional following a disaster to support communications among mobile devices.

In short, this thesis adds considerably to the understanding of the difficulties in the formation of direct device-to-device communications networks composed primarily of civilians' mobile devices, and how several facets of this problem can be mitigated. Several of the proposed enhancements are also implemented. Thus, this thesis also takes essential steps in the direction of realizing such solutions to

demonstrate their feasibility on real devices, intending to improve the tools available to civilians post-disaster.

ZUSAMMENFASSUNG

Mobile Endgeräte, wie beispielsweise Smartphones, haben ein enormes Potential in Katastrophensituationen eine wichtige Rolle als Werkzeug für Einsatzkräfte und die Zivilbevölkerung zu spielen. Durch den Wegfall der Mobilfunkinfrastruktur, der häufig mit Katastrophen einhergeht, werden die praktischen Einsatzmöglichkeiten dieser Geräte jedoch drastisch reduziert. Gerade in diesen Situationen, in denen ein immenser Kommunikationsbedarf bei den Personen im Katastrophengebiet besteht, ist die Kommunikationsfähigkeit eingeschränkt oder nicht vorhanden. Dies hebelt viele der Innovationen und des technischen Fortschrittes der letzten Jahre aus, die diese Geräte in einer solchen Situation so wertvoll machen könnten, die Auswirkungen der Katastrophe zu mindern.

Es gibt verschiedenste Konzepte und Lösungsvorschläge die eine direkte Kommunikation zwischen den Endgeräten ermöglichen und diese somit unabhängig von der Mobilfunkinfrastruktur werden lassen. Keine dieser Lösungen greift jedoch vollumfänglich in unserem Katastrophenszenario. So sind einige nur auf spezifischen mobilen Betriebssystemversionen verfügbar, andere führen hingegen zu unannehmbarem Energieverbrauch, in einer Situation in der Energiesparen häufig hohe Priorität hat. Andere basieren auf der individuellen Anpassung eines Betriebsystems oder benötigen Root-Zugriffsrechte und sind daher nicht praktikabel auf handelsüblichen Smartphones einzusetzen. Außerdem werden Fragen der Sicherheit nicht umfassend und zufriedenstellend gelöst und der Nutzer sieht sich daher einer Vielzahl potentieller Angriffe ausgesetzt. Zur Optimierung einer Lösung auf ein Katastrophenszenario sollte ebenfalls das Verhalten der betroffenen Bevölkerung einschließlich deren Bewegungs- und Kommunikationsmuster berücksichtig werden. Daraus lässt sich ableiten, dass hier noch ein offenes Forschungsfeld besteht, um den hohen Bedarf an eine angepasste und maßgeschneiderte Kommunikationslösung für Katastrophenfälle, die die zuvor angesprochenen Aspekte adressiert, zu decken.

Diese Arbeit liefert eine Sammlung von Lösungen und Konzepten die dazu beitragen, eine sichere direkte Geräte-zu-Geräte Kommunikation für Notfallmaßnahmen im Katastrophenfall bereitzustellen. Den zuvor angesprochen Problemen wird sich durch folgenden Beiträge dieser Arbeit angenommen: *(i)* Die Durchführung eines groß angelegten Feldversuches, um das Verhalten von Zivilisten während einer Katastrophe zu verstehen und zu beschreiben; *(ii)* Den Vorschlag eines praktikablen und leichtgewichtigen Konzeptes zur Inbetriebnahme einer sicheren direkten Kommunikation zwischen Smartphones, die auf lokale urbane Katastrophenszenarien zugeschnitten ist; *(iii)* Der Reali-

sierung neuer Strategien zum Energiemanagement für das Problem der Nachbarschaftserkennung, welche signifikante Energieeinsparung bieten bei nur minimaler Effizienz-Reduktion der Nachbarschaftserkennung; *(iv)* Eine Beschreibung eines neuartigen Konzeptes, welches es ermöglicht, im Katastrophenfall funktional gebliebene Endgeräte in einer Smart City Umgebung zur Unterstützung der mobilen Kommunikation einzusetzen.

Zusammenfassend trägt diese Arbeit wesentlich zum Verständnis bei, welche Problemstellung bei der Bildung von Geräte-zu-Geräte Kommunikationsnetzwerken, die hauptsächlich aus Endgeräten der Zivilbevölkerung gebildet werden, bestehen. Des Weiteren wird aufgezeigt, wie diese Probleme überwunden oder zumindest auf ein akzeptables Maß reduziert werden können. Eine Reihe der vorgeschlagenen Konzepte sind bereits implementiert und demonstrieren deren Machbarkeit auf echten Endgeräten. Damit geht diese Arbeit einen wichtigen Schritt in Richtung der Realisierung einer Lösung und versucht der Bevölkerung verbesserte Werkzeuge unmittelbar nach einem Katastrophenfall an die Hand zu geben.

ACKNOWLEDGMENTS

I would like to use the following lines to thank the persons who have actively accompanied me the last years on my way to this thesis, without the participation and support of so many, this work would not have been possible.

First of all I would like to sincerely thank my supervisor Prof. Dr.-Ing. Matthias Hollick for his trust, continued support and helpfulness during all these years.

I would like also to express my thanks to my co-supervisor Prof. Dr. Andreas Mauthe for accepting review this thesis and his invested time and valuable feedback.

Special thanks goes to Prof. Dr. Paul Gardner-Stephen for his stimulating exchange of ideas, insights into his vast experience in this field, and his unconditional willingness to help.

Furthermore, I would like to thank the German Federal Ministry of Education and Research (BMBF) within the SMARTER project and the Federal State of Hesse for funding my work.

I would like to thank all my colleagues for the pleasant working atmosphere, in particular, Lars Baumgärtner, Milan Stute and Jiska Classen for their feedback on this thesis, Lars Almon and Patrick Lieser for their collaboration and discussing ideas for several papers. I thank Doris Müller for her support as well as all my students for their contributions. Especially I thank Max, Tobias and Hauke.

Finally, I would like to express my deepest gratitude and love to Tobias for supporting me in all the years of my studies.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

APDU	Application Protocol Data Unit
AWDL	Apple Wireless Direct Link
BBK	Germany Federal Office for Civil Protection and Disaster Relief
BLE	Bluetooth Low Energy
BT Mesh	Bluetooth Mesh
BlueMergency	Bluetooth Mesh emErgency
C2C	Civilian-to-Civilian
C2R	Civilian-to-Responders
D2D	Device-to-Device
DTN	Delay Tolerant Network
DigiDOC	Digital Operations Center
ECDSA	Elliptic Curve Digital Signature Algorithm
ECS	Emergency Communication System
FEMA	Federal Emergency Management Agency
FOKUS	Fraunhofer Institute for Open Communication Systems
GATT	Generic Attribute Profile
GPS	Global Positioning System
HF	High Frequency
IBSS	Independent Basis Service Set
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
JSON	JavaScript Object Notation
LoS	Line-of-Sight
M2M	Machine-to-Machine
MANET	Mobile Ad Hoc Network
ND	Neighbour Discovery
NFC	Near-Field Communication
NGO	Non-governmental Organization
NINA	Emergency Information and Messaging App
ONE	Opportunistic Network Simulator
OPPNET	Opportunistic Networks
OoB	Out-of-Band

PGP	Pretty Good Privacy
R2C	Responders-to-Civilian
RSA	Rivest-Shamir-Adleman
SBD	Short-Burst-Data
SIESTA	SavIng Energy in STAtic Phases
SIG	Special Interest Group
SIM	Subscriber Identity Module
SMARTER	Smartphone-based Communication Networks for Emergency Response
SMS	Short Message Service
SSID	Service Set IDentifier
SoL	Sea of Lights
TETRA	Terrestrial Trunked Radio
UHF	Ultra High Frequency
VHF	Very High Frequency
WoT	Web-of-Trust

PREVIOUSLY PUBLISHED MATERIAL

This thesis includes material of published conference and workshop papers. Table 0.2 summarizes the publications considered in each chapter.

Table 0.2: Previously published material

	[1]	[2]	[3]	[4]	[5]	[6]
Part I: Introduction						
Chapter 1	☑	☑	☑	☑	☑	☑
Chapter 2	☑					
Part II: Analyzing Smartphone-based Emergency Communication Systems						
Chapter 3	☑	☑				
Chapter 4			☑			
Part III: Improving the Resilience of Smartphone-based Emergency Communication Systems						
Chapter 5				☑		
Chapter 6					☑	
Chapter 7						☑
Part IV: Conclusions and Outlook						
Chapter 8	☑	☑	☑	☑	☑	☑

Following the regulations of the Department of Computer Science at Technische Universität Darmstadt, I detail below the chapters which include verbatim and rephrased fragments from these publications. The complete list of my publications, including those out of the scope of this thesis, is presented on Pages 141 and 142.

CHAPTER 1 builds upon "Maintaining both Availability and Integrity of Communications: Challenges and Guidelines for Data Security and Privacy During Disasters and Crises" [1] and "Architecture for Responsive Emergency Communications Networks" [2]. Besides, it includes verbatim fragments from "Conducting a Large-scale Field Test of a Smartphone-based Communication Network for Emergency Response" [3]. Additionally, this section revises "Sea of Lights: Practical Device-to-Device Security Bootstrapping in the Dark" [4], "Siesta:

Smart Neighbor Discovery for Device-to-Device Communications", a work currently under submission [5], and "Bluemergency: Mediating Post-disaster Communication Systems using the Internet of Things and Bluetooth Mesh" [6].

CHAPTER 2 builds upon "Maintaining both Availability and Integrity of Communications: Challenges and Guidelines for Data Security and Privacy During Disasters and Crises" [1].

CHAPTER 3 Sections 3.2, 3.3 and 3.5 include verbatim fragments from "Maintaining both Availability and Integrity of Communications: Challenges and Guidelines for Data Security and Privacy During Disasters and Crises" [1]. Sections 3.2 to 3.4 build upon "Architecture for Responsive Emergency Communications Networks" [2].

CHAPTER 4 includes verbatim fragments from "Conducting a Large-scale Field Test of a Smartphone-based Communication Network for Emergency Response" [3]. Furthermore, it extends results from the Master thesis [7] of Yannick Dylla.

CHAPTER 5 includes verbatim fragments from "Sea of Lights: Practical Device-to-Device Security Bootstrapping in the Dark" [4]. Besides, it includes data obtained in the Master thesis [8] of Max Kolhagen.

CHAPTER 6 includes verbatim fragments from "Siesta: Smart Neighbor Discovery for Device-to-Device Communications", a work currently under submission [5]. Moreover, it extends results obtained in the Master thesis [9] of Tobias Schultes.

CHAPTER 7 includes verbatim fragments from "Bluemergency: Mediating Post-disaster Communication Systems using the Internet of Things and Bluetooth Mesh" [6].

CHAPTER 8 builds upon "Maintaining both Availability and Integrity of Communications: Challenges and Guidelines for Data Security and Privacy During Disasters and Crises" [1] and "Architecture for Responsive Emergency Communications Networks" [2]. Besides, it includes verbatim fragments from "Conducting a Large-scale Field Test of a Smartphone-based Communication Network for Emergency Response" [3]. Additionally, this section revises "Sea of Lights: Practical Device-to-Device Security Bootstrapping in the Dark" [4], "Siesta: Smart Neighbor Discovery for Device-to-Device Communications", a work currently under submission [5], and "Bluemergency: Mediating Post-disaster Communication Systems using the Internet of Things and Bluetooth Mesh" [6].

COLLABORATIONS

The publications mentioned above arise from collaborations with colleagues and international partners. Their content is the result of the valuable exchange of ideas and discussions among all authors, where each author contributed with his particular strengths. In this context and as far as possible, the following part is dedicated to describe and differentiate the contribution of each author.

Part 1. Analysis of Smartphone-based Emergency Communication Systems

The collaboration with several responder organizations during the Smartphone-based Communication Networks for Emergency Response (SMARTER) project allowed us to have a better understanding of post-disaster systems and their requirements. The description and summary of post-disaster systems and their requirements in Sections 3.2 to 3.4 were a joint work with P. Lieser, P. Gardner-Stephen and M. Hollick. Together with P. Lieser, I performed the analysis of the information services, the stakeholders and the requirement for post-disaster smartphone-based systems. My focus was the services, security and communications technologies, while P. Lieser focused mainly on the data management and prioritization mechanisms. P. Gardner-Stephen and M. Hollick contributed with valuable ideas and expertise on post-disaster systems.

The system model, threat model and security requirements for post-disaster communication systems as described in Section 3.5 was formulated during the visit of P. Gardner-Stephen at TU Darmstadt in 2016. I contributed by analyzing plausible threats from contemporary disaster and crisis events and discussed the security and privacy features of state-of-the-art communications mechanisms. While P. Gardner-Stephen contributed with its expertise in the definition of the principal risks and challenges that may arise during disasters, I defined practical guidelines for mitigating these risks. M. Hollick supported me with valuable comments and suggestions for possible security requirements.

In the context of the SMARTER project, a large-scaled field test of smartphone-based emergency communication systems was performed. Together with L. Almon, P. Lieser, T. Meuser and B. Richerzhagen, I carried-out the device configuration of each smartphone for the field test. L. Almon, P. Lieser, T. Meuser and B. Richerzhagen supported me configuring the tools for the data collection on each device. Our data analysis in Chapter 4 is based on the Master thesis of Y. Dylla that M. Hollick and L. Almon supervised. Y. Dylla developed the python scripts to handle all the gathered data, and provided a first

analysis of these data. Afterward, I did some improvements in the data processing, including the data validation and cleaning, and the presentation of our results for publication.

Part 2. IMPROVING THE RESILIENCE OF SMARTPHONE-BASED EMERGENCY COMMUNICATION SYSTEMS

Our first contribution for improving the resilience of Smartphone-based Emergency Communication Systems described in Chapter 5 was a decentralized authentication and key management solution. It is based on the Master thesis of M. Kolhagen that M. Hollick and I supervised. I started with the idea of using secure elements for a decentralized authentication and key management and proposed a topic for a master thesis. M. Kolhagen implemented such a system for Android devices based on the Web-of-Trust (WoT) concept. He also provided an evaluation using both simulations and real devices. I extended the simulation evaluation integrating the system into the ONE [10] simulator. I also revised the write-up that leads to our publication.

Our efficient neighbour discovery scheme for emergency communication systems in Chapter 6 was developed as part of the Master thesis of T. Schultes that M. Hollick and I supervised. Following my idea to adapt the neighbour discovery scheme for saving energy consumption in opportunistic networks, he developed the neighbour discovery scheme. He also provided an evaluation using both simulations and real devices. Later, I did some improvements of the implementation and extended the experiments including several movement models. I also revised the write-up that leads to our publication.

Finally, our concept of the integration of existing Internet of Things (IoT) solutions into post-disaster system in Chapter 7 was a joint work with L. Almon, H. Radtki and M. Hollick. I developed the concept, the practical measurements and the analysis of our proof-of-concept evaluation, while H. Radtki supported me by the development of our proof-of-concept as a smartphone application for Android devices. L. Almon contributed the technical configuration and set up the hardware for the experiments in the smart office scenario.

Part I

INTRODUCTION

Chapter 1 presents the goals, challenges and contributions of this thesis. Chapter 2 provides background information and related work about existing Emergency Communication Systems.

1 INTRODUCTION

The ubiquity of personal mobile devices, as well as their communication capabilities, e. g., Bluetooth or Wi-Fi, sensing functionality, and computational power, have led to their widespread use [11]. The number of mobile device users already exceeds five billion worldwide and is expected to continue growing. It is estimated that by 2023, the number of mobile devices grows to more than sixteen billion [12]. The majority of the population owns a mobile device to call, send messages, use mobile apps, or surf the Internet. In addition, there are already areas where these mobile devices have become an indispensable part of everyday life. For instance, the tendency of payments has changed in the last years from physical wallets to almost digital wallets such as contactless payment using Apple Pay, Google Pay. Also, mobile devices have shown to be very useful in several scenarios. The numerous sensors present in a smartphone, e. g., gyroscope, accelerometer, or proximity sensors, represent powerful tools to deal with a multitude of tasks. For instance, by including user's input and device mobility, they allow systems to collect and share environmental data more flexibly [13]. Furthermore, they feature decentralized connectivity that enables new communication paradigms, e. g., Device-to-Device (D2D) communication using Bluetooth, Wi-Fi, or other communication technology that supports a direct connection between devices.

Mobile devices have become an indispensable part of everyday life.

The ubiquity of mobile phones, as well as their communication capabilities enable new communication paradigms.

Nowadays, information and communication systems heavily rely on third-party providers to offer underlying security and communication services. These systems are commonly designed in a centralized fashion and scale to billions of users. However, if these centralized services are disrupted or overloaded due to natural or human-made disasters [14], large scale blackouts [15], or country-wide censorship [16], the users are left without practical solutions to establish secure communications using their mobile devices. For example, several cloud-based solutions assume the existence of a centralized trust party authority, e. g., a Public Key Infrastructure (PKI), which is responsible for key binding to user identities and validation of digital certificates. Hence, mobile application usage is severely restricted to support users' authentication in such scenarios.

Mobile applications heavily rely on third-party providers to offer basis security services.

Consequently, the use of smartphones for building self-organizing Mobile Ad Hoc Networks (MANETs) based on Delay Tolerant Networks (DTNs) has emerged in recent years [17, 18]. Such networks have two key strengths that make them well-suited to enable post-disaster communications: First, they are easily adaptable and allow users to communicate in a D2D manner, without the need for any fixed

Self-organizing mobile ad hoc networks are well-suited to enable post-disaster communications.

or conventional infrastructure, or end-to-end connectivity. Second, by taking advantage of human mobility, it is possible to exchange data opportunistically and also to reach places with a high concentration of nodes that become communication islands in partitioned networks.

IoT technology can aid to compensate scarce infrastructure.

Recent efforts also include the Internet of Things (IoT) technology for compensating against scarcity of infrastructure [19]. The rapidly growing IoT technology offers the possibility to improve post-disaster networks based on smartphones. According to [20], the number of connected IoT sensors will increase to almost 50 billion units by 2030. There is a wide range of real-life smart environments [21], from smart cities [22] to industrial operations [23]. Many of these IoT devices are battery powered and can aid in mediating communications in an emergency network.

1.1 MOTIVATION

Disasters leave the population in a very exposed situation, especially in terms of communication possibilities. A common characteristic after a disaster is the loss of mobile telecommunication capability [24]. By considering the growing interdependent character of critical infrastructures, a communication outage also means a serious restriction on daily activities [25, 26]. If the central communication infrastructure is not available, even simple routines such as buying gasoline, food, water, etc., would be either limited or impossible. For this reason, in the last decade self-organized and resilience concepts have become more and more important in networking systems [27, 28]. Thus, it is necessary to integrate mechanisms that allow an acceptable level of communication to cope in the absence of infrastructure [25]. Such mechanisms, for example, may deal with security features to counter potential threats. They may provide the self-organizing capability to build systems more adaptable and relocatable.

Post-disaster communication systems can provide an additional or backup communication channel.

In this thesis, the term resilience refers to the definition proposed by the authors in [26] as follows:

Definition 1. *Resilience: "Resilience of a communication network is its ability to maintain the same level of functionality in the face of internal changes and external disturbances as a result of large-scale natural disasters and corresponding failures, weather-based disruptions, technology-related disasters, and malicious human activities."*

In the context of crisis, civilians typically do not possess their own dedicated communications capacity, in contrast to many established relief organizations. Responders and civilians, however, can use different technologies, e. g., Bluetooth, Wi-Fi direct, or two-way radio, to communicate after a disaster. Thus, they can spontaneously build communication networks using their mobile devices to communicate with each other [29–31], as illustrated in Figure 1.1.

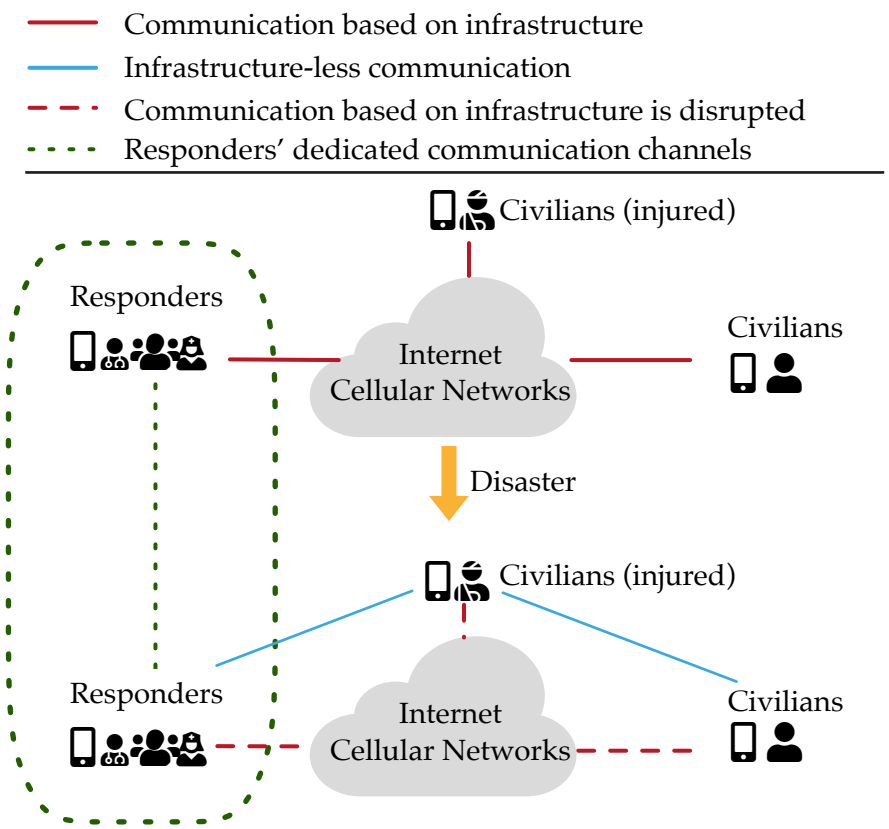


Figure 1.1: Self-organizing post-disaster systems using smartphones to facilitate the communication between civilians as well as between civilians and responders.

Most self-organizing post-disaster systems lack practical implementations.

While these post-disaster communication systems may not adequately replace cellular communication infrastructure, they can provide an additional or backup communication channel. Recent studies [17, 18, 31] have shown that post-disaster systems based on self-organizing MANETs are beneficial in dealing with the impact of the loss of communication or failures in the infrastructure emerging during a disaster. Since the validation of these systems under real conditions is a complex issue and, in most cases, not possible, several approaches use simulation to evaluate the performance of their system [17]. Using simulations based on synthetic models or trace-based models from everyday movement has the advantages of reproducability and flexibility. However, such simulations require understanding of the characteristics of human behaviour and their requirements in the aftermath of a disaster. Besides, systems tested only using simulation experiments may not be feasible under real-world conditions as they need to deal with real-world obstacles, transmission interference, as well as processing time in real devices.

Many solutions [32–35] provide a mobile application that allows civilians to gather information and report infrastructure problems

Practical decentralized solutions to bootstrap security on mobile devices are still missing.

after a disaster, request help, or send their location coordinates to enable rescue forces to find them. While these approaches deal with message routing, forwarding, and spreading in the affected area, they still lack practical decentralized solutions to bootstrap security on mobile devices. Most of these approaches either rely on a centralized organization to provide security credentials and user authentication, or focus on providing solely network layer security [36, 37].

Also, according to [38], the power requirements of D2D communications may severely limit the use of such networks in real-world situations. Many existing ad hoc network solutions [39–42] already propose methods to save energy, e. g., during the neighbour discovery phase. Nevertheless, most of the solutions on real devices focus mainly on a single communication technology, without using any modular design.

Many existing post-disaster systems need special hardware, custom kernels or software modifications.

In recent years, wireless sensor networks have become increasingly crucial for supporting post-disaster systems based on self-organizing MANETs [43]. However, most of these solutions need special hardware, custom kernels, or software modifications, e. g., rooting (Android) or jail-breaking (iOS) of smartphones. In this work, we concentrate on communication tools that ordinary civilians can make use of in the wake of disasters, aiming to optimize direct D2D communication.

1.2 GOALS AND CHALLENGES

The main goal of this thesis is to optimize communication between civilians in the event of disasters.

The main goal of this thesis is to contribute to the design and deployment of secure D2D communication for emergency communication systems. Despite the advantages as mentioned above of mobile devices, post-disaster networks based on smartphones also involve new challenges. Mainly, it is necessary to *(i)* investigate how to support spontaneous volunteers to build self-organizing distributed wireless networks, while considering real-world human behaviour, and *(ii)* improve the resilience of such systems, e. g., by providing mechanisms to deal with basic security services such as authentication or key management. Accordingly, the following four research goals were identified:

Goal 1. *Analyze how to enable the population to communicate without relying on a centralized infrastructure, while simultaneously considering real-world human behaviour in the face of disasters.*

Involving spontaneous volunteers in the disaster relief implies also to consider real-world human behaviour.

Currently, smartphone-based post-disaster systems are evaluated either using synthetic simulation models [44] or rely on trace-based models that cover everyday movement patterns [45–47]. Mostly, they try to mimic real-user behaviour and environmental characteristics, but they lack realistic assessment and scenario-specific models [48]. As a consequence, the user requirements for the systems and features are rather arbitrary. However, considering a disaster as a particular

use case, realistic simulation settings are crucial for getting a useful result. Therefore, a challenge is to design smartphone-based post-disaster systems that involve spontaneous volunteers in the disaster relief, while simultaneously taking into consideration their human behaviour. Thus, it should be ideally tested during a real crisis or a sufficiently realistic field exercise. The later has the advantage of avoiding unnecessary risks for all concerned.

Goal 2. *Establish security associations between mobile devices in a decentralized way.*

Security does not lose importance during a disaster as without features like authentication or integrity significant risks result.

As surveyed in our work [1], security does not lose importance during a disaster. For example, in Afghanistan terrorist groups disrupted communication infrastructure during the night to prevent civilians communicating with military forces [49]. However, during a disaster, it is often completely ignored due to missing knowledge of security mechanisms and the complexity required to implement secure communications. Indeed, security features, like authentication, confidentiality, and integrity, become mandatory, as without those features significant risks result, e. g., false information can be distributed during crises, resulting in confusion or a loss of trust amongst recipients [50, 51]. For instance, the lack of confidentiality is mainly a problem if private information is involved, such as the location and disposition of individuals and first responders. Many existing communications systems offer security features that depend on the availability of centralized infrastructure, e. g., Internet access is often required to check the validity of digital certificates. But if these centralized services go "dark", the users are left without practical solutions to bootstrap security on their mobile devices. Hence, the main challenge arises in bootstrapping security in partially disconnected networks.

Goal 3. *Develop adaptive and efficient neighbour discovery schemes for device-to-device communications.*

Saving energy consumption during device-to-device communications enhances the use of such networks in real scenarios.

Depending on the impact of the disaster, the acute phase of disaster response activities may span from a few minutes up to several days. Thus, the energy consumption required during D2D communications is a crucial factor for the use of such networks in real scenarios [38]. In this context, Neighbour Discovery (ND) represents one of the leading energy consumers. Practical ND solutions for mobile devices entail a number of new challenges over traditional wireless sensor networks. Particularly, ND schemes in emergency response scenarios need: *(i)* to deal with low discovery latency to support emergency response, *(ii)* to customize to user behaviour to increase the quality of experience, and *(iii)* to be implemented as a basic service that enables third-party apps.

Goal 4. *Compensate against scarcity of infrastructure by leveraging parts of digital cities that remain operational.*

The integration of IoT technology into post-disaster networks improves the resilience of such systems.

Building post-disaster networks based purely on smartphones remains a challenging task. The rapidly growing IoT technology offers the possibility to improve this situation. For instance, smart cities have become more important in the last decade as increasing numbers of digital devices, e. g., sensors or actuators, can communicate with each other using the Internet [22]. However, these devices have limited interoperability, and require Internet access to communicate and interact with one another. These factors limit the ability to integrate these devices into post-disaster systems. In this context, both a challenge and an opportunity arise to utilize the parts of digital cities that remain operational in case of disaster without using any special hardware or software modifications, thus mediating large-scale post-disaster D2D communication with communication tools that ordinary civilians can use.

1.3 CONTRIBUTIONS

This work includes the following contributions to achieve the goals mentioned above.

Contribution 1. *An In-depth Analysis of D2D Emergency Communication Systems to Identify Relevant Services and Requirements*

The first contribution covers an analysis of emergency communication systems and the identification of relevant services and requirements for such systems.

The first contribution implies an in-depth analysis of existing D2D emergency communication systems, which focus on enabling civilians to communicate in the aftermath of a disaster, to identify their assumptions as well as the security features they offer. Relevant disaster scenarios from the last decade, and the input of several responder organizations, such as the German Fire Departments, and the German Federal Office of Civil Protection and Disaster Assistance, are our basis for defining relevant stakeholders and services to be considered in smartphone-based post-disaster systems. In addition and as a result of our analysis, this contribution includes system and security requirements, possible threats, and challenges for communications technologies used during such events.

Contribution 2. *Evaluation of a Real-world Smartphone-based Self-organizing Emergency Communication System*

This contribution presents the results of a large-scale field test of a post-disaster system that relies only on ad hoc communication.

Based on the previous analysis, this contribution presents the insights of Smartphone-based Communication Networks for Emergency Response (SMARTER): a large-scale field test of a set of emergency services that relies solely on ad hoc communication. Over the course of a full day, we gathered data from smartphones distributed to 125 participants in a scripted disaster event. Additionally, the participants filled out a questionnaire after the field test to assess the subjective experience when interacting with specific disaster services. By evaluating the gathered data, SMARTER provides insights from civilians'

behaviour when utilizing smartphone-based communication networks in disaster scenarios. These results confirm the importance of real-world tests, especially if systems are designed for scenarios that are heavily affected by human behaviour. The SMARTER dataset is available to the research community [52] and thus can help with the design and evaluation of works targeting disaster relief, especially when utilizing smartphone-based communication networks.

Contribution 3. *Provide a Decentralized Secure Self-organizing Bootstrapping*

SoL is a lightweight scheme for bootstrapping D2D security tailored for local urban operations.

Existing distributed solutions such as the Web-of-Trust (WoT) solutions are not sufficiently lightweight and are neither well-suited for cross-application support on mobile devices, nor support strong protection of key material employing hardware security modules. This contribution presents Sea of Lights (SoL): a lightweight scheme for bootstrapping D2D security and for wirelessly spreading it to enable secure distributed self-organizing networks. It operates "in the dark" and provides strong protection of key material as well as an intuitive means to build a lightweight WoT. It adapts to the hardware capabilities of the host device and is able to utilize hardware security solutions to further improve the security of the underlying keys. SoL is tailored for local urban operations in scenarios such as the coordination of emergency response, where it facilitates containing the spreading of misinformation. SoL is developed as an Android service [53]. It comprises two layers. *(i)* The Trust Management Layer manages all operations related to the trust relations, and *(ii)* the Key Management Layer performs all operations concerning the underlying keys. Finally, a proof-of-concept was implemented for the Android platform to demonstrate and test its feasibility on real mobile devices. Its key performance aspects were further evaluated through simulation.

Contribution 4. *Optimize the Neighbour Discovery Process to Save Energy-consumption in D2D Communications*

SIESTA is an adaptive neighbour discovery scheme for saving energy during D2D communications.

This contribution proposes SavIng Energy in STAtic Phases (SIESTA), an adaptive neighbour discovery scheme for saving energy during D2D communications in self-organizing networks. SIESTA allows reducing energy consumption if node churn is low while offering fast response times for dynamic settings. As part of this contribution, an opportunistic networking framework for mobile devices based on SIESTA was implemented [54]. It is designed to allow mobile devices to participate in opportunistic networks while supporting energy-efficient neighbour discovery. Multiple third-party mobile apps can simultaneously connect to this framework, which is responsible for the abstraction of opportunistic communication. Finally, an Android application was developed as a proof-of-concept to demonstrate and test the feasibility of SIESTA on real mobile devices. The performance

aspects of the neighbour discovery scheme were evaluated employing simulation.

Contribution 5. *Integrate Existing IoT Solutions to Allow a More Resilience D2D Communication*

BLUEMERGENCY is a novel emergency network concept that utilizes parts of digital cities that remain operational in case of disaster.

With an increase in smart spaces such as smart homes and smart offices, we move towards digital cities that are deeply penetrated by IoT technology. Many IoT devices are battery powered and can aid in mediating an emergency network. In scenarios where the electrical grid is still operational, yet communication infrastructure has failed, non-battery powered IoT devices can similarly help to relieve congestion or build a backup network in case of cyber-attacks. With the recent release of the Bluetooth Mesh (BT Mesh) specification [55, 56], a common interface between mobile devices and the IoT has become available. This contribution proposes Bluetooth Mesh emErgency (BlueMergency), a novel emergency network concept that utilizes parts of digital cities that remain operational in case of disaster, thus mediating large-scale post-disaster D2D communication. Since the BT Mesh specification is backward compatible with Bluetooth 4.0, most of today's mobile devices can join such a network. That means, no special hardware or software modifications are necessary, especially neither rooting nor jail-breaking of the smartphones.

1.4 OUTLINE

This thesis is divided into four parts: introduction, analyzing smartphone-based emergency communication systems, improving their resilience, and conclusion.

This thesis is divided into four parts: introduction, analyzing smartphone-based emergency communication systems, improving their resilience, and conclusion. The Introduction part includes Chapters 1 and 2. Chapter 1 explains the primary research goals to allow *secure* D2D *communication for emergency response*.

Chapter 2 provides an overview of emergency communication systems: infrastructure-based and infrastructure-less solutions and their definition. It mainly considers related work with a focus on self-organizing solutions, their applicability, and their security features.

The contributions of this thesis involve two main aspects, namely, *(i)* analyzing smartphone-based emergency communication systems, and *(ii)* improving the resilience of such systems. According to these aspects, Chapters 3 to 7 detail the contributions.

Chapter 3 presents the smartphone-based emergency response scenario considered in this thesis. This chapter provides an in-depth analysis of existing smartphone-based emergency communication systems and summarizes their requirements as well as the most relevant services. It also describes the system and threat model followed in this work.

Chapter 4 details the result of the evaluation of a real-world smartphone-based self-organizing emergency communication system.

Chapter 5 describes a decentralized solution to allow bootstrapping security in self-organizing D2D communication networks during disasters. Furthermore, it presents the result of the evaluation of the key performance aspects using simulation as well as to demonstrate and test the feasibility of the proposed decentralized authentication solution on real mobile devices.

Chapter 6 introduces an adaptive neighbour discovery scheme for saving energy during D2D communications in self-organizing networks. This chapter also describes the evaluation procedure and the performance results by means of simulation, as well as the implementation of the Android application used to test the feasibility of SIESTA on real mobile devices.

Chapter 7 details the BlueMergency concept which supports and strengthens large-scale post-disaster D2D communication by integrating the parts of digital cities that remain operational in case of disaster.

Finally, Chapter 8 concludes this work.

2

BACKGROUND AND RELATED WORK

The previous chapter summarized the goals and contributions of this thesis, namely, to contribute to the design and development of secure Device-to-Device (D2D) communication for emergency response systems. This chapter examines the current state-of-the-art of emergency systems that provide communication in the aftermath of disasters. Section 2.2 summarizes the general concept of Emergency Communication Systems (ECSs), existing channels used for the communication as well as their security features. Subsequently, Section 2.3 explains self-organizing ECSs in detail. In particular, it discusses solutions that include smartphones in their systems to facilitate communication between rescuer teams and civilians.

2.1 MOTIVATION AND CONTRIBUTION

Communication is an important "force-multiplier" during disasters and crises.

Communication is an important "force-multiplier" during disasters and crises [57]. The challenge is that during such events, communications capability is typically reduced, while, conversely, demand for communications increases. As a result, supplementary communications capabilities are often brought into disaster and crisis zones in an attempt to bridge this gap. Our contribution is an overview of several existing technologies utilized by responders as communication channels during a disaster. We also summarize and discuss the security and privacy features of state-of-the-art communications mechanisms.

2.2 EMERGENCY COMMUNICATION SYSTEMS

Since 1970, large natural or human-made disasters are becoming more frequent. Figure 2.1 visualizes statistics from the Emergency Events Database (EM-DAT) of the Center for Research on the Epidemiology of Disasters (CRED) International Disaster Database. These statistics include disasters that meet at least one of the following criteria:

(i) The number of people killed is ten or more,

(ii) The number of people affected is hundred or more,

(iii) There is a declaration of a state of emergency, or,

(iv) There is a call for international assistance.

As depicted in Figure 2.1, the number of natural disasters such as earthquakes, floods or extreme weather, has increased from 100

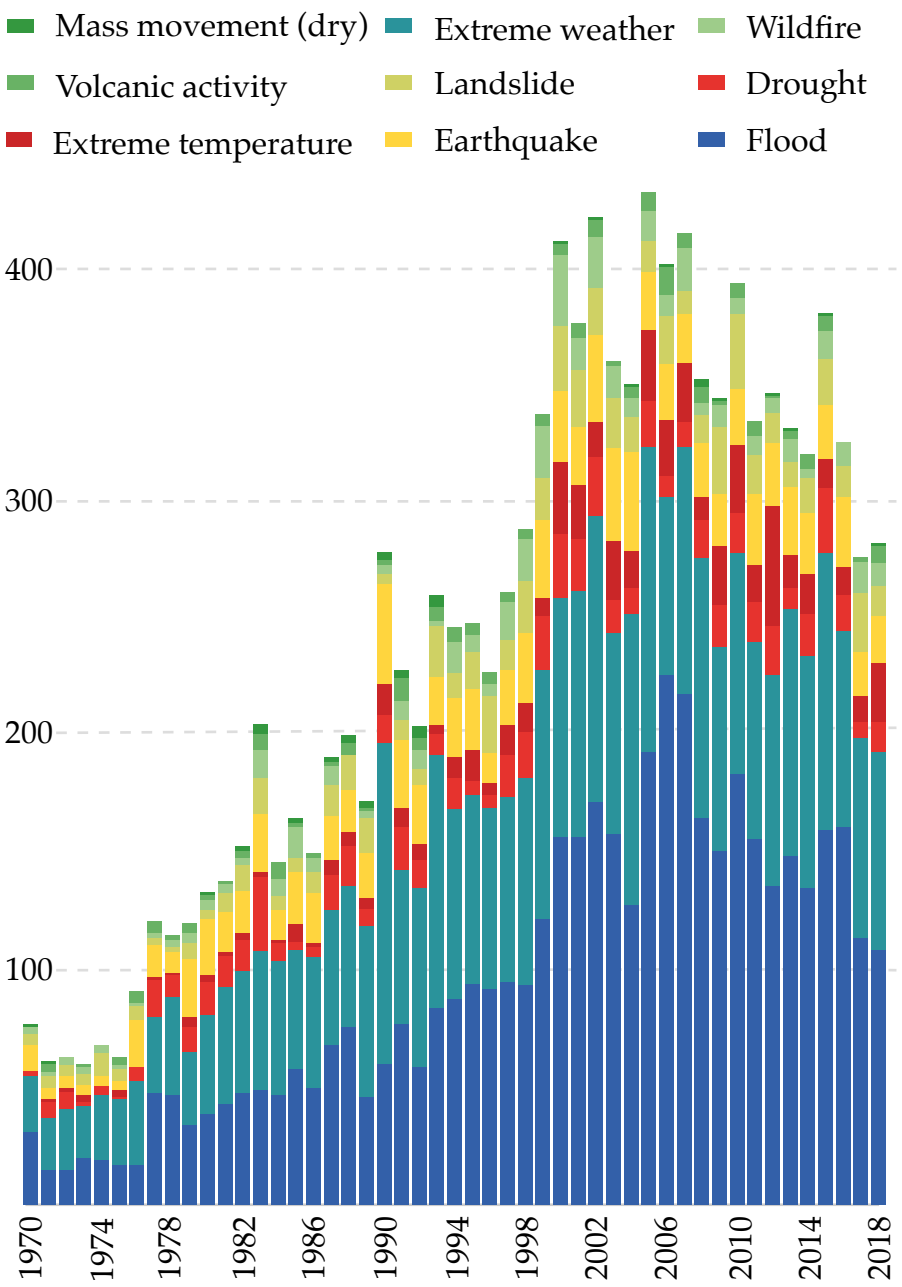


Figure 2.1: The annual reported number of natural disasters, categorized by type. This report includes both weather and non-weather related disasters. Source EMDAT (2017), OFDA/CRED International Disaster Database, Université catholique de Louvain – Brussels – Belgium. (adapted from [58])

The entire communication infrastructure is vulnerable to damage after a disaster.

to almost 400 per year. Such events have shown the vulnerability of the entire communication infrastructure, including cellular networks and telecommunication, to damage after a disaster. The loss of these communication systems hampers the rescue operation. Hence, we firmly believe that ECSs can play an important role in facilitating relief efforts in such situations. In this section, we refer to an ECS as follows:

Definition 2. *Emergency Communication System: "Emergency Communication refers to communication means and methods required for guarantying the rescue, emergency aid, and necessary communication by a comprehensive use of various communication resources in case of a natural or artificial sudden emergency. The primary objective of emergency communication systems is to provide reliable communication services to the victims located in the coverage holes due to the damage of infrastructure." [59]*

In other words, the concept of ECS focuses mainly on providing communication in the aftermath of a disaster. Such systems help to mitigate the impact of the disaster, by allowing rescue teams, civilians and victims to communicate inside as well as outside of the disaster area. These systems, however, may suffer a lack of security, providing either none or weakened security feature(s). This lack of security is particularly the case for features such as user authentication that depends on some kind of centralized infrastructure.

The concept of ECS focuses mainly on providing communication in the aftermath of a disaster.

2.2.1 *Infrastructure-based Emergency Communication Systems*

Perhaps the most straightforward scenario is using mobile telephony standards. It may also be that existing Internet connectivity is being used.

2.2.1.1 *Cellular Networks*

Cellular networks were designed to provide voice applications based on digital technology. They offer improved confidentiality, authentication, and integrity compared with the first generation analog cellular networks.

The security of cellular networks has improved with each successive generation of cellular technology.

While their security situation has improved with each successive generation of cellular technology, significant security issues remain and are constantly uncovered. Different studies and important examples [60–62] have demonstrated the feasibility of some attacks successfully exploiting the existing vulnerabilities and weaknesses of the underlying standards or poor operational practice by operators, e. g., by redirecting user traffic or theft of valid user identities, particularly in the face of a determined adversary who has the means to obtain specialized hardware that allows interception of 2G and 3G communications with relative ease.

However, significant security issues remain and are constantly uncovered.

Such hardware is available for less than US$1,000, placing such attacks well within reach of many adversaries. Even though cellular devices support new cellular technologies such as 4G and upcoming 5G, old technologies such as 2G and 3G remain active and are still the most used technologies for emergencies, as well as in deployed Internet of Things (IoT) and Machine-to-Machine (M2M) devices [63].

The main additional security improvements of 4G networks, for example, are focused on key management and protection against

physical attacks against base stations. Nonetheless, some security issues remain in the 4G networks [64–66]. In addition, some studies have already identified security vulnerabilities in 5G networks [67, 68].

Cellular networks are designed with "lawful intercept" capability, which can be particularly hazardous in civil unrest situations.

Also, cellular networks are designed with "lawful intercept" capability included, and therefore any use of such networks must take into account that not only the local government, but also potential adversaries with sympathizers within cellular carriers, may be able to intercept all communications, and use the advanced location capabilities of modern cellular base stations to obtain pervasive location data on users, including reliable predictions of where users are likely to be at a future time and date. This issue can be particularly hazardous in civil unrest situations, where one or more of the belligerents have reason to be opposed to the delivery of humanitarian relief in an area [69].

2.2.1.2 *Satellite Radio*

Satellite communications are widely used during disasters.

Satellite communication can offer high-speed data and video transmission in crisis. Many systems, however, suffer from problems such as weak security properties, issues in the synchronization process for the communication, and in some countries their usage may not be allowed [70]. Notwithstanding the above difficulties, newer satellite communication tools, such as Short-Burst-Data (SBD) modules connected to the Iridium constellation, offer the ability to communicate from most locations on the surface of the earth using a Short Message Service (SMS)-like interface. Also, only a small battery-powered satellite terminal is needed. It can be carried in a pocket and can pair with a smartphone.

Satellite communication systems, however, involve numerous vulnerabilities that attackers could exploit.

The security on the Iridium SBD service is described by "security by obscurity". Authors in [71], however, have determined that an attacker could listen to all Iridium SBD data directed to a given locale, by demodulating the broadcast signal from each satellite as it passes overhead, using only a few hundred dollars of equipment. This attack is particularly concerning, because the SMS-like service is unencrypted, and could be easily spoofed. That is, a determined adversary could potentially transmit signals that an Iridium SBD would interpret as having come from a satellite; thus, allowing an adversary to inject themselves arbitrarily into conversations.

The transmissions from the satellites are unencrypted, so this could be implemented in a manner that uses intelligence gathered from the transmissions to allow the mounting of sophisticated attacks that would be difficult for an end-user to detect. In 2014, IOActive [72] evaluated several satellite communication systems and identified numerous vulnerabilities that attackers could exploit. For example, attackers can disrupt all communications on some satellite systems by compromising just a few devices.

2.2.1.3 *Social Media*

In recent years, different disaster scenarios have widely shown the importance and benefits of social media in such situations, e. g., Twitter, Facebook, webblogs, wikis and other web-based resources [73–76]. These media enable a communication channel between different actors in the disaster area, but also facilitate the coordination, organization and involvement of spontaneous volunteers and civilians in the rescue efforts. Their wide availability and diverse facilities make them valuable to spread information widely in a short period. However, those same characteristics can be abused by adversaries, e. g., by creating multiple fabricated identities and using those to spread false information [77]. Platforms such as crowdsourcing and related mapping tools have begun to play prominent roles following disasters, allowing the collection, classification and organization of vital information, which significantly increases its value and utility in the response effort. These communications channels, however, build on existing communications infrastructures — mainly the Internet — with a central infrastructure, which itself may be affected after a disaster.

The use of social media in disaster scenarios has increased rapidly.

Due to the vast volumes of data and redundant information generated by such media, the identification of relevant messages without an appropriate prioritization of the information can be difficult, affecting the ability for a prompt and efficient response by rescue organizations. An interesting example was Hurricane Sandy in 2012, where more than 20 million tweets about the disaster were generated [78]. Furthermore, the open nature of social media where every person can publish new information, or repeat existing information, complicates the validation of the data being spread, making it easier for malicious users to manipulate data, or in some cases, cause the spreading of false information. The Safety Check feature activated by Facebook after the Nepal earthquake in 2015, was a good example of the misuse of social media during disaster scenarios [79].

Their wide availability and diverse facilities, however, can be abused by adversaries, e.g., by spreading false information.

2.2.2 *Self-organizing Emergency Communication Systems*

Where conventional communications are disrupted, it may be necessary to use personal communications media that are less secure than those ordinarily used. For example, analog or digital radios may be used in place of cellular mobile telephony.

2.2.2.1 *Analog Radio*

Analog radio has played a prominent role in disaster communications for many decades. In particular, Ultra High Frequency (UHF) and Very High Frequency (VHF) hand-held radios are frequently used to provide communications among personnel deployed during and following disasters. High Frequency (HF) radio is still present in

Analog radio is an unsecured broadcast medium.

many situations. However, its role is diminishing and increasingly being replaced in the field by lower-cost satellite based-solutions, such as the deLorme inReach [80]. deLorme inReach allows global communications reach, without the complications of maintaining and operating an HF radio installation, including ensuring that trained personnel are available. Analog radio is also an unsecured broadcast medium. That is, any party with a suitable radio can listen to all communications. Indeed, all parties must listen to all communications if they are to hear communications that are intended for them.

Any party with a suitable radio is able to listen all communications, or replay old recorded communications.

In situations where it is desirable to send non-confidential information and to reach multiple parties, the broadcast property of analog radio is beneficial, e. g., the disposition of members of a team as they carry out their activities. However, even in such cases, adversaries can easily listen to communications, replay recorded communications or more actively participate in communications in a variety of subversive, or even merely disruptive manners. For instance, an adversary can replay communications simply by recording the transmissions of others on a channel, and then replaying them into the microphone of a radio at a later time. This is because analog radio lacks confidentiality, authenticity and integrity.

2.2.2.2 *Digital Radio*

Digital radio provides several improvements over analog radio.

The typical example of this technology in Europe is Terrestrial Trunked Radio (TETRA), which allows the exchange of speech and status messaging with a limited data rate. Digital radio systems offer some improvements over analog radio: Their communications often support confidentiality. Some digital radio systems can authenticate communications and ensure their integrity. However, this is not the case for all digital radio systems. Hence, it is necessary to gain an adequate understanding of how confidentiality, authentication and integrity are provided by the radio system, and how they can be protected against common attack paths, such as theft, loss of a radio handset or traffic analysis, which imply a significant threat in some environments, e. g., in the presence of militias.

Some digital radio systems require some form of supporting central infrastructure.

Furthermore, different analyses [81–83] have identified significant security weaknesses of these systems, which lead to potential attacks that could affect the provided security features such as confidentiality. For example, an adversary can get access to sensitive data, track devices, or analysis exchanged traffic. Also, some digital radio systems still require some form of supporting central infrastructures, such as a base station or central repeater.

2.2.2.3 *Off-grid Ad Hoc Networks*

In addition to the traditional communications system, distributed Mobile Ad Hoc Network (MANET) have been developed over the past

twenty years or so, primarily enabled by the development of 802.11 Wi-Fi [84]. These networks may use wireless technologies such as ad hoc Wi-Fi, Wi-Fi Direct, or Bluetooth to allow a direct communication between mobile devices. The general intent of such networks can be summarized as facilitating the creation of networks without reliance on conventional fixed infrastructure. Within the humanitarian space, projects of potential interest include, without limitation, the FreiFunk and associated projects in Europe [85, 86], the Commotion Wireless project from the USA [87], and the Serval Project from Australia [88–91]. Each of these projects has a particular focus. For instance, FreiFunk and the related movement facilitates the provision of (typically wireless) Internet access, independent of existing infrastructure. The Commotion Wireless project is primarily interested in providing secure Internet and intranet access in difficult environments, such as providing communications for dissidents under oppressive regimes. The Serval Project is primarily focused on providing secured mobile telecommunications without dependence on existing infrastructure, with an emphasis on disaster response and isolated communities. The differing approaches and intentions of each project result in a diversity of security properties of these networks. However, many modern incarnations pay particular attention to the issues of confidentiality, authenticity, and integrity of communications — including the difficult matter of managing the routing of communications among the devices in a MANET [31, 92]. When contemplating using such systems, particular emphasis should be placed on ensuring that the desired properties are provided by the particular system being considered.

Different projects focused on MANETs as a viable solution to implement multi-hop communication in emergency scenarios.

The differing approaches each project results in a diversity of security properties of these networks.

2.3 SMARTPHONE-BASED SELF-ORGANIZING EMERGENCY COMMUNICATION SYSTEMS

Nowadays, smartphones are an integral part of everyday life. Over the years, their usage has been established not only in many daily activities such as social interaction, but also in critical situations such as emergencies and crises. During the last fifteen years, civilians have demonstrated how valuable their support and contribution are during the relief effort [93]: They have collected information about missing people, or created repository sites to exchange information about the devastated area. However, during the first 24 hours, the communication infrastructure is usually either entirely out of order or at least overloaded. Besides, the 72 hours after a disaster, known as the *"golden 72 hours"* [94], are decisive and crucial in an emergency, since in most cases, only people which are rescued within that time, have a good chance of surviving. Therefore, decentralized infrastructure-less communication solutions, especially based on smartphones, have been studied and proposed in the last years. In this context, this section summarizes and compares several relevant existing smartphone-based

Civilians have demonstrated how valuable their support and contribution is during relief efforts

ECSs, which allow the civilians to coordinate and communicate during a disaster. Some of these solutions were briefly described in the previous section.

2.3.1 *Comparison of Existing Solutions*

This subsection presents existing smartphone-based ECSs. These solutions are classified into two categories: commercial and research projects.

2.3.1.1 *Commercial Projects*

Commercial projects require a central infrastructure to enable communication.

Commercial solutions in the field of emergency communication are mainly limited to the services that allow data exchange between rescue teams and the population. These services, however, require a central infrastructure to enable communication.

Many solutions provide a mobile application to enable civilians to report infrastructure problems after a disaster.

To mention here: the Federal Emergency Management Agency (FEMA) from the US-Department of Homeland Security or the Digital Operations Center (DigiDOC) from the American Red Cross. The FEMA mobile app [95] features weather alerts, a map showing the location of the disaster centers, etc. This app also enables civilians to report the situation awareness of buildings or roads after a disaster, e. g., by sharing photos. The DigiDOC [96] uses the data shared in the social media during and after a disaster to collect information about the situation in the affected area. Regarding privacy concerns, they only process accessible public information. In addition, the Red Cross uses various social channels such as Facebook or Twitter to disseminate information. The Red Cross also facilities smartphone applications [97] for specific weather events such as hurricanes, wildfires or floods. These apps contain behavioural advice in the event of a disaster. They also can show live information about a specific event, e. g., an app can display and predict the direction of fire propagation, which in turn allows the population to get safe.

Other projects enable government agencies to send warnings and behavioural advice.

Further projects are KATWARN [98] from the Fraunhofer Institute for Open Communication Systems (FOKUS) on behalf of the German public insurance companies and Emergency Information and Messaging App (NINA) [99] from the Germany Federal Office for Civil Protection and Disaster Relief (BBK). Both applications are warning systems that enable government agencies, e. g., fire brigade control centers, to send by SMS, E-Mail or push notification, warnings and behavioural advice to the people affected by a disaster. Also, users can configure location-based warnings. While in the NINA app the location-based warnings require Global Positioning System (GPS), in KATWARN these warnings are not carried out with GPS, but use base stations and WLAN access points.

However, all these projects are functional only if there is a connection to conventional communication infrastructures, e. g., the Internet, as

all the data provided by these applications is stored and processed on centralized servers.

2.3.1.2 *Research Projects*

Even though the commercial projects mentioned above are helpful, they do not facilitate direct data exchange between spontaneous volunteers to support organization and cooperation in the event of a disaster. In contrast, research projects are more focused on providing communication between civilians during a disaster. Most of them do not require a connection to the mobile network or the Internet. Research projects such as SOS-Cast [100] or Help Beacons System [101] are Android applications developed to enable civilians to send SOS messages. SOS-Cast helps responders to find trapped persons. A user broadcasts a SOS message, including its name, physical condition and location. The messages are then relayed via civilian phones until they reach a responder device. Communication is only supported from civilians to responders. The Help Beacons System allows sending help messages in proximity in an ad hoc manner. This system uses the Service Set IDentifier (SSID) to transmit the content of the message. The Help Beacons app establishes an ad hoc connection between the smartphone of the injured person and the smartphone of a rescue responder.

Most of existing research projects do not require a connection to the mobile network or the Internet.

Furthermore, projects such as INKA [102] or ENSURE [103] are solutions that integrate spontaneous volunteers in relief efforts. These solutions use Web 2.0 applications in the government agencies site to able communication between responders and civilians.

Several approaches allow civilians, e.g., to send their location coordinates, to request help, or to gather information about the current situation in the disaster area.

Twimingt [104] is another research project which uses an Android application to allow communication between twitter users via Bluetooth using an epidemic routing protocol. It needs as a prerequisite a Twitter account or an Internet connection to create one. The messages are stored locally and are sent to the Twitter servers whenever connected to the Internet. Twimight supports only hashtags, i. e., it lacks user and group communications. The Serval Project from Australia [88–91] provides a smartphone app that allows text messaging, voice calls, and file sharing, with an emphasis on disaster response and isolated communities. Previous versions of the Serval Mesh app used the Independent Basis Service Set (IBSS) mode in rooted Android devices to provide peer-to-peer communication. The current version enables ad hoc communication by using Bluetooth. Additionally, they include external devices, so called Serval Mesh Extender, to allow communication using Wi-Fi.

Additional research projects focus on: *(i)* Providing communication between civilians and responders, e. g., for collecting information about the current situation in the disaster area (a kind of crowdsourcing) [105], *(ii)* Monitoring of responders, e. g., by collecting and processing medical sensor data of responders in disaster scenarios

[106], or, *(iii)* The use of social media to help authorities to deal with different scenarios [107].

2.4 SUMMARY

We present a suite of comprehensive solutions that contribute to the design and deployment of secure device-to-device communication for ECS.

The ECSs mentioned above are not necessarily applicable to all disaster scenarios, their importance and requirements can differ according to the features of the emergency scenario, as well as by the communication mode(s) required. We were only able to find relatively few studies or related work that supply directly helpful information about possible issues and security requirements for such technologies in disaster scenarios.

The security properties of the communication options available in a disaster zone may not be immediately apparent, and as adversaries become more and more active during disaster response activities, there is a compelling need to provide honest users with practical evidence-based information that allow them to make informed decisions about the use of the available resources while minimizing the risk for harm. Possible risks include surveillance, censorship, inter-mediation or otherwise interference with the communication channels. For example, a militia or other informal power-block may monitor Internet communications in order to gain advantage or further their victimization of others. In some locations it is also possible that surveillance may be used to gather material in order to seek expulsion or incite or commit extra-judicial violence or other actions against disaster responders, e. g., in areas where religious or other extremist activity is present.

Overall, the results indicate the lack of security for several communication technologies. For instance, analog radio communication and 2G cellular networks are considered insecure channels, nonetheless, these technologies continue to be significant communications channels used during disasters. Furthermore, different countermeasures to avoid many of the 2G vulnerabilities have no effect in the inter-operation between 2G and 3G networks. In addition, the Internet based platforms are provisioned and operated by untrusted third parties, and their security depends on the service providers. Alternative systems such as VoIP or chat applications implement proprietary protocols and security countermeasures, which imply interactions between different technologies that can also lead to unexpected results which may in turn result in security issues.

Although there are several projects focused on the design and implementation of infrastructure independent post-disaster communication systems, most of them: *(i)* Still lack the integration of human behaviour and their requirements in the aftermath of a disaster, *(ii)* Depend of central infrastructure to bootstrap security in a decentralized way, *(iii)* Require optimized energy consumption, and *(iv)* Do not include existing wireless sensor networks to improve the resilience of such

systems. Instead of proposing another specific system, we present a suite of comprehensive solutions that contribute to the design and deployment of secure D2D communication for ECSs.

Part II

ANALYZING SMARTPHONE-BASED EMERGENCY COMMUNICATION SYSTEMS

This part of the thesis analyzes existing mechanisms and solutions to facilitate civilian communications using smartphone-based ECS. Chapter 3 highlights the most common communications needs in the aftermath of a disaster and, identifies relevant requirements and services to be included in smartphone-based ECS. It also describes a general system and threat model that should be taken into account for such systems. Finally, Chapter 4 presents the findings of the real-world field test conducted as a proof-of-concept of a self-organized smartphone-based ECS.

3

SMARTPHONE-BASED EMERGENCY RESPONSE SCENARIO

Previous chapters have briefly explained the general concept of Emergency Communication System (ECS), communication technologies used in such systems as well as their security features. Also, they have presented several technical solutions that enable spontaneous volunteers to build self-organizing distributed wireless networks [100–105, 107], and thus enabling the population to communicate using their mobile devices without relying on a centralized infrastructure. These self-organizing distributed wireless networks build on user participation and leverage Mobile Ad Hoc Network (MANET) or Delay Tolerant Network (DTN) technology to facilitate message routing, forwarding, and spreading in the affected area.

This chapter first provides a representative list of disasters from the last decade in Section 3.2, highlighting common factors. Section 3.3 summarizes main stakeholders, as well as communication technologies used in such situations. With this information, Section 3.4 raises the most relevant civilians' requirements for post-disaster smartphone-based systems. Typically, in such situations, the most critical personal communications needs focus on the exchange of small but vital data, such as SOS messages, telling family and friends that you are safe, or sharing situational awareness [108].

3.1 MOTIVATION AND CONTRIBUTION

Each disaster scenario is different and its impact depends on each specific situation. On the one hand, earthquakes warning systems can detect the nondestructive primary waves, which implies a short time slot between 60 and 90 seconds before the destructive secondary waves arrive. On the other hand, hurricanes and their trajectories can be monitored typically for hours, which implies more time in advance, allowing people to take preventive measures. Nonetheless, they have several common factors: Most of them imply partially or totally damaged communication channels. They also have demonstrated that civilians tend to organize themselves. Communication is needed by the rescuers to coordinate their efforts. Civilians also need to communicate with each other, e. g., with their families, friends and rescuers. The contribution of this chapter is to analyze and highlight communication issues that occurred in these scenarios as well as relevant characteristics of civilians' behaviour, as well as plausible threats from contemporary disaster and crisis events. In this context,

Each disaster scenario is different, however they have a number of common factors: partial or total damage of communication channels.

this chapter also presents the system model, threat model and security requirements for post-disaster communication systems.

3.2 RELEVANT DISASTER SCENARIOS

Large natural or human-made disasters are becoming more frequent and their impact has significantly grown.

The number of natural or human-made disasters and their impact have significantly grown in the last years. This section focuses primarily on four relevant scenarios to identify the most common communications needs from the perspective of both organizations and individuals.

3.2.1 *Earthquake and Tsunami*

Warning and relief efforts were impaired by damage to infrastructure and lack of communications.

In April 2015, Nepal suffered a magnitude 7.8 earthquake, causing significant damage to the local telecommunications infrastructure. The disruption of communications complicated relief efforts. It hindered the coordination of help efforts, slowing response, especially during the crucial first hours [109]. One year later, an earthquake with the same magnitude as in Nepal struck along the central coast of Ecuador. It substantially impacted all infrastructure, i. e., electricity, water supply, and telecommunication [110]. In both cases, warning and relief efforts were impaired by damage to infrastructure and the lack of communications. Particularly, following the Nepal earthquake, citizens played an essential role in reducing these effects, assisting relief efforts through collecting, disseminating and exchanging information and news about the ongoing situation in the disaster area via social networks. Social media was also used to search for missing people or relatives, and to reassure others of their safety.

3.2.2 *Hurricane*

Responders were unable for days to share information and to inform the affected population about the damage.

In 2017, in the span a few weeks, the Caribbean was devastated by three hurricanes (Irma, Harvey and Maria) [111]. Their collective damages were estimated at over 478 billion dollars. Hurricane Maria, e. g., led to the most significant power outage in the history of Puerto Rico ever recorded. It caused massive damage in the entire communication infrastructure, including telecommunication and cellular networks, resulting in the isolation of thousands of people. Thus, the power blackout implied also a very prolonged communication outage. Two months after the hurricane approximately one third of the cellular sites were still out of service [112]. The pervasive and widespread communications failures also substantially hampered relief efforts. Responders, for instance, were unable to share information, or to inform the affected population about the damage, for days.

Table 3.1: Overview of relevant disaster scenarios and their issues.
We consider following notation: ● fully applies, ◑ partially applies

Issue	Earthquake / Tsunami	Hurricane	Bush Fires	War/Unrest
Loss of Communications	●	●	●	◑
Isolation of People	●	●	●	◑
Response Difficulties	●	●	●	●
Use of Social Media	●	●	◑	●
Collaboration of Citizens	●	●	●	◑
Search for Missing People	●	●	◑	◑
Lack of Information	●	●	●	◑

3.2.3 *Bush Fires*

In 2009, the Black Saturday bush fire affected a widespread area in the southern Australian state of Victoria [113]. The Black Saturday was Australia's worst bush fire since the Ash Wednesday fires of 1983, resulting in 173 fatalities, with communications services unavailable in many areas [114].

Similarity, the Camp Fire in 2018 was one of the deadliest bushfires in the history of California [115], causing at least 85 fatalities. In both cases, the damage and overload in the communication infrastructure as well as the lack of information about the accessibility of the affected areas, greatly impaired relief efforts. Before responders could act, they had to collect information about the impact of the disaster to facilitate access [116]. Furthermore, affected regions did not receive any warnings and evacuation instructions in a timely and reliable manner; thus compounding the situation. Nonetheless, the collaboration of local communities, and local and international organizations, helped to provide support to people affected by the disaster.

The collaboration of local communities, local and international organizations helped to provide support to people affected by the disaster.

3.2.4 *War and Unrest*

War and civil unrest also often disrupt communications infrastructure, through either damage or other actions of the belligerents. Such unrest also acts to impair the development and extension of telecom-

Unrest acts to impair the development and extension of telecommunications infrastructure.

munications infrastructure. For example in South Sudan years of civil conflict and warfare have acted to prevent investment in telecommunications infrastructure [117]. Syria is also an example of this, while the regions controlled by rebels have no access to the Internet and because cellular networks have been destroyed or are out of service, the government-controlled regions have an entire infrastructure.

3.2.5 *Common Factors*

The aforementioned use-cases are only examples of how users and their needs influence the emergency response networks dedicated to helping them. While these use-cases vary, they exhibit several common factors as show in Table 3.1. Indeed, if we consider these and several other representative factors for the above use-cases, we find that they almost all apply to every use-case, although differences may arise in the relative significance of each factor. For instance, natural large-scale disasters severely affect the information and communication capabilities of the population by damaging infrastructure, making communication systems unavailable or knocking out the power. Thus, the loss of communications capacity, or isolation of people and communities from one another, are common by most of them. Human-made disasters such as war or censorship, are deliberate activities focused to disrupt the communication or to isolate people. Such situations are commonly targeted at certain regions, thus the loss of communication can, e. g., affect only selected broadcasting channels, or be limited to specific hours during the day.

3.3 DISASTER SCENARIO

In this section, we present the definition of disaster considered in this work. We derive the stakeholders based on this definition.

3.3.1 *Definition*

There is considerable variation in the definition of a disaster, both in terms of the scope of the kind of events included as well in the nomenclature used [118]. We further refer to the definition proposed by the United Nations as follows:

In a disaster there is a need for external support and additional communication capability is required.

Definition 3. *Disaster: "..A serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources." [119]*

That is, the overarching defining characteristic of a disaster, as compared to, for example, an accident or other non-disastrous undesirable events, is that in a disaster, there is a need for external support. In

the case where a disaster involves communications, this implies that additional communications capability or capacity is required to be introduced to the disaster zone. This need for external support may then require that responders, civilians, existing services and authorities, and any other parties active in the disaster zone, resort to communication tools, technologies, suppliers or media that they would not regularly use. As a result, the resulting communications may have drastically different actors and requirements compared with regular use.

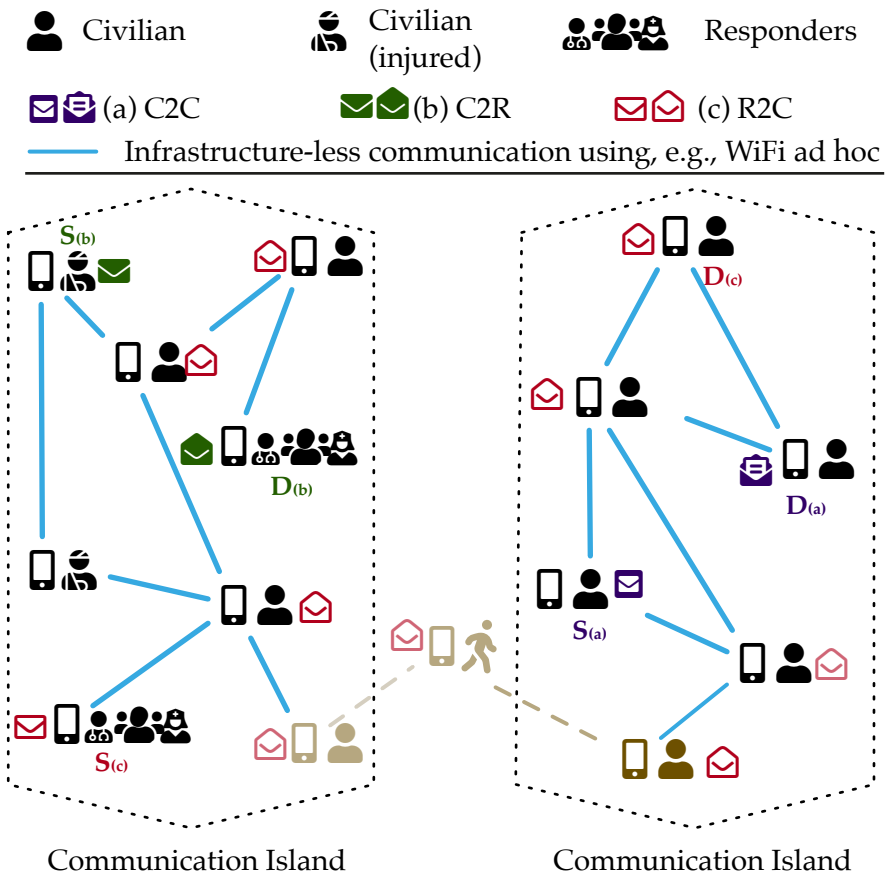


Figure 3.1: An example of the three communication pathways considered in this thesis: (a) between cilivians –Civilian-to-Civilian (C2C), e. g., private message between civilians, (b) from civilians to responders – Civilian-to-Responders (C2R), e. g., help requests, (c) from responders to civilians – Responders-to-Civilian (R2C), e. g., broadcast warning messages.

3.3.2 *Stakeholders*

It is extremely difficult to cleanly divide the roles of people in a disaster zone.

The roles of people during a disaster are complex. Many beneficiaries of help are at the same time responders. A person may, for example, be a beneficiary of food and water, but then assist the response efforts

by searching for survivors or restoring telecommunications services. Such persons may provide help in both individual and institutional capacities. Furthermore, the institutions or organizations which they serve may either be pre-existing ones, e. g., a cellular carrier or national disaster management organization, or a newly formed ad hoc relief organization [120]. Thus, it is tough to divide the roles of people in a disaster zone cleanly. Together with our evaluation of the cases surveyed, this led us to the understanding that communications between civilians in a disaster zone is both of vital importance, and often particularly vulnerable, as civilians typically do not possess their own dedicated communications capacity, in contrast to many established relief organizations. Therefore our approach concentrates on communication tools that ordinary civilians can make use of in the wake of disasters, as depicted in Figure 3.1. As such, our focus is the facilitation of Civilian-to-Civilian (C2C) communications. Organizational or institutional communications are also explored, but only in so far as they can be directed at, or received by civilians, i. e., Responders-to-Civilian (R2C) or Civilian-to-Responder (C2R) communications. Communication between organizations is outside of the scope of this thesis.

Our approach concentrates on communication tools that ordinary civilians can make use of in the wake of disasters.

3.3.3 *Communication Technologies*

The main characteristics of existing communication technologies that enable direct communication between mobile devices can be summarized as follows.

3.3.3.1 *Bluetooth and Bluetooth Low Energy (BLE)*

Bluetooth is a communication technology present in almost all smartphones. It is defined according to the IEEE standard 802.15.1 [121]. Bluetooth exists in two different variants: Classic (Bluetooth before 4.0) and Bluetooth Low Energy (BLE) (BLE, 4.0 and up). Its range and number of connections are limited to a few meters and up to eight devices respectively. Bluetooth has a transmission rate to a maximum of 2 Mbps. The main difference between Bluetooth Classic and BLE is that BLE reduces energy consumption. For instance, Apple's Multipeer Connectivity Framework [122] or p2pkit use BLE for the neighbour discovery process. However, it is not compatible with the previous versions, i. e., old mobile devices do not support BLE.

Bluetooth is a communication technology that is present in almost all smartphones.

3.3.3.2 *Wi-Fi Direct*

This technology enables mobile devices to act as access points. It is defined in the Wi-Fi Peer-to-Peer (P2P) Technical Specification [123]. Other devices (*clients*) can connect directly to the device acting as an access point (*master*). The number of connections is limited, as it is

Wi-Fi Direct enables mobile devices to act as access points.

not possible to connect any number of end devices at the same time. Currently, most of the smartphones support up to eight devices. The power consumption of the master is also significantly increased.

3.3.3.3 *Wi-Fi Independent Basis Service Set (*IBSS*) Mode*

The IBSS mode is defined according to the IEEE standard 802.11 for Wi-Fi [124]. Each device can communicate directly with other device, and the number of connections is not limited. For supporting multihop capabilities it is necessary to implement a routing protocol at the network layer. This mode, however, is not available on mobile devices by default. IBSS mode is only supported by jailbreaking a smartphone.

To support this mode, it is necessary to jailbreak a smartphone.

3.3.3.4 *Wi-Fi Infrastructure Mode*

This technology is based on communication with the existing infrastructure. It is defined in the IEEE standard 802.11 for Wi-Fi [124]. The devices connect to an access point that is responsible for the management of the network. There is no direct Device-to-Device (D2D) communication, instead, they use the access point to communicate. Thus, they need to remain within the radio range of the access point to communicate with each other.

There is no direct communication between devices.

3.3.3.5 *Wi-Fi Aware*

Wi-Fi Aware is a new communication technology that facilitates the discovery of services offered by neighbouring devices and a direct connection between devices without the need of cellular or infrastructure connection.

It is defined in the Wi-Fi Aware Alliance [125]. The functionality of Wi-Fi Aware is similar to Apple Wireless Direct Link (AWDL) from Apple [126]. The devices form a cluster and select a master. Then all devices synchronize with the master's clock. However, it does not support backward compatibility and only a small number of new smartphones support this mode.

Wi-Fi Aware does not support backward compatibility.

3.3.3.6 *Smartphones Manufacturer Frameworks*

The Multipeer Connectivity framework is developed by Apple [122]. It enables offline D2D communication between iOS devices without the need for an Internet connection. This framework facilitates discovery of services provided by nearby devices and connects with them.

Google Nearby is a framework developed by Google [127]. Similar to the Multipeer Connectivity framework, it allows a device to discover service announcements by other nearby devices. If a nearby service is discovered, a device (*client*) connects automatically to the other device (*server*). Hence, both devices can now exchange data in the form of bytes, files or streams. Both, however, use standard wireless

They use standard wireless technologies to enable D2D communication.

technologies to enable D2D communication: Google Nearby uses Bluetooth and Wi-Fi Direct, and Multipeer Connectivity uses AWDL, a proprietary combination of Wi-Fi and BLE which has been extensively analyzed in [126]. In addition, they do not support interoperability, i. e., cross-platform D2D communication between smartphones.

3.4 REQUIREMENTS AND SERVICES

Due to the wide range of scenarios and their specific characteristics, it is difficult to generalize and mandate specific technology choices and security settings. Likewise, it is impractical to specify requirements for all imaginable disaster scenarios in detail. Nevertheless, based on the relevant scenarios summarized in Section 3.2 and the input of several responder organizations such as the German Fire Departments, and the German Federal Office of Civil Protection and Disaster Assistance, we identify relevant requirements as well as services to be considered in a smartphone-based post-disaster system.

3.4.1 *Requirements*

We identify relevant requirements for a smartphone-based post-disaster system based on the input of several responder organizations and relevant scenarios.

Self-organizing post-disaster networks may be used in varying scenarios by people with very different requirements, and types of information to be exchanged. This part of the thesis provides a list of requirements that such a system should meet:

3.4.1.1 *System Requirements*

- The system should facilitate communication channels from civilians to responders and vice versa.
- The system should allow coordinating the exchange of resources, e. g., tools, machines, food, as well as assistance.
- The user should be able to search for missing persons.
- The system should enable users to send a distress message.
- It should be possible to send a sign of life, e. g., health or location to family and friends.
- The system should consider the available smartphone's sensors to include additional functionality, e. g., send user location information by using GPS data.
- Collaboration between the civilians and responders without a central infrastructure should be possible.
- Communication between users after changes in the topology or network participants should be guaranteed.

- Battery life must be considered to maximise communication during extended power outages.
- Users should be able to enter or to leave the network at any time. The number of users and their mobility should not be limited.
- The system should allow collaborative communication between users independent of their type of smartphone.

3.4.1.2 *Security Requirements*

We also identify the main security requirements when implementing a system for use in a disaster.

The security requirements can differ according to the nature of the emergency scenario.

- *Confidentiality*: There are scenarios where it is vital to ensure that only the specified person can read the exchanged information [73, 128]. Attacks against this security goal aim to get access to sensitive information without accurate authorization. Hence, different methods and mechanisms are necessary to keep the content of a message secret from unauthorized users. In specific scenarios, however, where the data is public by itself, this property may neither be mandatory nor desirable.
- *Authenticity*: The receiver of a message should be able to corroborate that the purported sender is, in fact, the authentic author of the communication [129], e. g., for public alerts or warnings from rescuers. Without such an authentication mechanism, users could impersonate one another, with considerable scope for disseminating misinformation with malicious intent.
- *Key Management*: The management and exchange of key material between users on the network without prior communication should be guaranteed.

Furthermore, attacks against the integrity of communications aim to modify legitimate information, for example, replacing a valid text of any communication with text chosen by the attackers. In this context, it is necessary to verify if the exchanged information between two parties was altered during transmission, as well as to protect the content of a message against any alteration. In most cases, this is a mandatory property, as otherwise, an attacker could maliciously cause arbitrary misinformation. Anonymity, privacy, social accountability and non-repudiability represent an additional set of security properties that are particularly important when private persons communicate with one another, with the public at large, and in some cases, with government and authorities. Together, they allow users to interact without excessive fear of the consequences of their communications, or of the consequences of the communications activities of others (including the passive collection of communications). However, the focus

Integrity, anonymity, privacy, social accountability and non-repudiability are not within the scope of this thesis.

of this thesis is on communications among persons and organizations where the opposite is the case: where it is highly desirable for the authenticity of persons and their actions to be sustained. Therefore these topics are not within the scope of this thesis. However, they are not necessarily irrelevant to all disaster scenarios: their importance can differ according to the nature of the emergency scenario. For example, anonymity can be of significant importance in scenarios where a government controls communication channels. In such cases, it is important that the opposition or other people with differing opinions or anti-government positions cannot be identified, or at least cannot be distinguished among a group of senders [130].

3.4.2 *Services*

We identify and highlight the most relevant services for smartphone-based post-disaster systems.

The relevant scenarios summarized in Section 3.2 are only examples of how users and their needs influence emergency response networks dedicated to helping them. Based on this information, we identify and highlight the most relevant services for smartphone-based post-disaster systems.

- *SOS Emergency Messages*: This service allows people to send an urgent request for help to responders. The message may additionally be sent to neighbouring nodes that can act as first responders. This service works as an addition and not as a replacement to national emergency numbers, such as 112 in Europe, 000 in Australia and 911 in the USA.
- *I am Alive Notifications*: I am Alive Notifications enable the affected population to report their status information, e. g., location, health, and needs to other users in the post-disaster network. As mentioned in the previous section, social networks like Facebook, and Non-governmental Organizations (NGOs) like the Red Cross, implement such services on demand, mostly based on websites hosted on central servers. These services are rarely integrated, resulting in fragmentation of information, and often requiring users to submit their information on multiple systems, further straining communications infrastructure.
- *Person-Finder*: Person-Finder provides the counterpart to I am Alive Notifications: the possibility to ask about people assumed to reside in the area around the incident. To facilitate this, the service should allow searching for people based on different information, e. g., last known location or via photo. Geographic forwarding schemes may be employed to limit and refine searches to the assumed location of an individual.
- *Situation Assessment*: This service allows the affected population to report observations from the disaster area, such as damage

reports or availability of supplies, to either responders or the affected population.

- *Information/News*: Information/News services allow responders to make announcements regarding currently existing, or potentially evolving hazards in a specific area to the public. This service could use various dissemination modes, targeting groups, individuals, areas, or any combination.
- *Resource Market Registry*: This service is used to match requests for resource, e. g., requests for fuel, energy, water or medical supplies to offers from the affected population. This service provides a tool for self-organizing resource sharing based on information about needs and requests. The information should be exchanged among the affected population, but only in specific regions, to prevent unnecessary information transmission, and thus minimize the required communications capacity.
- *Tasking*: The Tasking service is similar to the Resource Market Registry Service, but focuses on human resources, i. e., enabling responders or the affected population to recruit and manage personnel in achieving particular relief initiatives of individuals.
- *Messaging Services*: Messaging service allows private messaging similar to Short Message Service (SMS) between two parties, enabling the affected population to communicate with family, friends, or others for any necessary purpose.

3.5 SYSTEM AND THREAT MODELS

In this section, we describe a general system model for smartphone-based post-disaster communication systems. Furthermore, we take plausible threats from contemporary disaster and crisis events into account to define a threat model for disaster scenarios.

3.5.1 *System Model*

We consider ubiquitous mobile devices equipped with a variety of common sensors. The sensory capabilities of such devices can provide helpful information about the extent or severity of damage at the site of the disaster [131] as well as the status of the device's owner through activity recognition [132]. Each node can act as the data source, destination, or relay station and thus needs to decide whether data is forwarded, stored or discarded. Additionally, in such networks, where the interconnection time between nodes is not predictable, an end-to-end communication channel cannot be guaranteed. We do not limit our discussion to any specific communication technology; thus, we assume the existence of mechanisms for the data

We assume the existence of mechanism for the data routing/forwarding/spreading and physical interfaces required for direct D2D communication.

routing/forwarding/spreading and physical interfaces required for direct device-to-device communication.

3.5.2 *Threat Model*

The impact of an attack can vary according to the capabilities of the adversary as well as the scenario or situation in which an attack occurs.

Adversaries mainly take actions that induces losses upon other parties.

A user in a communication network during a disaster can act in any of the following roles: *(i)* an honest user, who contributes to the communication, cooperates with neighbours, acts according to the specified protocols, rules, or, *(ii)* a malicious user, who tries to manipulate or subvert regular communications. An adversary's behaviour and the impact of an attack can vary according to the capabilities of the adversary as well as the scenario or situation in which an attack occurs. Adversaries can work alone and independently (*single attackers*), or collaborate with other malicious users (*colluding attackers*). It depends on the goals and the motivation of the attacks. On the one hand, colluding attackers can be desperate people, who try to take advantage of available resources without regard for others, for example, to meet their basic needs for food, shelter and other materials. For these actors, they can perhaps be modelled from a game theory perspective as seeing the situation as a zero-sum game, and they are seeking to maximize their gain, without being hindered by the fact that it necessarily increases losses to other parties. That is, their objective is their gain, rather than the loss of others. On the other hand, there can be actors such as terrorists, who can also be colluding attackers, but who are actively trying to exploit destruction and chaos in civilian communication causing panic and confusion. They can perhaps be modelled from a game-theory perspective as seeking to minimize the sum of the game from the perspective of other parties. That is, rather than failing to be hindered by the presence of a zero-sum game, they are actively motivated by this. As this analysis reveals, while their motivations and thus, modes of operation may differ, they have the same final effect of undertaking actions that induce losses upon other parties.

In this subsection, we are going to give a high-level overview of possible adversaries that can be considered during a disaster scenario. These categories can differ and need to be adapted according to the features of the emergency scenario, as well as by the communication mode(s) required.

a Non-cooperative user's behaviour: In some situations, when normal users (civilian or organization) compete to gain some limited resources, they may cease cooperative actions, as they actively seek to optimize their resources. Their behaviour can affect the entire communications channel.

b Militias: The Haiti Earthquake of 2011 saw many examples of this kind of adversary [73]. Militias broke into stores and induced a

state of violence and anarchy. Without a security mechanism for communication channels, the militias can listen to the communications of others, and use this intelligence to their advantage, and therefore, the disadvantage of others [74].

c Terrorists: A terrorist has different purposes as looters or non-cooperative user's behaviour. For instance, he wants to create fear in the population, to gain international publicity for a terror group, but also to support a political or religious ideology, perceived or actual inequitable treatment, among other factors [133, 134].

d Looters: During Hurricane Katrina of 2005, fabricated reports of the shooting of rescuers and civilians, acts of violence, were reported [129]. The spread of rumors about looting and the lack of authority's presence contributed to a general rise in panic and a wide distribution of inaccurate information to citizens. Attackers used this information and looted abandoned properties or tried to take the resources of isolated community residents.

e Politically motivated organizations: In the Russian - Georgia conflict of 2008, governmental and civilian infrastructure was the victim of cyber-attacks, whose primary purpose was to disrupt and to compromise communication within Georgia, as well as to gather intelligence from and about military and political groups [128].

3.6 SUMMARY

Foundational security features become mandatory to minimize significant risks.

Technologies summarized in Section 3.3 implement technical solutions to enable D2D communication without any central infrastructure, however, none of them provides an adequate implementation to be considered as the most feasible solution for ECSs. There is no feasible solution that supports multihop, long-range communication and a transmission data rate up to 100 Mbps among the off-the-shell devices. Most of them do not scale sufficiently well in terms of the number of users or, in the case of Bluetooth, also have a significantly limited range. Other solutions, such as Wi-Fi ad hoc, are outdated and imply high energy consumption. Also, the lack of interoperability between existing solutions confirms the need for a cross-platform solution that does not exclude most of the conventional smartphones used by the population.

Existing commercial solutions provide most of these services, however, they are based on a centralized client-server architecture.

Existing commercial post-disaster solutions individually provide most services mentioned in Section 3.4. However, as of today, all of them are highly dependent on centralized infrastructure, i. e., based on a client-server architecture. For example, some websites or apps supply interactive maps for actual or potential disasters, such as hurricanes or tsunamis (Disaster Alert [135]). Additionally, many solutions enable

users to report an incident and to get feedback about the current status of service restoration (FEMA App [95]). Furthermore, although most of these services exist for institutions and organizations, we are not aware of citizen-oriented Resource Market Registries or Tasking Services. Even if they were available, dependence on communications infrastructure would remain an obstacle to their use.

Finally, as mentioned in Section 3.5, security is often completely ignored due to missing knowledge of security mechanisms or the complexity of secure communications. Nevertheless, foundational security features, like authentication, confidentiality and integrity become mandatory, as without those features significant risks arise, e. g., false information can be distributed during crises, resulting in confusion or a loss of trust amongst recipients.

4

REAL-WORLD EVALUATION OF A SMARTPHONE-BASED EMERGENCY COMMUNICATION SYSTEM

In the previous chapter, we have summarized and discussed the importance of smartphone-based communication networks in emergency response scenarios, where communication infrastructure is impaired or overloaded. In this chapter, we present the results from the field test to gain insights from civilian behaviour when utilizing smartphone-based communication networks in disaster scenarios. These results have been previously published in [3], and are extended in this thesis. The chapter is organized as follows. We first introduce our motivation and contribution in Section 4.1. The field test setup, the general device configuration, as well as the description of the data collection methodology are provided in Section 4.2. The gathered data comprises user interaction, mobility and additional sensor readings, that can be used as a foundation for simulations for present and future disaster communications systems. Next, we analyze the collected data in Section 4.3, highlighting scenario-specific interaction and movement behaviour of participants. In Section 4.4, we present related work. Finally, some concluding remarks are given in Section 4.5.

4.1 MOTIVATION AND CONTRIBUTION

To adapt and improve these emergency communication systems from the lessons learned, they should be ideally tested during a real crisis [48], or a sufficiently realistic field exercise. The later has the advantage of avoiding unnecessary risk for all concerned. However, most of them are evaluated using simulation models, trying to mimic realistic user behaviour and environmental characteristics for post-disaster scenarios. Despite simulations being an essential mechanism, e. g., to evaluate performance and scalability of systems, they normally lack important characteristics of real-world human behaviour, especially of civilians in disaster scenarios. The simulation models are either *(i)* solely based on the analysis of tactical issues of civil protection and input from FEMA or other organizations [136], *(ii)* relying on traces gathered in everyday life, e. g., on campuses, during conferences, or in office buildings [45–47], or *(iii)* only considering behaviour of professional disaster relief personnel [137, 138].

Simulations lack important characteristics of real-world human behaviour, especially of civilians in disaster scenarios.

Yet, to design and evaluate works targeting disaster relief it is necessary to consider and understand real-world human behaviour, specially of civilians in disaster scenarios. To this end, we conducted

a large-scale field test in conjunction with experts from the German Federal Office of Civil Protection and Disaster Assistance (BBK), the German Federal Agency for Technical Relief (THW), local fire departments, and other NGOs. The main idea of this test was to asses the effectiveness of such a solution and to evaluate the usage by emergency services that relied solely on ad hoc communication. Over the course of one day, we gathered data from smartphones distributed to 125 participants in a scripted disaster event. Additionally, participants were asked to answer a set of question about the subjective experience when interacting with our Android app as well as with specific disaster services. Figure 4.1 shows the setup and configuring of the mobile devices for the field test.

Over the course of one day, we gathered data from smartphones distributed to 125 participants in a scripted disaster event.

Figure 4.1: Configuring of the mobile devices for the field test.

4.2 FIELD TEST SETUP AND DATA COLLECTION

The Field test took place in September 2017 at the military training area *Senne* near Paderborn in Germany. Figure 4.2 visualizes the layout of the field test area containing three villages (A, B, C) made of brick buildings. The linear distance between villages B and C is 700 m and between A and B is 4 km. 125 volunteers participated in the test between 09:30 and 16:30. Participants had to find family members, help each other, and share resources after a complete breakdown of the communication infrastructure caused by a grid blackout. To evaluate user behaviour in stressful situations, two fictive events took place in villages A and B, involving professional actors. In village A, a lightning strike hit a gas station at 13:00 and injured a couple of

Participants had to find family members, help each other, and share resources after a grid blackout.

Figure 4.2: Senne layout: the large-scale field test area.

A lightning strike and a chemical accident (fictive events) took place in villages A and B, involving professional actors.

people with the need for immediate help and shelter. In village B, hazardous substances were released at 14:30 after the cooling system at a chemical plant failed, requiring immediate evacuation. Figures 4.3a and 4.3b show volunteers during the lightning strike in village A and the chemical accident in village B.

Actors further increased distress by role playing, for example a mother desperately searching for her child. At the beginning of the field test, participants received a smartphone and a portfolio with information about their character. The character was completely fictitious to protect the privacy of participants. Participants were divided into three groups and distributed over the three villages. The portfolio contained home address (village), age, and family relations of the respective character. Additionally, tasks like search for your family members, meet at the home address, or search for specific resources such as water or medical supply were stated. Each participant started with at least three resources. The main goal of the field test was the evaluation of a smartphone-based communication network supporting a set of emergency services (e. g., *SOS Emergency Messages*, *Resource Market Registry*, *Person-Finder*) as described in Section 3.4. In addition to technical insights into the underlying ad hoc network, we also addressed the usability and utilization of the proposed services in a realistic scenario.

4.2.1 *Data Collection*

A mobile application smarter *was developed as proof-of-concept for Android-based smartphones.*

We implemented a proof-of-concept of a set of emergency services to demonstrate the feasibility of smartphone-based communication networks in emergency response scenarios. A mobile application *smarter*[1] was developed on Google Nexus 5, 6P and Samsung Galaxy S6 devices. Figures 4.4 and 4.5 show the screenshots of the *smarter* app.

It uses the bundle protocol implementation from IBR-DTN [139, 140] to communicate and exchange data directly between nearby

1 http://smarter-projekt.de/demonstrator/

(a)

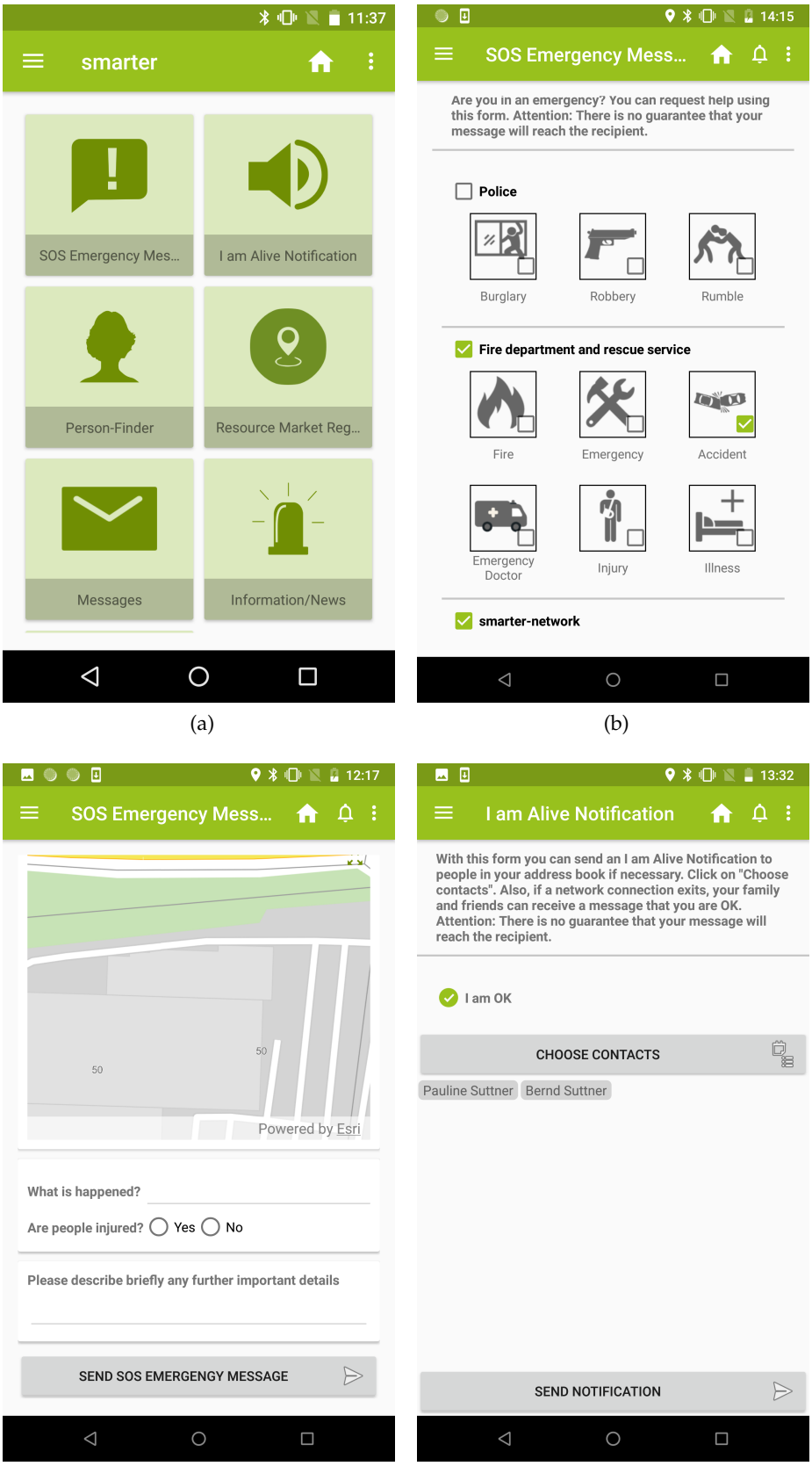
(b)

Figure 4.3: Volunteers during the field test: (a) the lightning strike in village A, and (b) the chemical accident in village B.

We use IBR-DTN to communicate and exchange data directly between nearby devices.

devices. IBR-DTN was designed for mesh nodes. The core functions are implemented in C++. Additionally, it offers a library in Java to port the functionality to Android-based smartphones.

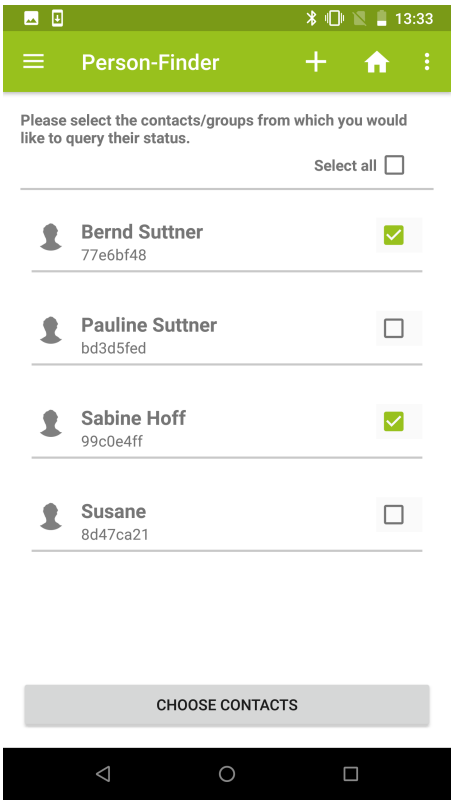
On each device *smarter* was pre-configured with a personalized address book containing only contacts according to the portfolio of the respective character. The smartphones were delivered without a Subscriber Identity Module (SIM) card, i. e., they had no connection to a mobile phone provider. In addition, no Internet access was



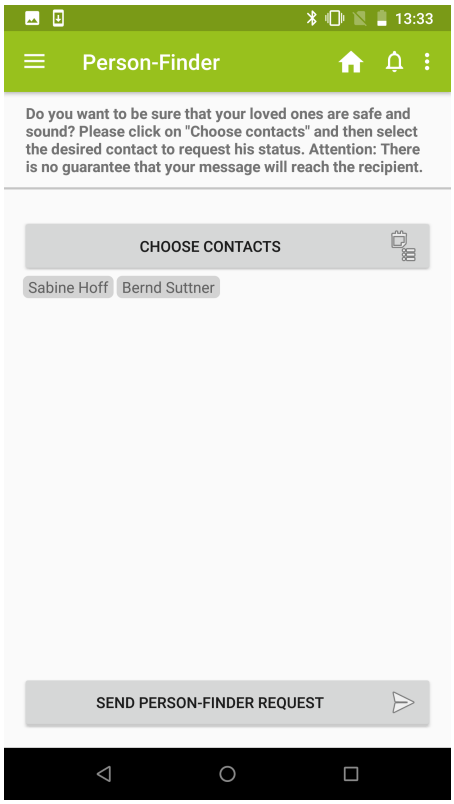
(a) (b)

(c) (d)

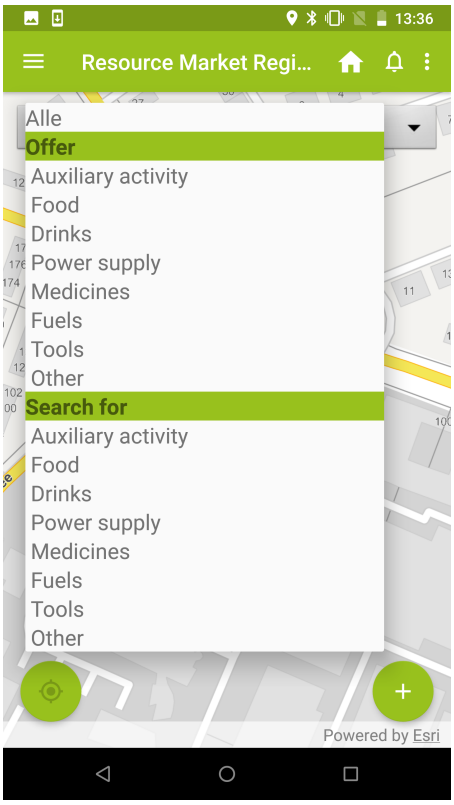
Figure 4.4: Screenshots of the SMARTER app: (a, b, c) SOS Emergency Message , (d) I am Alive Notification.



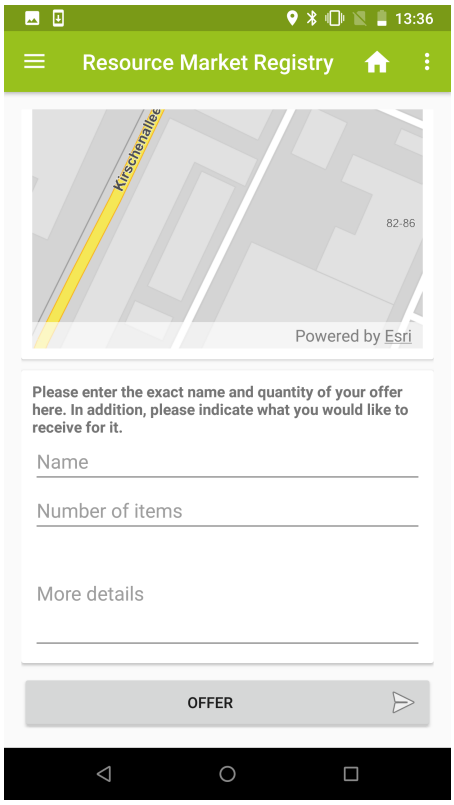
(a)



(b)



(c)



(d)

Figure 4.5: Screenshots of the SMARTER app: (e, f) Person-Finder, (g, h) Resource Market Registry.

provided. During the whole field test, we recorded sensor, network, and application-related data. To compensate the increased energy consumption, each participant received a battery pack with sufficient energy for the duration of the field test. Sensor data was recorded on average every second and saved in a local SQLite database. We recorded Global Positioning System (GPS) locations, accelerometer readings, brightness, air pressure, and gyroscope readings. Previous research has already shown, that data gathered from this set of sensors supplies sufficient information to recognize a person's activity, as well as to identify if a person performs a disaster related activity such as crawling on the floor or walking with an injured leg [141]. The brightness sensor can be used to determine if the phone is in the pocket or held in the hand of a user. The sensor data can be used for future research directions. We logged all user interaction with our application. We also captured sensor data and network statistics with an additional logging framework. We used the device-specific unique identifier *DTN-ID* provided by IBR-DTN to tag all measurements.

The smartphones had neither Internet nor connection to a mobile provider.

We log sensor, network, and application-related data.

4.3 DATA ANALYSIS

We investigate the performance and scalability aspects of the scripted scenario by analyzing delay and hop distribution, number of neighbours, participant speed, and connection data between mobile devices. We mainly focus on these metrics, as they are the most common metrics required by simulation tools and the mobility models. Table 4.1 summarizes the results of our data analysis. To prevent the results from being inconsistent because the participants were transported in a bus to each village, we have considered only the data collected between 10:30 and 15:30 for our analysis. Due to various problems: hardware (smartphone model, SD card overloaded.), software (logging, app malfunctions.), user device handling, and the loss of one device, we could not gather a complete dataset of all devices. Out of the 125 devices, 119 contributed to the network and app dataset and 96 were used to build the GPS traces. As the devices had neither access to Internet nor connection to any other time synchronization source, it was not possible to have a perfect time synchronization between all devices. Because of that, we consider the devices with the most number of connections (from 90 connections) as those with the reference time, i. e., we took the timestamp of those as the ground truth and synchronized all other devices based on this information.

Out of the 125 devices, 119 contributed to the network and app dataset and 96 were used to build the GPS traces.

4.3.1 *Mobility Traces*

This part analyzes the GPS data of each device to quantify the participant walking speed and the number of neighbours that each participant had throughout the whole field test.

Table 4.1: Results from the data analysis.

Metric	Median	Mean	Standard deviation
Connection distance (m)	30.21	44.47	41.45
Contact duration (s)	96.00	299.75	630.17
Walking distance (km)	11.25	11.22	4.81
Walking speed (m/s)	0.18	0.52	0.62
Number of neighbours (d = 44m)	7.13	7.26	2.40
Message size (byte)	303.00	567.97	607.30
Multicast delay (min)	15.22	19.89	18.33
Multicast propagation (# nodes)	28	25.8	18.39
Cluster coefficient	0.29	0.30	0.05

(a)

Figure 4.6: GPS track at the training area Senne.

Some participants were isolated from the network most of the time as they used alternative routes.

We replicated the movement of each participant throughout the whole training area as well as in each village as depicted in Figure 4.6. Most of the participants walked the same route on which they were transported to each village. However, there were also some users, who used alternative routes. As a result, they were isolated most of the time from the network, establishing either few or no connections with other participants.

4.3.1.1 *Participant Walking Speed*

The speed recorded along the field test confirms previous results showing normal person speed of 0.5 m/s.

Figure 4.7 visualizes the participant speed recorded along the field test. First, it confirms previous results about the normal person speed with an average of 0.5 m/s [136]. Second, we also observed some quite static behaviour of participants (around 35 % of the time), with few peaks corresponding to speeds between 0.25 m/s and 1-1.5 m/s. These values are the result of the mobility pattern reproduced by our specific

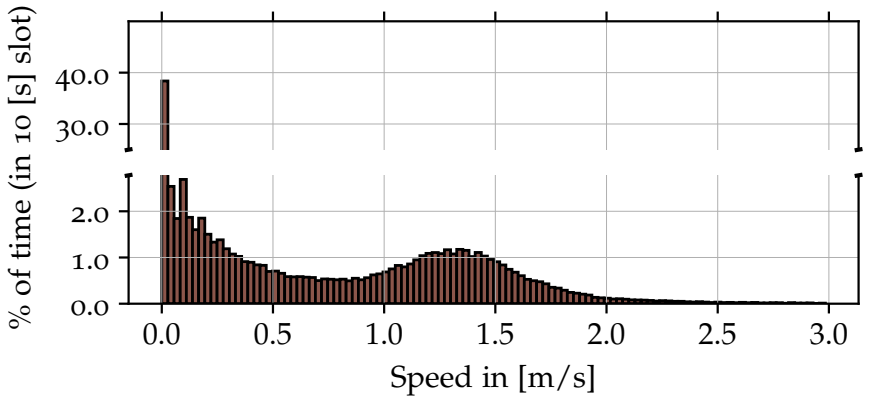


Figure 4.7: Walking speed distribution.

scenario: the static time represents, e. g., breaks in each new encounter in order to exchange information and resources. The peaks are the contribution of the participant movement from a village to another one. Finally, by considering the walking speed between 0.5 m/s and 2 m/s, Figure 4.7 shows a normal distribution rather than a uniform distribution. Therefore, future research should consider selecting a walking speed with a normal distribution for simulation experiments. By using such a distribution it is possible to represent a more realistic network where the nodes move fast and slow, e. g., injured people can be simulated with a walking speed lower than a non-injured people.

The walking speed has a normal distribution rather than a uniform distribution.

4.3.1.2 *Number of Neighbours*

For our analysis, we chose three values to set the maximal distance between two devices considered neighbours: 25, 44 and 110 m. We took these values based on the results from the analysis of the network data as shown in Figure 4.14: most of the 50 percent up-connection were within approx. 25 m, the mean was around 40 m, and 90 percent of the connections were within 110m. Figure 4.8 shows the distribution of the neighbours during the field test. On average, each participant had between six and eight neighbours. Most of the contacts occurred at the start and the end of the test (around 10:30 and 15:30), during the lunch (between 12:00 and 12:45), as well as during our two simulated events (between 13:00 and 15:00). Moreover, even in the walking phase most of the device had at least three neighbours. This indicates that the network density during the field test was mostly sparse, on average many devices had few close neighbours.

Participants moved in small groups most of the time.

Many of the groups were built upon the relationships between users as described in the portfolio. But, we also found that participants moved in small groups most of the time, including persons who are not in their family circle.

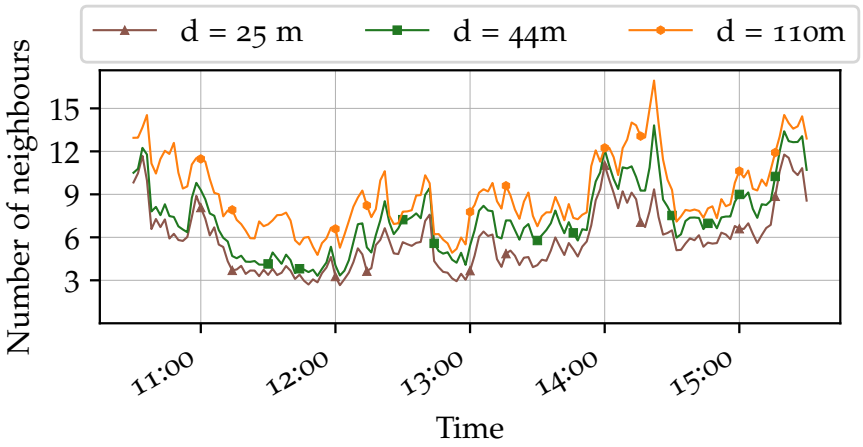


Figure 4.8: Number of neighbours aggregated over 2 minutes and considering three maximal distance between two devices.

4.3.2 *Application Interaction Patterns*

This section presents the results of the user interaction analysis from the application data.

4.3.2.1 *Number of Messages*

During the whole field test participants generated 2,236 unicast messages.

The messages generated with our application were sent as a bundle via IBR-DTN. Between 10:30 and 15:30 the participants generated 2,236 unique messages. This corresponds to an average of 7.5 unique messages generated per minute. During this time, the total network traffic was of 14,649 messages. As depicted in Figure 4.9, the participants began the field test very motivated and created many messages during the first hour. Resulting in a peak at around 10:30. Afterwards the amount of messages slowly declined to almost none at around 12:30. Upon the announcement of lunch the usage increased again, as well as at the beginning of the subscenarios. While we explicitly forbade use of the app before reaching the starting points most participants did not comply. For future field test we advise enforcing such rules in software rather than trusting the participants.

User participation decreased over the time.

4.3.2.2 *Use of Emergency Services*

Resource Market Registry and SOS Emergency Messages generated the most network traffic, as both were multicast messages.

The participants were bound to only use our smarter-app to interact with the network. Figure 4.10 visualizes the network traffic grouped by services as well as usage over all services by considering the messages created by users. The message size was on average 567.97 bytes with a standard deviation of 607.30 bytes. Considering the interconnection times and the theoretical bandwidth of the Wi-Fi channel, the generated traffic is well below of this theoretical limit. This is highly dependent on our design choice, to solely provide text based services.

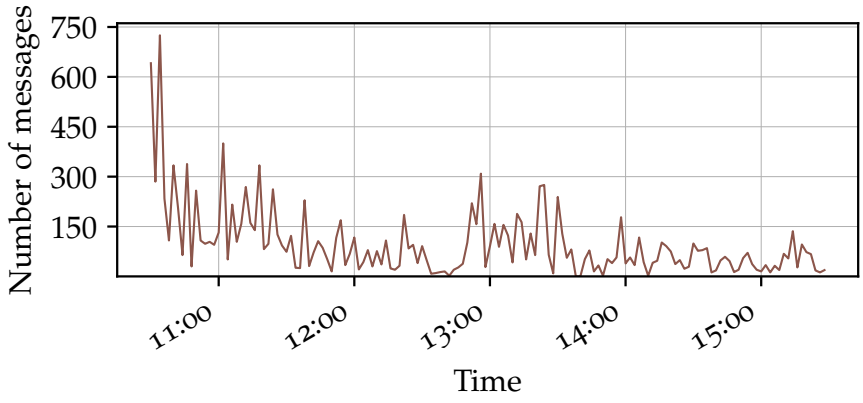


Figure 4.9: Received multicasts aggregated over 2 minutes

Including multimedia content as images and audio or video recordings could have overloaded the network. The trend of services usage was similar to a normal situation: participants used mainly the chat service. Interestingly, the SOS Emergency service and Resource Market were not used as expected. We believe that this result is mainly due to a lack of familiarity with these services. Although these services can be very helpful during a disaster, they lose importance and are useless if users do not know how to use them. An important point for the deployment of future systems is to guarantee an adequate level of user familiarity with their services. As shown in Figure 4.10, the usage pattern of the services changes if we consider the total network traffic. In this case the *Resource Market Registry* (approx. 70%) and *SOS Emergency Messages* (approx. 20%) generate the most network traffic. This result is reasonable as both messages are multicast, i. e., they are retransmitted by each user on each encounter.

4.3.3 *Network Data*

In this section, we explore information about connection duration and connection distance of a device pair. We also present the propagation delay of the messages.

4.3.3.1 *Node Degree*

We analyze the empirical distribution of the network node degree and compare with the number of neighbours. As depicted in Figure 4.11, the number of established connections remained below the number of possible connections. This information highlights the need to improve mechanisms for establishing connections between devices under real conditions, and thus to optimize D2D communications. Moreover, Figure 4.12 visualizes node degree and number of neighbours over time. Although both distributions present similar behaviour at the

The number of established connections remained below the number of possible connections.

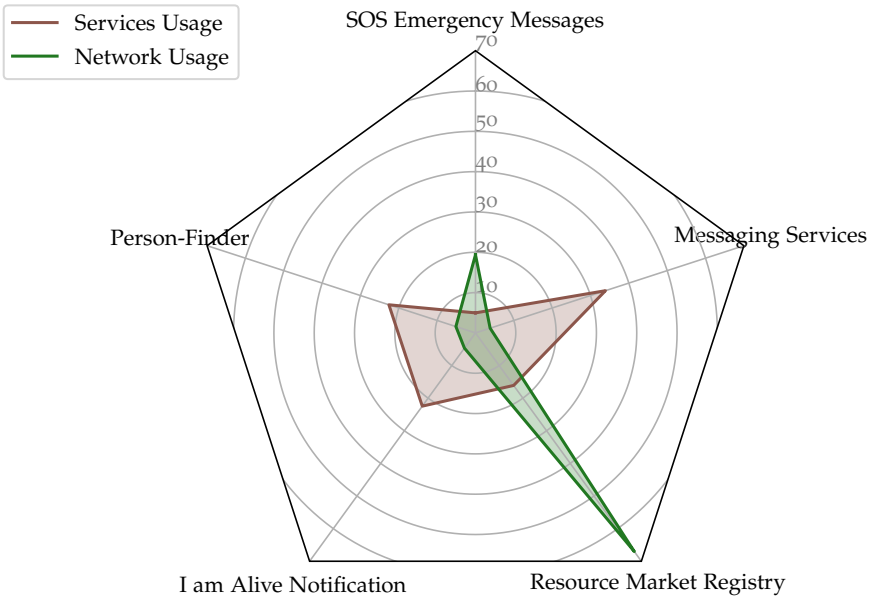


Figure 4.10: Smartphone-based Communication Networks for Emergency Response (SMARTER) service usage.

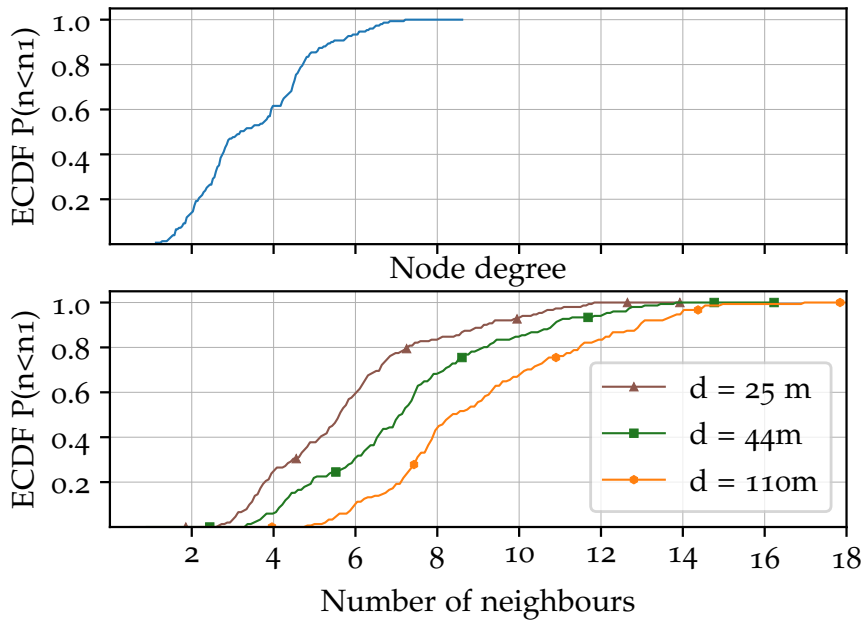


Figure 4.11: ECDF node degree and number of neighbours.

beginning, they differ slightly between 13:00 and 15:30. We cannot state with certainty the reason for this difference. As the number of neighbours is obtained from the GPS data and the node degree from the network data, it may influence this variation. We assume that the node degree was affected by the location of the participants as

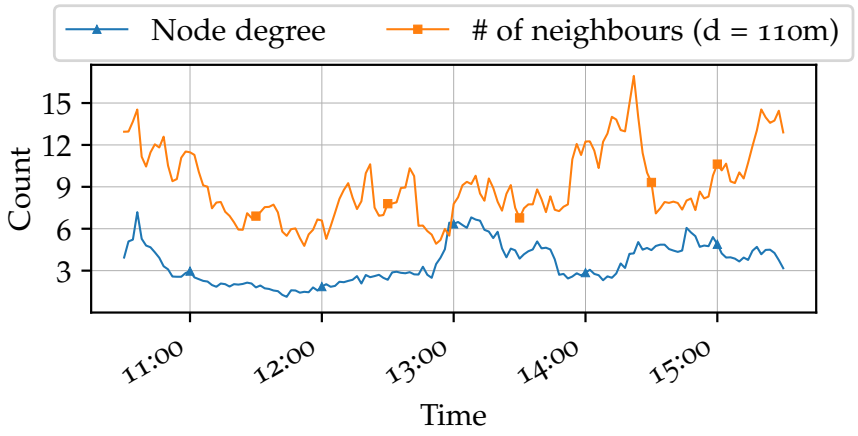


Figure 4.12: Node degree and number of neighbours over time aggregated over 2 minutes.

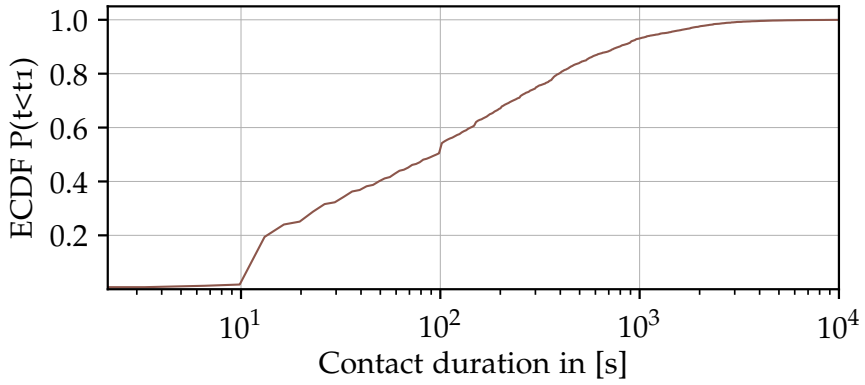


Figure 4.13: ECDF of the connection duration.

well as the weather conditions. During these slots of time participants relocated inside buildings because it was raining.

4.3.3.2 *Connection Duration*

Most of the connections had a duration time of 100 seconds.

We show the empirical cumulative distribution function in Figure 4.13 using a log scale for the x-axis of the duration of a connection between two devices. Interestingly, we found that most of the connections had a duration time of 100 seconds. This value is the result of the behaviour mentioned in Section 4.3.1: where participants moved most of the time in small groups. This information can impact directly on some assumptions and decisions in forwarding strategies: e. g., the time available to exchange data in each device encounter.

4.3.3.3 *Connection Distance*

90 percent of the established connections was within approx. 110 m.

As depicted in Figure 4.14, 90 percent of the established connections was within approx. 110 m. This value can be considered as expected

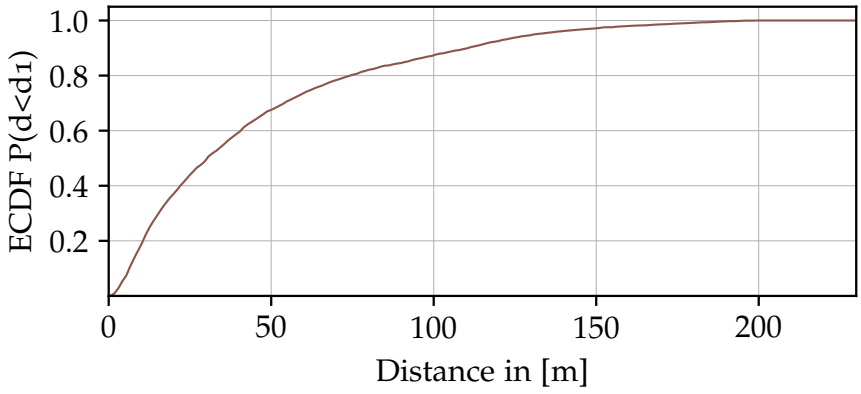


Figure 4.14: ECDF of the connection distance.

in an area where a free Line-of-Sight (LoS) is given. Connections with a distance longer than 150 m are uncommon, but also possible.

4.3.3.4 *Propagation Delay*

The propagation delay describes the delay of a message from sender to destination. Figure 4.15 shows the propagation delay for multicasts during the defined lifetime of a bundle, in our scenario it was 60 minutes. We consider two significant cases: the delay for the best performing multicast as well as for the median. On average a bundle was successfully transmitted to 25.8 nodes or 20.8 percent of the network. The best performing multicast reached a total of 94 nodes or 75.8 percent. Overall the results show, that 20 percent of the messages got delivered to the destination directly. This can easily be explained by looking at the mobility patterns of the participants. Since most of them formed groups and had always a couple of neighbouring nodes nearby, multicasts originating in one group reached each group member without delay. Upon a meeting of different groups, many messages are delivered in a short timeframe, which explains the steps visible in the figure. The initial direct distribution of the best multicast to 20 neighbouring nodes in under one second shows the performance capabilities of the network.

The best performing multicast reached a total of 94 nodes or 75.8 percent.

4.3.3.5 *Cluster Coefficient*

A common metric to measure the interconnectivity of nodes over time is the cluster coefficient as described in [142]. The cluster coefficient indicates the degree to which nodes tend to form groups or cluster in a network. We calculated it based on the network logs. The results in Figure 4.16 show, that the highest connectivity was right at the beginning of the field test with around 0.41. This was expected, as the participants turned on their devices before the official start of the test, while they were still waiting to be brought to their starting point. Two

The highest connectivity was right at the beginning of the field test with around 0.41.

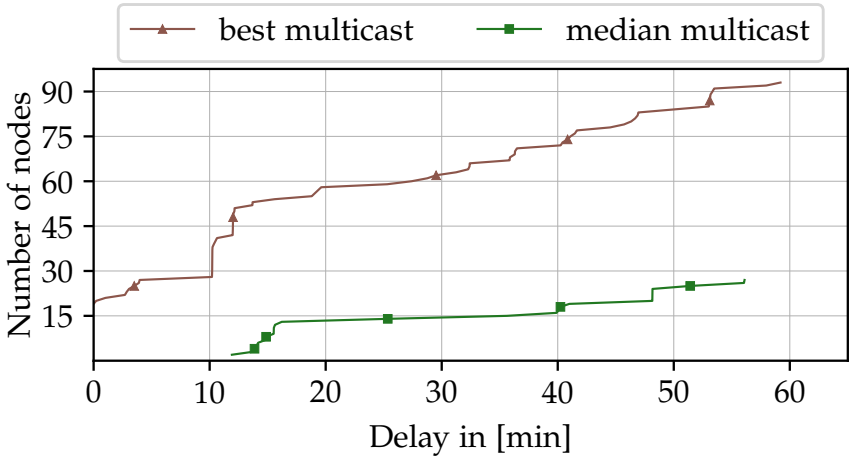


Figure 4.15: Propagation delay for multicasts

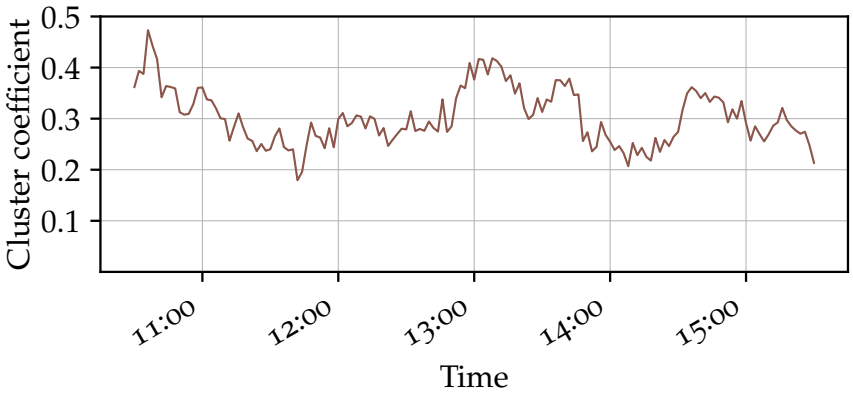


Figure 4.16: Cluster coefficient of the interconnectivity of nodes over time.

peaks at around 13:00 and 14:30 reflect the lunch break followed by our two subscenarios. The low spot at 14:00 is not reflect in the GPS traces, meaning that the connectivity of the devices decreased while they should have been in close proximity. This is most likely due to the then occurring rain and the following reaction of the participants to seek shelter in nearby buildings. The loss of LoS and the walls of the buildings reduced the effective communication range.

4.4 RELATED WORK

Most existing works rely on synthetic movement models, but for post-disaster systems realistic simulation settings are crucial for getting meaningful results.

There is a variety of useful infrastructure independent services for emergency response [101, 104]. Usually, researchers utilize simulation tools to evaluate such services or their communication protocol. Simulation-based evaluation provides advantages in terms of reproducibility and cost-efficiency. But, considering a disaster as a particular use case, realistic simulation settings are crucial for getting meaningful

results. Specially in MANETs, realistic movement of nodes is crucial for a meaningful performance evaluation. Yet, most existing works rely on synthetic movement models such as a random walk or random waypoint [44]. To address this problem, researchers have already proposed different mobility models for post-disaster systems [136, 143, 144]. However, most of them are based on weak assumptions about user behaviour such as walking speed or grouping, without being able to prove if such assumptions depict reality. As surveyed by Aschenbruck et. al. [44], there is a plethora of trace-based movement models based on real human movement records. However, these trace-based models cover everyday movement patterns. [137] is the only known disaster-related analysis of movement behaviour that uses GPS data of firefighters, but they do not consider civilians. In addition, due to the privacy concerns, the data is not made publicly available. We are the first to provide insights into the behaviour and the interactions of civilians in a post-disaster scenario based on a large-scale field test.

4.5 SUMMARY

In this chapter, we presented a large-scale field test of a smartphone-based ad hoc communication network in an emergency response scenario. During a scripted emergency scenario, 125 participants used a mobile application to find family members, reach out for help, and share resources after a complete breakdown of the communication infrastructure. We gather mobility traces, smartphone sensor data, application interaction patterns, and network logs of civilians in a large-scale field test specifically for emergency response. We present a thorough analysis of the data gathered during the seven hour event, highlighting scenario-specific mobility and network characteristics. Our results show, that a smartphone-based ad hoc network between more than one hundred smartphones provides sufficient connectivity for relevant emergency services. As mentioned before, due to the wide range of scenarios and their specific characteristics, it is difficult to generalize settings and metrics for all ad hoc communication networks in emergency scenarios. However, we firmly believe, that it is necessary to take into consideration our findings in the design and development of such systems. For instance, given the behaviour of participants, connections lasted five minutes on average, exceeding the estimations stated in related work. Group-building contributed to these results, leading to devices having three neighbours on average. This finding about stable connections can be very helpful in forwarding strategies, e. g., to adapt some assumptions and decisions about the time available to exchange data in each device encounter. Additionally, real-world impact of obstacles and crowd density lowered the achievable communication range. These results are very promising, especially in terms of the assumptions about connectivity, since in real circumstances the

We provide a sound analysis of the data gathered during the seven hour event, highlighting scenario-specific mobility and network characteristics.

density of users is even higher than in our experiments. Our results confirm the importance of real-world tests specially if systems are designed for scenarios that are heavily affected by human behaviour.

Part III

IMPROVING THE RESILIENCE OF SMARTPHONE-BASED EMERGENCY COMMUNICATION SYSTEMS

This part of the thesis presents several mechanisms to improve the resilience of smartphone-based ECS. Chapter 5 provides a decentralized solution to deal with the security services. Chapter 6 describes the proposed adaptive neighbour discovery scheme for saving energy in smartphone-based ECS. Finally, Chapter 7 presents a mechanism to mitigate the impact of scarce infrastructure after a disaster by integrating the Internet of Things (IoT) devices that remain operational in case of disaster into smartphone-based ECS.

5

SECURE SELF-ORGANIZING BOOTSTRAPPING FOR EMERGENCY COMMUNICATION SYSTEMS

We have presented the insights from a real-world evaluation of a smartphone-based emergency communication system in Chapter 4. In this chapter, we present Sea of Lights (SoL)[1], a lightweight scheme for bootstrapping Device-to-Device (D2D) security and for wirelessly spreading it to enable secure distributed self-organizing networks. It has been previously published in [4], and has been extended in this chapter.

This chapter is organized as follows. In Section 5.1, we briefly present our motivation. The system model and the adversary model are summarized in Section 5.2. Section 5.3 describes the design and introduces the architectural concepts of the SoL framework, as well as provides implementation details. We present the results of the evaluation of SoL, covering both simulation results in Section 5.4 as well as measurements from our Android implementation in Section 5.5. In Section 5.6 we summarize related work. Finally, in Section 5.7, we discuss implementation and performance issues.

5.1 MOTIVATION AND CONTRIBUTION

Mobile users using smartphones dominate Internet usage.

Today's conventional communication infrastructure is centered around a rich set of applications such as social media, emails, which build on the Internet and are commonly designed in a centralized fashion and scale to billions of users. By now, mobile users using smartphones dominate Internet usage. These smartphones can support hundreds of mobile applications, which heavily rely on third-party providers to offer basic security services. Identity providers such as Google or Facebook have active user bases of two billion each, and the subscriber number of mobile operators exceeds five billion unique users as of early 2019. However, recent disasters [14–16] severely affected the information and communication capabilities of the population by damaging infrastructure, making communication systems unavailable, or knocking out the power. Consequently, millions of people in need of help were literally left "in the dark", without ready-to-use access to backup power and stripped of even essential means of communication. Hence, in the absence of central infrastructure, the users are left without practical solutions to bootstrap security on their mobile devices.

In the absence of central infrastructure the users are left without practical solutions to bootstrap security on their mobile devices.

1 The name is inspired by silent protests such as candlelight vigils, where light is spread among the candles of a large group of people, effectively forming a "sea of lights".

As a result, mobile application usage is severely restricted to support users in such scenarios. A typical assumption in emergency scenarios is that only honest users participate in establishing and running the network, and existing solutions often forgo security means [1]. Besides, users with malicious intent may limit or affect communication, thus causing severe threats to the credibility and reliability of the data.

Most current WoT solutions are ill-suited for cross-application support on mobile devices and do not support strong protection of key material using hardware security modules.

Distributed solutions to bootstrap security, such as the Web-of-Trust (WoT) exist. However, existing approaches are still complex and require educated users [145]. Moreover, most current WoT solutions are ill-suited for cross-application support on mobile devices and do not support strong protection of key material by means of hardware security modules.

In contrast, SoL is designed to complement existing self-organizing network solutions by providing a lightweight and agile solution for decentralized authentication, key management, and trust management. SoL comprises two layers. *(i)* The *Trust Management Layer*, which manages all operations related to trust relations. This is in charge of bootstrapping on demand, and of creating and maintaining trust relations. *(ii)* The *Key Management Layer*, which is responsible for generating key material and managing access to these keys in a secure fashion. This layer cares for management the key security, e. g., by choosing an appropriate key storage according to hardware capabilities and available secure elements on the mobile devices.

5.2 SYSTEM AND ADVERSARY MODEL

In this section, we provide an overview of the system and the threat model considered in this chapter.

5.2.1 *System Model*

Each device is imprinted with an identity, which is unique and unchangeable.

We consider users owning mobile devices capable of direct device-to-device communication. In the following, we use the term entity to refer to the logical entity formed by an authorized user and her device. Each device is imprinted with an identity, which is unique and unchangeable. For a smartphone, this could be the International Mobile Equipment Identity (IMEI), a unique device fingerprint. Each device has a mechanism to discover devices in its proximity, such as a one-hop neighbour discovery mechanism. Applications running on the devices are assumed to be independent of each other, i. e., each application can define its own set of security requirements. No prior trust relationships or security association between entities exist, i. e., no information or knowledge about other entities is stored on a device beforehand. Centralized infrastructure to bootstrap security is unavailable. Utilizing direct contact and with the users in the loop, pairwise trust relationships between entities can be established. Note

Applications running on the devices are assumed to be independent from each other.

that we do not assume any technology for the data routing/forwarding/spreading since SoL is agnostic regarding such mechanisms.

5.2.2 *Adversary Model*

We assume adversaries that can act passively or actively as insiders, i. e., our adversary is a regular user of the network. Adversary capabilities follow the Dolev-Yao assumptions [146]: the adversary is, hence, capable of active interception or modification of traffic, she can fabricate and destroy messages, but is not able to break cryptographic primitives. The key goal of SoL being to bootstrap security, i. e., to provide authentication, key management and trust management services to the users, we define the main attack goals to be to disrupt these services. In particular, this entails impersonating other entities within the network.

The main goal of an arbitrary adversary is the impersonation of another participant in the network.

5.3 THE SECURE BOOTSTRAPPING CONCEPT

In this section, we present SoL, a lightweight scheme for bootstrapping device-to-device security and for wirelessly spreading it to enable secure distributed self-organizing networks. SoL is designed to complement existing self-organizing network solutions by providing a lightweight and agile solution for decentralized authentication, key management, and trust management. Any third-party mobile app can utilize the services of SoL, which offers an interface to access its security services. The security configuration can be performed at per-app granularity. Public/private key pairs generated by a third-party application (=sub-keys) can be authenticated with SoL. Hence, our framework registers the public key of a sub-key, signs it, issues a certificate and is further responsible for its distribution.

SoL complements existing self-organizing network solutions by providing a solution for decentralized authentication, key management, and trust management.

5.3.1 *Overview*

In this section, we highlight the design concept and architecture of the proposed SoL framework. We explain the technical realization in detail in Section 5.3.4. SoL is a framework that provides cross-application security services for device-to-device communication settings. Our architecture comprises a key management as well as a trust management component, which are managed and developed as two independent elements.

5.3.2 *Decentralized Authentication*

The term *trust* has a vast meaning, from the psychology perspective to networking. In this chapter, we refer to the definition proposed by authors in [147] as follows:

Definition 4. *Trust:"...is a subjective assessment by an agent/other peer node on the reliability and accuracy of information received from or traversing through that node in a given context [...] Trust reflects the belief [...] on the honesty, integrity, ability, availability and quality of service of target node's future activity/behaviour."*

The decentralized authentication bases on a simplified version of the WoT paradigm, where each mobile device generates its public/private key pair and signs the public key of other devices.

In our case, the proposed decentralized authentication is based on a simplified version of the WoT paradigm, where each mobile device generates its own public/private key pair and signs the public key of other devices. Similar to other WoT solutions, trust in SoL is determined by a trust level and a maximum certification path, the so-called degree. In contrast to Pretty Good Privacy (PGP), the trust level is not manually applied to different users. In our approach, the trust level is automatically assigned following the trust level rules defined as follows.

- **Ultimate (U)** for the owner,
- **Trusted (T)** for direct trust relations, where an object signed directly by **U** is trusted,
- **Known (K)** for transitive relations (second degree and further), where an object signed directly by **(T)** is known, or an object signed by **n**-**K** is defined as known. **n** represents the minimum number of known signatures required to validate an unknown signature. Additionally, the degree defines if a transitive relation can still be considered known. We do not set a fixed value of **n** and **degree**, but allow for user configuration. This variable configuration enables to tune the scalability of the system to different use cases.

Trust management is carried out in two main protocols: handshake and synchronization.

In our approach, trust management is carried out in two main steps, each implemented using a dedicated protocol. The handshake protocol covers the bootstrapping and establishment of mutual trust, and the synchronization protocol manages the unidirectional synchronization of the local trust repository. We denote a public key as *pk*, e. g., *pk[a]* is the public key of Device A. Note that a certificate is represented as *signature[issuer,subject]*, where *subject* is the device whose public key was signed, and *issuer* is the device who signed the public key of the subject, e. g., *signature[a,b]* represents the certificate of *pk[b]* issued by Device A.

5.3.2.1 *Handshake Protocol*

The Handshake Protocol covers the bootstrapping and establishment of mutual trust.

Figure 5.1 illustrates the data flow between two devices performing the handshake protocol. It consists of the exchange of public keys and signatures between devices in proximity, to establish a direct trust relationship between two devices. Furthermore, a verification method is needed to perform key authentication procedures. Our survey of existing pairing schemes [148] has shown that to improve both security and usability, it is also necessary to develop adaptable verification schemes that are independent of specific physical or human-computer interaction channels. In case of considering any human interaction in the verification procedure, it is additionally needed to include this interaction in the security chain of the system.

Human interaction should be included in the security chain of a system.

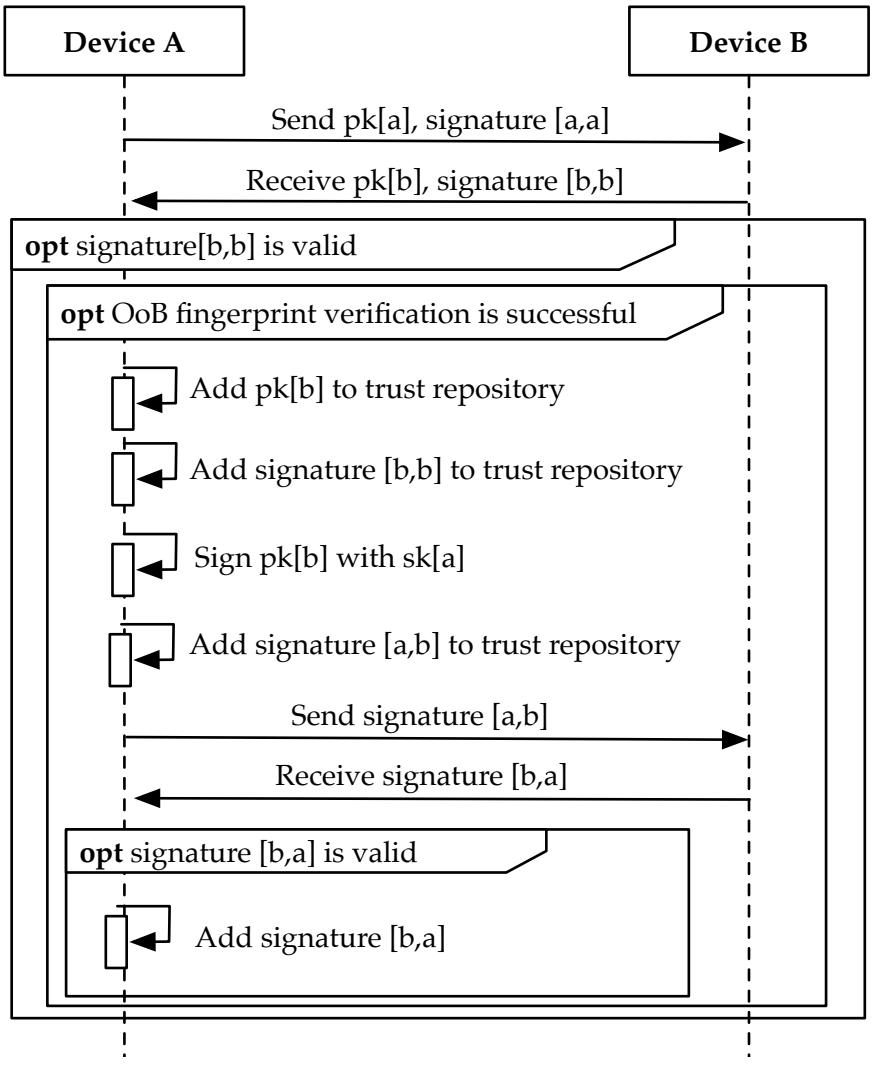


Figure 5.1: Bootstrapping trust process from *Device A*'s perspective.

Hence, in our framework implementation, we perform the key verification using existing Out-of-Band (OoB) verification methods (see Section 5.3.4). Since comparing all bytes of public keys can be tedious

and susceptible to errors, we use a short representation of these called *fingerprints*. In our approach, a fingerprint is the cryptographic hash value of any given public key. Once the OoB fingerprint verification is successful, the devices generate a certificate and assign a trust level according to the process mentioned previously. These certificates are then exchanged between devices and stored locally in their repositories.

5.3.2.2 *Synchronization Protocol*

The Synchronization Protocol manages the unidirectional synchronization of the local trust repository.

Once a trust relationship has been bootstrapped, the devices can obtain information about the transitive trust relations. Figure 5.2 clarifies this process.

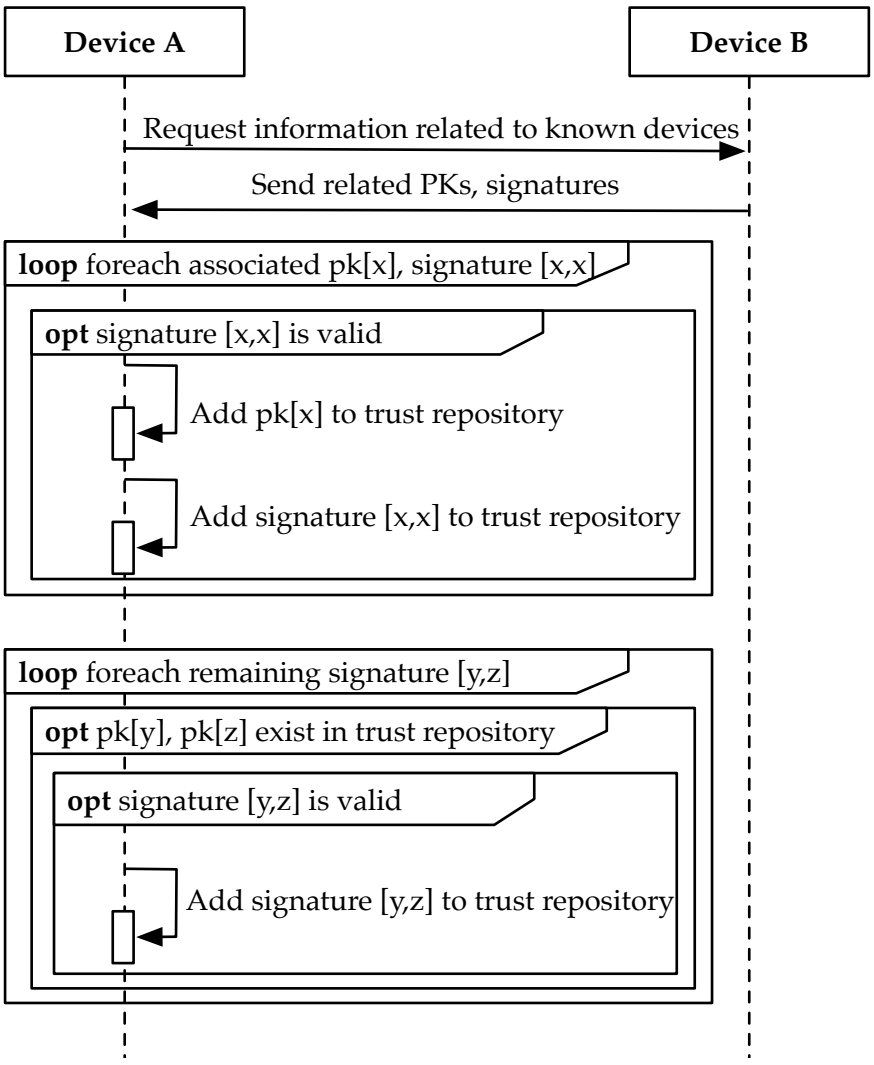


Figure 5.2: Unidirectional synchronization process from *Device A*'s perspective.

The synchronization of the trust repository between two devices operates as follows: *Device A* requests from *Device B* information

related to a set of known devices, *Device B* responds with the public keys and signatures related to the queried devices. *Device A* merges the information into its local trust repository. Finally, *Device B* performs the same procedure to synchronize his trust repository.

5.3.3 *Key Management*

One of the most important security aspects in any system is key management. For further discussion, we consider the definition presented by authors in [149] as follows:

Definition 5. *Key Management: "In order to have keys readily available for every communication, keys need to be managed securely and efficiently. [...] key management should introduce as less overhead as possible. Main goal of a key management scheme is to ensure confidentiality of information."*

The key management is responsible for the management and protection of the private authentication key from misuse and key extraction.

According to this definition, the key management component in our framework is responsible for the management and protection of the private authentication keys from misuse and key extraction. The proposed solution is designed and implemented as a flexible solution, where the methods for key management can be hardware- or software-based solutions. It depends on the methods supported by the devices, e. g., keys can be stored in external Near-Field Communication (NFC) tokens, TEE-based storage as AndroidKeyStore, etc. Note that irrespective of the method, the selected storage method requires a PIN, password or an additional unlock mechanism. Our approach involves two groups of keys: *(i)* the initial authentication key, which only aims to achieve authentication and trust between the devices, and *(ii)* sub-keys.

Sub-keys can be used to provide additional security properties.

Sub-keys are public/private key pairs, which can be used to provide additional security properties, e. g., confidentiality. A third-party app generates these keys and authenticates them with our framework using the initial authentication key.

5.3.4 *Architecture*

As shown in Figure 5.3, SoL is designed as a two-layer framework, which handles both trust and key management. It resides on the application layer of the Android architecture.

5.3.4.1 *Trust Management Layer*

The main task of this layer is the maintenance of the trust relationships on a device.

The main task of this layer is the maintenance of the trust relationships on a device. It includes the management of the trust repository, controlling the data, e. g., existing public keys, certificates, sub-key certificates, as well as checking the validity and trustworthiness of incoming data. Furthermore, this layer performs the protocols mentioned in

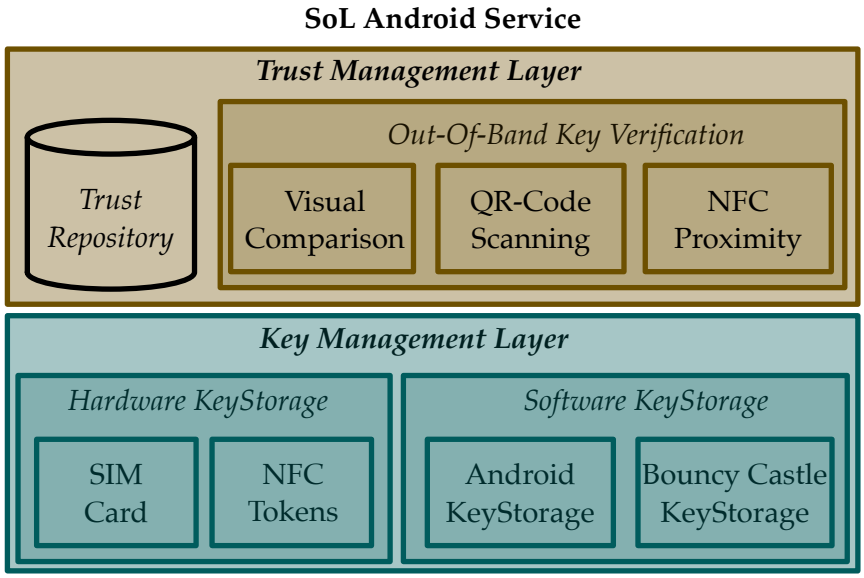


Figure 5.3: The SoL architecture is designed as an Android service.

Section 5.3.2: handshake and synchronization. We use *fingerprints* and *key IDs* to identify a longer key with a short representation. The fingerprint is calculated using SHA-256, and the key ID is derived from the 64 LSBs of the public key. We create a directory that contains all data concerning trust relations for each known device (=*subjects*). The directory's name is the hexadecimal representation of the fingerprint for a subject public key. The directory contains the subject public key, signatures over the subject public key, as well as all sub-keys and their respective certificates attached to the subject. All these data are serialized and stored persistently as Base64-encoded files. The generated files are located in the application's private directory. This layer is also responsible for key verification. After the successful completion of the handshake protocol, the key exchanged in this protocol needs to be authenticated. As surveyed in our work [148], a plethora of secure device pairing schemes has been proposed to perform authentication procedures after key exchange. Our framework allows for easy extensibility by facilitating the new implementation, extension, or replacement of key authentication modules. Currently, we have implemented the following existing authentication mechanisms:

This layer is also responsible for the key verification, i. e., the authentication of the exchanged key.

- **Visual comparison:** The remote and the own fingerprint are color-coded and displayed to the users, as shown in Figure 5.4.
- **Scanning a QR code:** Both fingerprints are encoded in Base64 and encapsulated in a QR code. The user is required to scan the remote QR code. The scanning is performed using the ZXing (Zebra Crossing) project [150].

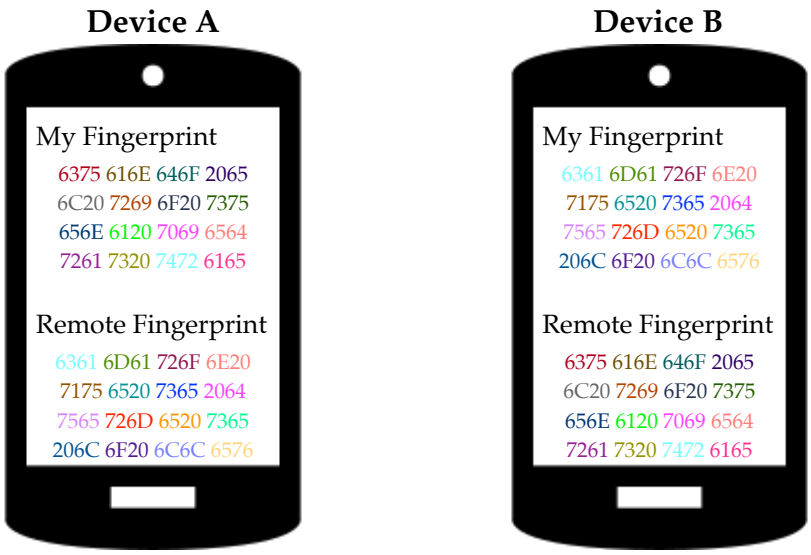


Figure 5.4: Example of the visual comparison method implemented in SoL.

- **Using NFC technology:** When the devices are in close proximity, they exchange the fingerprints automatically.

5.3.4.2 *Key Management Layer*

The main goal of this layer is the initialization of the private authentication key, and the support of additional operations where the initial authentication key is involved. It includes to sign keys, to issue certificates. Moreover, this layer controls whether a storage is unlocked before performing any cryptographic operation. Whenever the storage is locked, user interaction is needed for unlocking it, e. g., by introducing a password, lock pattern, or a PIN. This layer also offers an interface to the upper Trust Management Layer. This layer is split into the following sub-modules:

The main goal of this layer is the initialization of the private authentication key, and the support of additional operations where this key is involved.

- **SoftwareKeyManager:** This sub-module supplies a software-based Keystore solution developed for Android versions before 4.3. The Keystore bases on the Bouncy Castle library. The files generated in this module are protected using a user-provided PIN or pass-phrase.
- **AndroidKeyManager:** The AndroidKeyManager is the solution for Android versions from 4.3 on. This module utilizes the official Android API Keystore, which introduces an application private credential storage concept, but also (if available) enables additional security by offering support for hardware-based solutions.
- **HardwareKeyManager:** The HardwareKeyManager represents an additional abstraction layer for the key storage. It is the basis

module for all hardware-based solutions, as all these solutions employ a similar protocol based on specific Application Protocol Data Unit (APDU) commands to communicate with Java Card Applets. Our current implementation covers three hardware-based solutions, which include the key storage and also perform the required signature operations: *(i) SmartcardManager* handles the communication with NFC smart cards. *(ii) SeekManager* supports the connection to available readers, e. g., UICC. The Seek Manager manages the communication with the existing SEEK for Android framework [151]. *(iii) YubiKeyManager* permits communication with YubiKey NEO hardware tokens [152].

5.3.5 *Solution-dependent Settings*

Our implementation prioritizes the hardware-based key manager solutions. We also abstract the network layer tasks.

In our implementation, we abstract the network layer tasks, that is, neighbour discovery and data transmission. This abstraction allows replacing the ad hoc communication with another technology at any time. In our proof-of-concept, we used Wi-Fi Direct as the ad hoc communication technology. Moreover, we prioritize the selection of the key manager according to the solutions supported by the device.

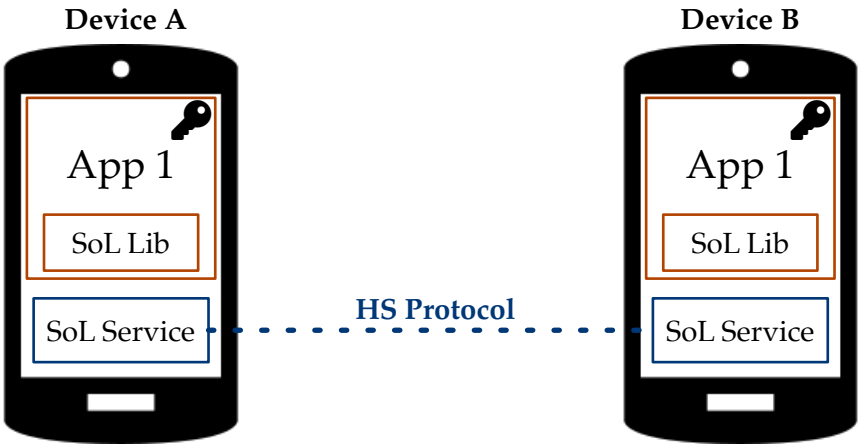
5.3.5.1 *Configurable Properties*

We define several properties as configurable:

- **maxdegree:** defines the maximum number of transitive relations that can still be considered valid.
- **numknown:** fixes the number of required known signatures to validate an unknown signature.
- **maxsubkeys:** determines the maximum number of sub-keys that an application can register.
- **signaturealgorithm:** represents the selected signature algorithm, e. g., Rivest-Shamir-Adleman (RSA) or Elliptic Curve Digital Signature Algorithm (ECDSA).

5.3.5.2 *Choosing the Most Suitable Key Manager*

Our selection prioritizes hardware-based solutions. During the initialization of the SoL service, it checks whether any reader is available. If it exists, the *SeekManager* is chosen. If it does not exist, we ask the user if she wants to utilize other supported hardware-based methods, e. g., *SmartcardKeyManager* or *YubiKeyManger*. Otherwise, we examine the running Android version and automatically select the suitable software-based module.



HS Protocol:
- Exchange of public keys and signature
- Verification:
  + Signatures
  + Fingerprints over secure channel
- Signing public key and exchange issued certificate

Figure 5.5: SoL Android service performing the handshake protocol.

5.3.6 *Integration into Other Applications*

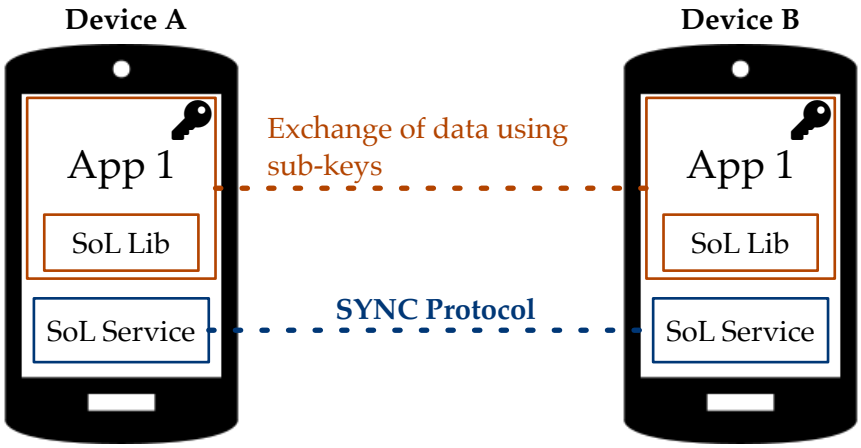
The proxy SoL library allows an app to communicate with the SoL service.

We provide a proxy library (=SoL *library*) that allows an app to communicate with the SoL service simply and directly. The main tasks of this proxy library include:

- Validate the installation, availability and successful initialization of the SoL service.
- Trigger the service to start the handshake protocol.
- Check existing trust relationships with a neighbour.
- Retrieve additional information about a neighbour.
- Request and register app specific sub-key certificates.
- Return the sub-keys associated to a specific fingerprint.

By using our framework, multiple apps running on a smartphone neither need to build nor to maintain their own trust repository.

To clarify the use of our SoL framework, we assume the following scenario. Let *App 1* be a chat app that wants to provide secure communication between devices in a decentralized manner. For doing so, it creates a sub-key using an asymmetric algorithm scheme. To benefit from our framework, *App 1* uses the SoL *library* to register the generated public key in our framework. Hence, the SoL service signs the key and issues a certificate. Finally, the certificate and the public key are stored in our local trust repository. Then, the SoL service takes care of the distribution and synchronization of the public key as well



SYNC Protocol:
- Synchronisation and update of the trust repository:
  + Fingerprints
  + Public keys (PK), PK signatures
  + Sub-keys (SK), SK signatures

Figure 5.6: SoL Android service performing the synchronization protocol.

as its certificate. It implies that multiple apps running on a smartphone neither need to build nor to maintain their trust repository. Figures 5.5 and 5.6 show the data flow between devices in the scenario mentioned above.

5.4 SIMULATION

We investigate the performance and scalability aspects of the trust management layer by means of simulation using the Opportunistic Network Simulator (ONE) [10].

5.4.1 *Simulation Setup*

We investigate the performance and scalability aspects of the trust management by means of simulation using the ONE.

Each node starts with a maximum of 3 sub-keys. Each experiment runs for 12 hours (720 minutes) and nodes exchange their data every 10 seconds, if in proximity. The maximum degree of transitive trust relations varies from [1,3]. The plots show averages over 6 different experiments: one per transitivity degree (degrees 1 to 3) using 2 possible signature algorithms (RSA or ECDSA). Each run is seeded with numbers from the interval [1,5], resulting in a total of 30 runs. We use BouncyCastle JCA for signing and key generation operations. Detailed simulation settings for the ONE are provided in Table 6.1.

Table 5.1: SoL simulation settings

Parameter	**Value(s)**
Dimensions *w x h*	3000 x 3000 [m]
Simulation duration	12 [h], i. e., 720 [min] or 43200[s]
Number of nodes	120
Experiment	6 (3 trust degree $\times$ 2 signature algorithms)
Runs	5 per experiment
Mobility Model	RWP
Speed	0.5, 1.5 [m/s]
Routing Algorithm	DirectContact
Buffer size	20 [MB]
Transmit speed	2 [Mbps]
Transmission range	10 [m]
Maximum trust degree	1 (direct) - 3
Number of Sub-keys	3
Size per Sub-key	4096 bit
Signature algorithm	RSA (2048 bit) , ECDSA (256 bit)

5.4.2 *Evaluation Metrics*

We analyze four evaluation metrics for this layer: the propagation of trust relations, memory consumption, bandwidth consumption and computational overhead. We show average values and omit the confidence intervals, which are sufficiently small and would hamper readability.

5.4.2.1 *Trust Relationships*

The propagation of trust includes direct and implicit relationships.

The propagation of trust includes direct and implicit relations, i. e., intermediaries relationships between two devices. An implicit relationship is set where a direct relationship can not be established. Generally, with each encounter, the number of implicit relationships increases faster than direct trust relationships. Therefore, to evaluate our trust management implementation, we measure the overall trust relationship between devices in a system using SoL.

5.4.2.2 *Memory and Bandwidth Consumption*

Memory and bandwidth consumption are also important metrics to evaluate our implementation. In our case, we compare the memory and bandwidth consumption of both signature algorithms RSA or ECDSA.

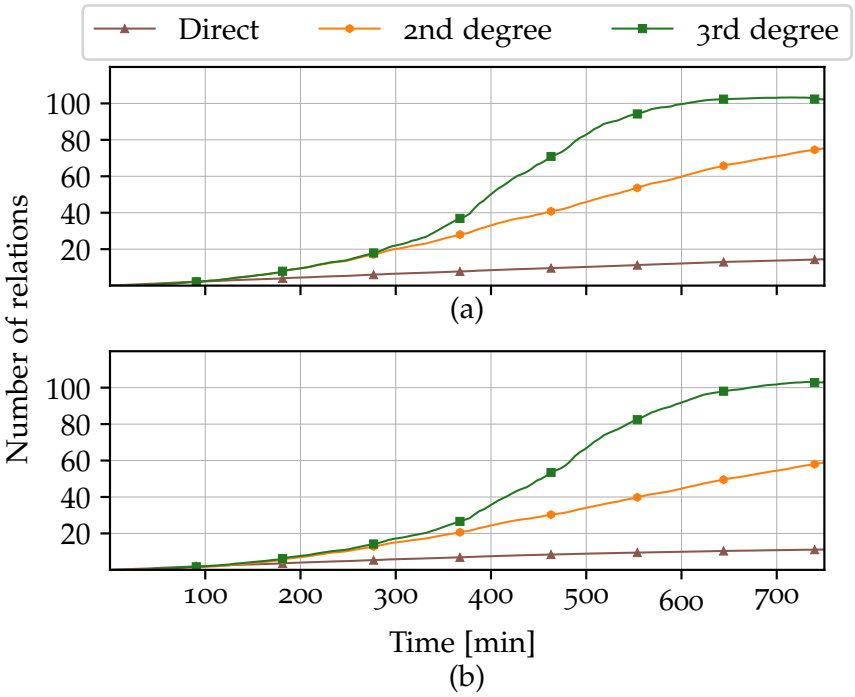


Figure 5.7: Propagation of trust in the network using: (a) RSA, (b) ECDSA.

For the memory consumption, we determine the file size required for public keys, sub-keys and signatures in the repository. In terms of bandwidth consumption, we compare the bandwidth overhead during the handshake and synchronization phase.

5.4.2.3 *Computational Overhead*

The computational overhead considers the number of operations realized during the simulation.

We analyze the computational overhead of our solution based on the number of operations realized during the simulation. Because the number of operations is the same for both signature algorithms, we do not separate the results into ECDSA and RSA.

5.4.3 *Results*

While implicit relationships increase exponentially, the direct trust indicates a linear property.

Figure 5.7 shows the number of direct trust relationships as well as implicit relationships. While implicit relationships increase exponentially, the direct trust indicates a linear property. The number of direct trust relationships remains almost the same and it does not depend on the maximum certification path. Instead, it varies according to the number of performed handshakes between devices.

As depicted in Figure 5.8, the memory consumption is directly influenced by the selected trust degree as well as the signature algorithm. First, our results confirm the existing findings regarding both algorithms: RSA exhibits higher memory usage than ECDSA for the

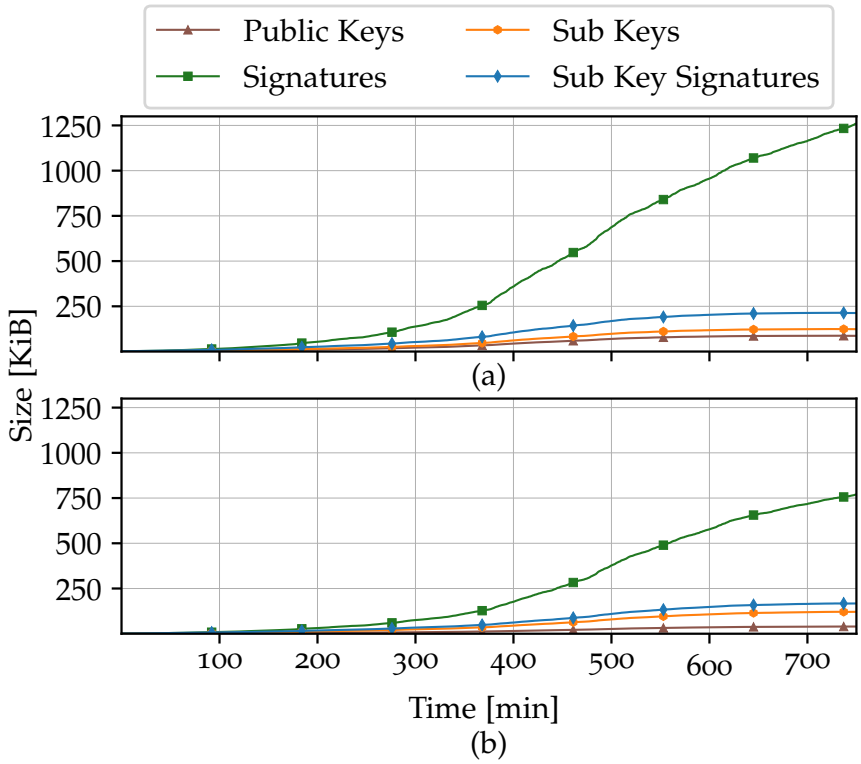


Figure 5.8: Memory consumption in a third degree network using: (a) RSA, (b) ECDSA.

generation of primitive public keys, sub-keys and the signatures. As the number of collected signatures of known devices increases with each neighbour encounter, the storage space in the repository is mainly occupied by signatures. This, in turn, implies a considerable memory overhead; thus each node collects and stores signatures according to the trust degree selected.

Figures 5.9 and 5.10 show the bandwidth overhead and usage required for the handshake and the synchronization phase. Although the bandwidth usage is constant during the handshake protocol, it increases rapidly in the synchronization phase, depending on the selected maximum degree of trust relations.

Query operations account for the overwhelming part of usage bandwidth, which further increases with increasing trust degree.

Furthermore, if we split the data transferred during the synchronization phase into *query* and *response* operations as illustrated in Figure 5.9, we notice that query operations account for the overwhelming part of usage bandwidth during the synchronization, which further increases with increasing trust degree. This is a significant result: on the one hand, a trust degree higher than one is essential to scale up the WoT faster. On the other hand, such a higher degree burdens the network and, thus, may impact the expansion of the WoT due to overload situations. In Chapter 8 we suggest possible optimization mechanisms to minimize this issue. As shown in Figures 5.11 and 5.12, verification

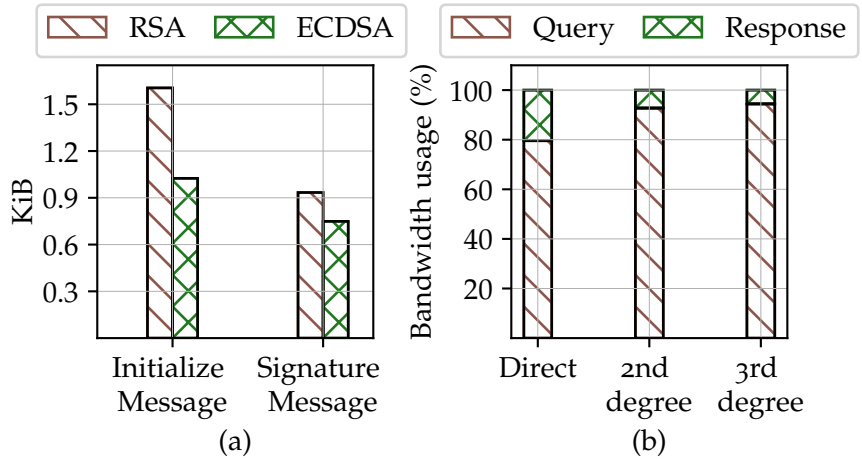


Figure 5.9: Bandwidth usage during: (a) handshake phase, (b) synchronization phase split into query and response operations.

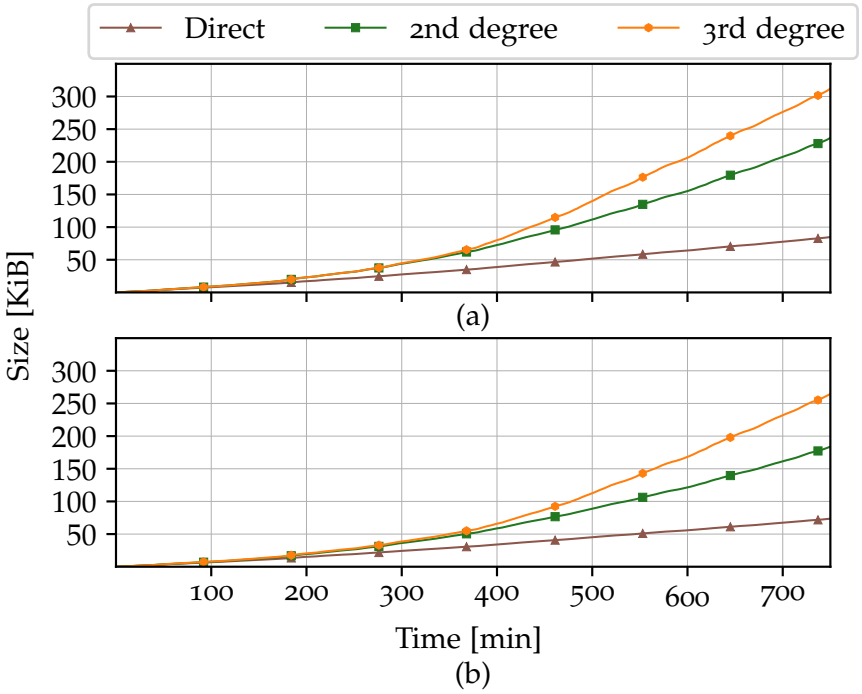


Figure 5.10: Bandwidth usage during synchronization phase in the network using: (a) RSA, (b) ECDSA.

represents the most significant operation performance-wise. Its growth is exponential and directly associated with the trust degree.

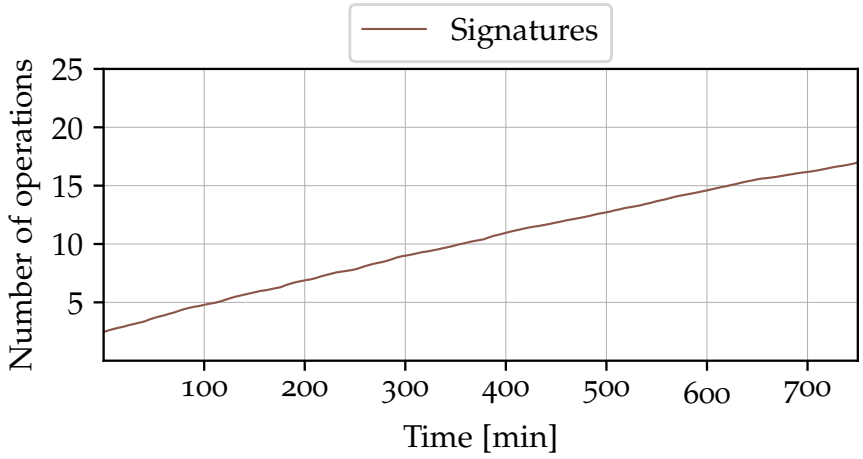


Figure 5.11: Computational overhead by considering the total numbers of signing operations in the network using RSA.

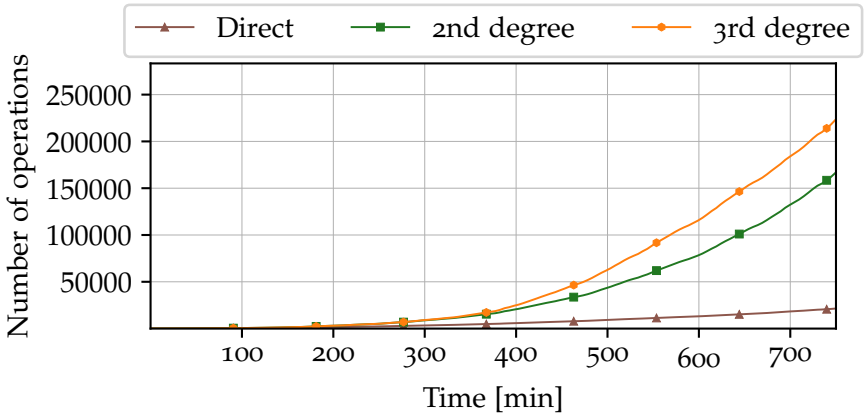


Figure 5.12: Computational overhead by considering the total numbers of verification operations in the network using RSA.

5.5 EXPERIMENTAL EVALUATION

We demonstrate and test our implementation on real devices to show its feasibility and test the computational performance of the key management part.

5.5.1 *Experimental Setup*

The hardware-based storage experiment is performed with a smartphone and an NFC token.

A proof-of-concept of SoL was implemented on Android-based smartphones to demonstrate the feasibility of our framework on real devices. The evaluation of this layer covers the two supported cryptographic algorithm and compares both in terms of efficiency and performance. Additionally, we compare hardware- and software-based key storage mechanisms. Detailed experiment settings are provided in Ta-

Table 5.2: SoL proof-of-concept settings.

Parameter	**Value(s)**
Signature algorithm	RSA (2048 bit)
	ECDSA (256 bit)
Devices	1 ThinkPad X220, 8GB RAM, Ubuntu 64 bit
	1 Google Nexus 5, Android version 6.0
	1 YubiKey NEO (NFC token)
Key Generation	2 key-pairs (*kp1*,*kp2*)
	1 invalid signature
Issue signatures	1000 by *kp1*
	200 by *kp2*
Verifications	1000 (valid)
	200 (invalid)

ble 5.2. The hardware-based storage experiment is performed with a smartphone and an NFC token. Additionally, we use a laptop for the software-based storage experiment. We repeat the experiment 15 times. Each iteration takes place as follows:

1. First, two key pairs are generated: *kp1* that is considered as valid, and *kp2*, which issues invalid signatures. It means a signature is valid only if *kp1* issued it.
2. After the key generation, *kp1* issues 1000 signatures, and *kp2* issues 200 signatures.
3. Finally, the issued signatures are verified using *kp1*.

5.5.2 *Evaluation Metrics*

We evaluate the performance of two signature algorithms by executing three cryptographic operations: generation, signing, and verification (see also [153] for existing performance studies of the employed algorithms).

5.5.3 *Results*

The performance of the NFC token is not measured for the verification of signatures, as only operations regarding the private key are carried out on it.

Figure 5.13 shows the performance of RSA and ECDSA executing cryptographic operations. ECDSA has better performance regarding the key generation and issuing signatures. RSA, however, is more efficient for verifying signatures. Note that the hardware-based approach offers a poor performance for signing operations since the processor embedded in the NFC token is relatively slow. Notwithstanding, this

result depends directly on the capabilities in terms of cryptographic operations supported by the token. For example, if a token has a dedicated cryptographic co-processor for such operations, it is faster compared with another one who performs cryptographic operations on the regular micro-processor.

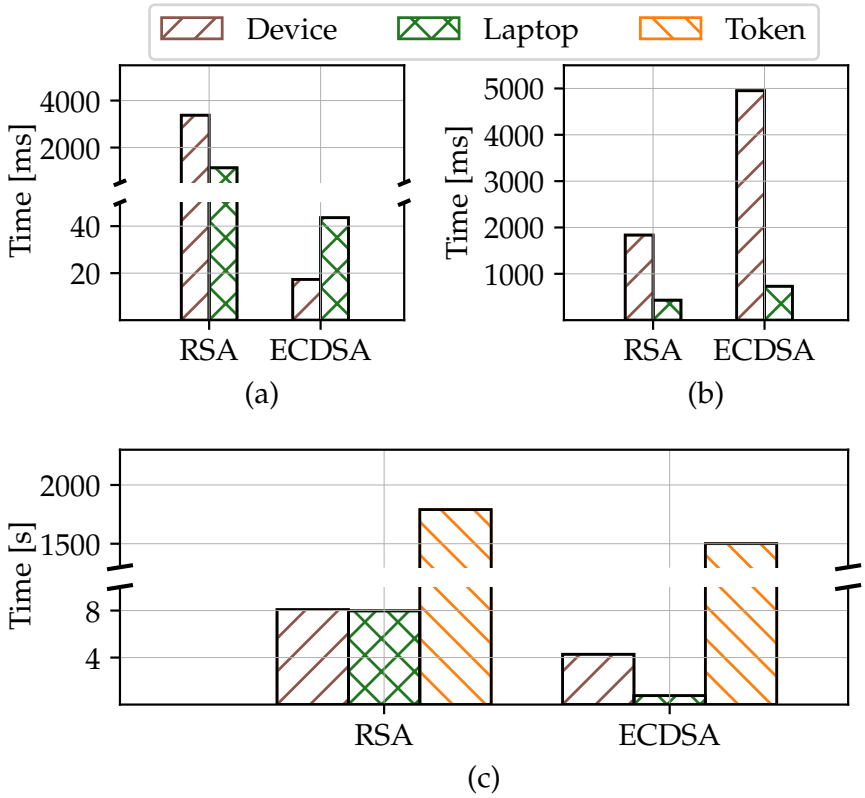


Figure 5.13: Comparison between RSA and ECDSA: (a) key generation, (b) key verification, (c) key signing.

5.6 RELATED WORK

Existing work in the field of security in decentralized networks focuses mainly on the communication, providing secure routing protocol solutions, improving the fairness of the users in the network.

Existing work in the field of security in decentralized networks focuses mainly on the communication, providing secure routing protocol solutions [36, 37], improving the fairness of the users in the network [154], increasing the robustness of such networks by detecting corrupt nodes [155, 156].

Our work aims at proposing a solution to bootstrap security services while integrating a scheme for authentication and key and trust management in a decentralized fashion. Several studies focusing on trust establishment [157] and key exchange using mobile devices have also been extensively analyzed [158, 159]. Furthermore, there are also some proposals using existing security hardware on smartphones [160] and how these can be exploited to create different security levels. However,

most of them either assume the existence of servers or lack an evaluation in both simulation and real devices. Our work differs from the solutions above in that we propose, inspired by the approaches based on WoT model [161, 162], a more bare-bones implementation of decentralized authentication to make it more practical. Yet, our scheme offers cross-application support and easy integration into existing apps. In our proposed scheme, each entity creates its public/private key and—after handshaking—issues certificates for its neighbours. In addition, we consider the use of secure elements to provide a secure mechanism of key management locally in the devices. Finally, we investigate performance by means of simulation, and we test our implementation on real devices.

5.7 SUMMARY

We propose a more bare-bones implementation of decentralized authentication. In addition, we consider the use of secure elements to provide a secure mechanism of key management locally in the devices.

This chapter presented SoL, a framework to bootstrap security for device-to-device settings. SoL is designed and implemented as an Android service. SoL uses asymmetric cryptographic algorithms: RSA and ECDSA. It also implements a simplified version of the WoT paradigm. It features a Trust Management Layer and a Key Management Layer. The former manages all operations and methods related to the trust relations: bootstrapping, maintaining and synchronization. It also deals with the OoB key verification. The latter performs all operations concerning the underlying keys: initialization, generation and management. It supports both software and hardware-based key storage solutions. Furthermore, third-party apps which utilize our library can benefit from our framework by offering an authenticated and secure communication. To this end, they can create and register the application-specific sub-keys in our service. Finally, the implementation of a proof-of-concept demonstrates the feasibility of our solution on real devices. Simulation results confirm the trade-off between trust transitivity and synchronization overhead: transitive trust facilitates a much faster coverage, while direct trust is conserving bandwidth, but limits trust coverage. We make our framework available as open source [53]. We foresee several performance improvements. Introducing the concept of a timeout interval together with a register to remember users and a timestamp of previous encounters can help in saving bandwidth. Then, a new synchronization with a specific user is only allowed after the timeout has expired. Furthermore, we can also employ bloom filters for checking already known or trusted users. Thus, it constrains the query part from the synchronization phase. Finally, even though our scheme builds on the direct physical interaction of users the trust level of transitive relations can be configured, i. e., there is a specific control on how far information generated by malicious devices will spread into the network.

6

ENERGY-EFFICIENT NEIGHBOUR DISCOVERY FOR EMERGENCY COMMUNICATION SYSTEMS

After having presented our solution for decentralized authentication, key management, and trust management in Chapter 5, in this chapter, we focus on the neighbour discovery process for emergency communication systems. In this chapter, we further refer to Neighbour Discovery (ND) based on the definition proposed by authors in [163] as follows:

Definition 6. *Neighbour discovery:"... is the bootstrapping primitive that discovers all the neighbors of a mobile device. An efficient neighbor discovery should enable a node to discover its neighbors within a short delay for other functionalities to launch as quickly as possible. [...] only after an initial discovery can a node set up communications with others."*

In other words, it enables a device mainly to find if other devices are in range. Thus most opportunistic mobile phone applications build on ND. During a discovery process, a device can take one of the three possible modes: *listening*, *active probing*, and *sleeping*.

During a discovery process, a device can take one of the three possible modes: listening, active probing and sleeping.

Figure 6.1 clarifies these modes: a device in *active probing* broadcasts small packets (called hello messages) periodically, and starts listening to the channel for possible responses. Devices in *listening mode* scan the communication channel periodically for advertisements and reply to the sender of a hello message. This chapter based on our work *[5]*, which proposes an adaptive ND scheme considering device speed and user preferences to calculate an optimal probing interval. Hence, it reduces power consumption during static situations. Besides, we present an opportunistic networking framework for mobile devices based on SavIng Energy in STAtic Phases (SIESTA).

We propose an adaptive neighbour discovery scheme that reduces power consumption during static situations.

This chapter is organized as follows. In Section 6.1 we briefly introduce our motivating scenario. Section 6.2 provides an overview of our system model and our adaptive ND scheme. in Section 6.3 we explain the design and introduce the architectural concepts of the SIESTA framework and implementation details. The results of the evaluation of SIESTA are presented in Section 6.4 and Section 6.5. In Section 6.6 we summarize related work. Finally, Section 6.7 concludes this chapter.

6.1 MOTIVATION AND CONTRIBUTION

In recent years, mobile devices have contributed to the rapid growth of opportunistic networking frameworks and applications [164, 165]. Opportunistic Networks (OPPNET) allow users to communicate in a D2D

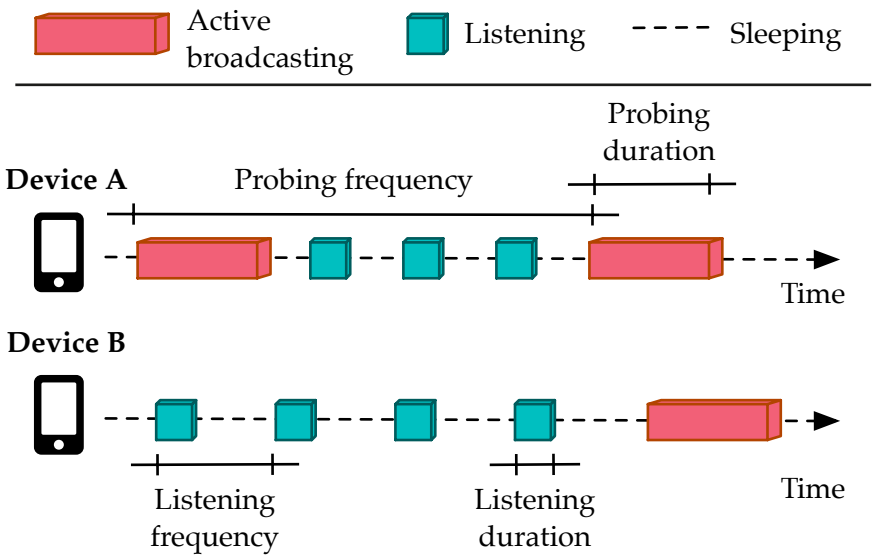


Figure 6.1: Neighbour discovery concept.

manner, without the need for an infrastructure-based network [166]. By taking advantage of the nodes' mobility, devices exchange data opportunistically only when nodes are within the transmission range. These networks play an essential role in providing communication in challenging conditions such as natural or human-made disasters [14], in rural areas [167], large scale blackouts [15]., where infrastructure-based networks are overloaded or not available. However, the energy consumption of existing opportunistic networking solutions is one main limiting factor hindering deployments [38]. In this context, ND represents one of the main energy consumers. Practical solutions to reducing energy consumption during this process already exist [40, 41, 168]. However, existing approaches are still complex, and there is a lack of implementations for real devices [40, 41, 169].

Neighbour discovery represents one of the main energy consumers in opportunistic networking frameworks and applications.

We propose, inspired by [41], an energy-efficient ND process called SIESTA, which adapts the probing interval depending on device mobility. Yet, in our scheme, the devices stay in listening mode when they do not move. We also include user preferences and battery level to calculate the probing interval. Furthermore, we compare SIESTA against two other neighbour discovery schemes: *(i)* without any mobility awareness, i. e., such a scheme uses a constant probing frequency, and *(ii)* the scheme proposed by [41]. Finally, we evaluate the performance using simulations, and through a prototype implementation on real devices.

6.2 SYSTEM MODEL

In this section, we provide an overview of our system model. We also present our ND scheme SIESTA. It is an adaptive neighbour discov-

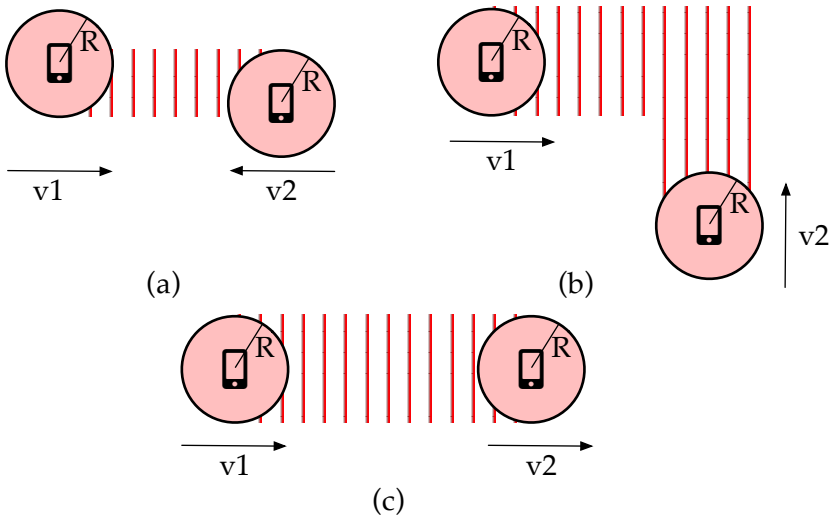


Figure 6.2: The SIESTA-ND basic encounters: (a) moving towards each other, (b) crossing, and (c) overtaking another device.

ery scheme for saving energy during D2D communications in self-organizing networks. SIESTA allows reducing energy consumption, if node churn is low while offering fast response times for dynamic settings.

6.2.1 *System Model*

Our solution adapts the probing and listening properties to optimize energy consumption.

Our proposed system adapts the probing and listening properties to optimize energy consumption. Regarding the device context information, we utilize the speed as well as user preferences to adapt the discovery process. We consider users owning mobile devices capable of direct D2D communication. The communication technology needs to support three modes: active probing, listening, and sleeping. As shown in Figure 6.2, we assume three basic encounter situations between devices: *(i)* going towards each other, *(ii)* crossing, or *(iii)* overtaking another device. That is, we consider the most common possible encounters of mobile devices, i. e., when a device is within the communication range of other devices.

6.2.2 *SIESTA Neighbour Discovery Scheme*

SIESTA adapts the discovery parameters only if a device is moving. In contrast, static devices stay in listening mode.

SIESTA-ND is an adaptive scheme focusing on reducing energy consumption. It adapts the discovery parameters only if a device is moving. Devices broadcast actively to indicate their presence in the neighborhood. They adapt their probing interval based on their context: because the environment changes faster and other devices are in their communication range for a shorter time, devices scan more often when moving faster. In contrast, static devices stay in listening mode to de-

tect other devices in the communication range. We use the equation introduced by Troel [170] as a baseline to deduce the probing interval $T_{probing}$:

$$T_{probing} = \frac{a \times R}{2 \times v} \tag{6.1}$$

Where:

- v: is the speed of a device.
- a: is a constant to determine the minimum distance required between two devices to detect each other when moving in communication range.
- R: represents the communication range of a device.

The discovery process should finish whilst one device is within the communication range of another device.

To successfully detect a neighbour, the discovery process should finish while one device is within the communication range of another device. For all three encounter alternatives considered in SIESTA-ND, this implies that the discovery process must take place within a maximum distance of two times the communication range. For simplicity, we assume the same speed for both devices. In addition, we can optimize (6.1) by increasing $T_{probing}$. This consideration focuses on saving energy, but it influences the number of discoveries directly. Even so, it still allows a successful discovery, mainly in a scenario where one device is static. Replacing these assumptions in (6.1), we get the following equation:

$$T_{probing} = 2 \times (\frac{2 \times R}{2 \times v_{own}}) = \frac{2 \times R}{v_{own}} \tag{6.2}$$

Our scheme introduces an energy-saving variable E, a high value of E means a low energy consumption.

Now, taking (6.2) as a basis, we can switch to a more realistic scenario. First, the discovery process is not discrete, which means it needs some time $T_{avg\_discovery}$. In addition, the time required for establishing a connection, and transmitting data ($T_{transmit}$) should be considered. Both $T_{avg\_discovery}$ and $T_{transmit}$ reduce the available probing interval to ensure a successful discovery. Additionally, our proposed discovery method introduces an energy-saving variable E. This variable takes values from the range $0 < E < 1$, where a high value means a low energy consumption. E allows adapting the probing interval flexibly. For example, E can be adapted according to the current battery level of a device, or some user preferences can also influence this value. Finally, we can adjust (6.2), resulting in:

$$T_{probing} = E \times (\frac{2 \times R}{v_{own}} - T_{avg\_discovery} - T_{transmit}) \tag{6.3}$$

6.3 ENERGY-EFFICIENT NEIGHBOUR DISCOVERY CONCEPT

Smartphone-based communication networks are fundamental for providing services in post-disaster scenarios. However, these networks also involve new challenging scenarios: high power consumption for the devices involved in the communication, short connectivity opportunities to exchange data, lack of knowledge about opportunistic routing paths, security. In this section, we highlight the design concept and implementation of our SIESTA-ND framework for opportunistic networks.

6.3.1 *Architecture*

Our architecture comprises three components: context, strategy, and communication.

SIESTA-ND provides cross-application services for OPPNET. Our architecture comprises three components: context, strategy, and communication. Note that these components support and combine several methods, e. g., battery level, device speed or static strategy, to provide a modular solution. We developed the SIESTA framework for the Android platform and implemented it as a bound service residing on the application layer. Figure 6.3 visualizes the components of the SIESTA framework.

6.3.1.1 ***Context***

The context is responsible for collecting and processing the context information.

The context component is responsible for collecting and processing the context information. Currently, our solution supports the following context information: user preferences, device speed, and battery level. The user preference allows a trade-off between saving power consumption and performance. We use activity recognition data and the battery level to get the current context data of a device. The Google Play Services Activity Recognition API[1] provides a confidence value about the most probable activity of a user, e. g., walking, running, biking or remaining still. We use this confidence value and multiply it with a speed value. We define the following speed values depending on the user activity: $1.5\frac{\mathrm{m}}{\mathrm{s}}$ for walking, $3\frac{\mathrm{m}}{\mathrm{s}}$ for running, and $6\frac{\mathrm{m}}{\mathrm{s}}$ for biking. We also consider static activities when a user is in a vehicle or a train, i. e., its speed is higher than biking activities. Furthermore, each application defines how often to get notification about the current activity (=*update interval*). The update interval impacts energy consumption directly: shorter intervals consume more energy than long intervals. To set a suitable interval, we test the activity recognition using different intervals: $100\mathrm{ms}, 500\mathrm{ms}, 1000\mathrm{ms}, 3000\mathrm{ms}$, and $5000\mathrm{ms}$. As a result, we determine that $5000\mathrm{ms}$ is enough to identify activity changes. In addition to the activity recognition, we request updates on the current

We use the Google Play Services Activity Recognition API to determine the activity of a user.

1 https://developers.google.com/location-context/activity-recognition/

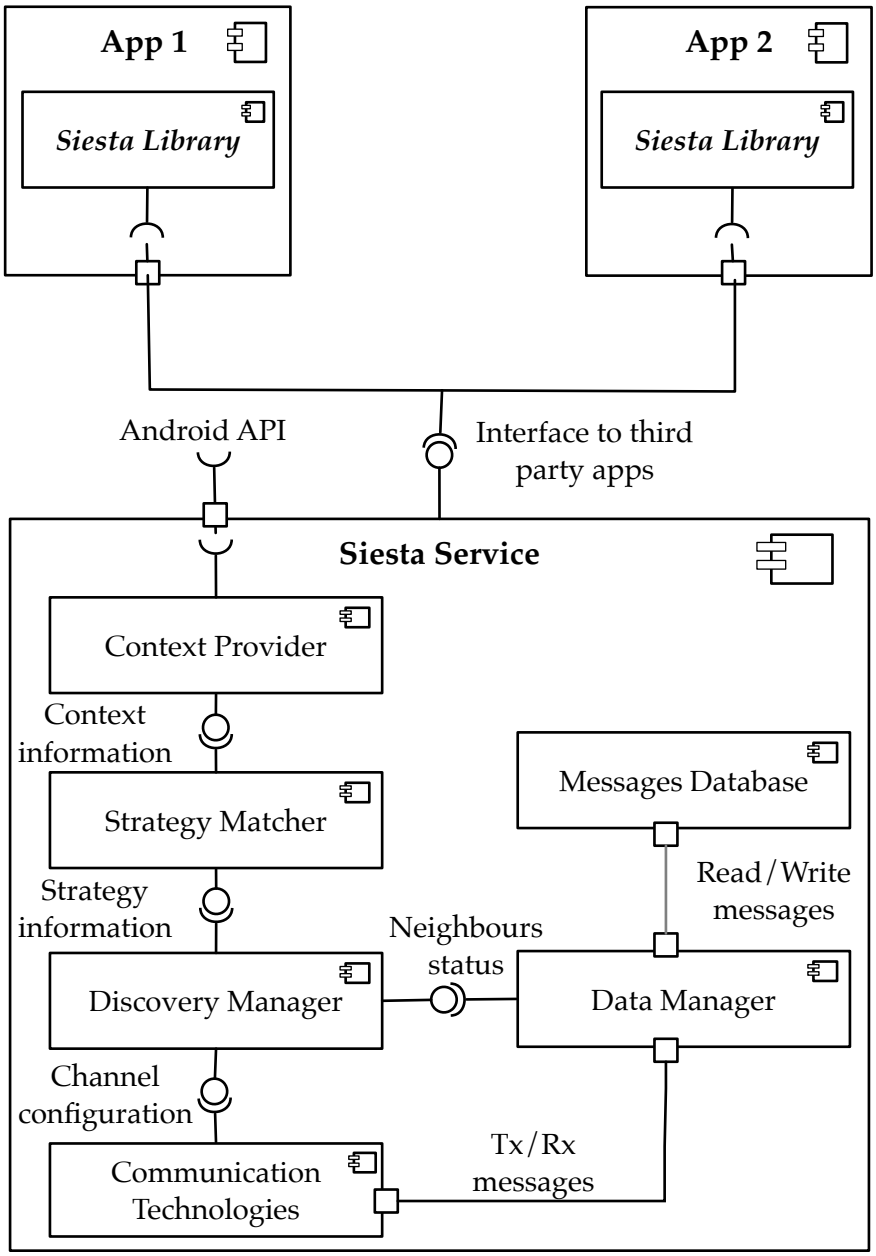


Figure 6.3: The SIESTA framework is designed as an Android service.

battery level each hour. As highlighted in the Android documentation, a continuous update also implies high energy consumption.

6.3.1.2 *Strategy*

The Strategy defines the discovery parameters for a neighbour discovery scheme.

This component defines the discovery parameters for an ND scheme, e. g., discovery interval or discovery mode. It implements different ND methods. As input, it requires the probing interval, discovery mode, and the energy-saving value. Our current implementation covers three algorithms:

- **Constant**: It uses a fixed probing interval and stays in active probing mode.
- **Hess** et al. [41]: Devices enter in the listening mode when moving with a velocity above a certain threshold. When devices are static or moving with low velocity (below a defined threshold), they change to the active probing mode. The probing interval is configurable.
- **SIESTA**: Per default, a device starts in the active probing mode. It changes to the listening mode when a device stays static for a long time (*threshold*); the default value of this *threshold* is two minutes. The final probing interval is calculated in the communication component, depending on the communication range, discovery duration, and transmission speed.

6.3.1.3 *Communication*

This component matches the strategy, its requirements and parameters with the supported communication technologies.

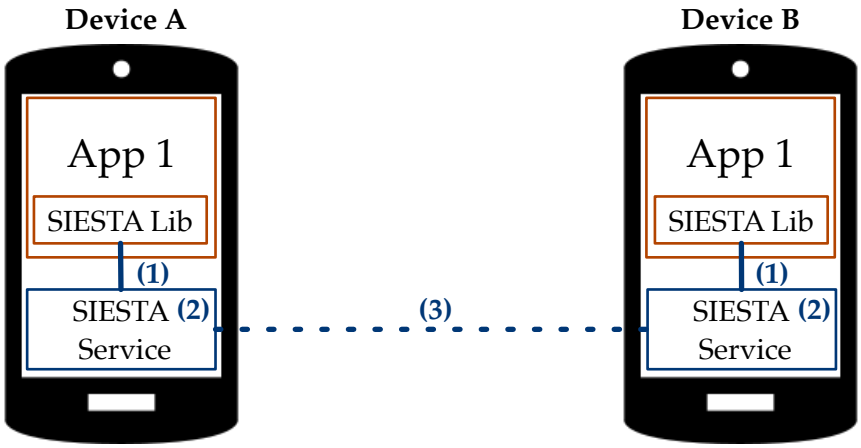
This component matches the strategy, its requirements, and parameters with the supported communication technologies. Currently, our framework supports two communication technologies: Bluetooth and Wi-Fi Direct.

- **Bluetooth:** Our implementation bases on the Briar project [171]. The connections are established using Bluetooth insecure channels. Devices attempt to communicate through our framework use the Bluetooth device name to discover other participants.
- **Wi-Fi Direct:** Even though this technology does not fulfil all requirements, we can adapt it for use in our framework. For that, we define a low-power and a high-power mode. Devices in the low-power mode utilize a constant probing duration and frequency. Otherwise, they stay in active broadcast mode. In our scenario, we choose five seconds as probing duration and velocity of $6\frac{\mathrm{m}}{\mathrm{s}}$ as the threshold to change between low-power and high-power mode.

To select a suitable communication technology, it is necessary to check if the available technology fulfils the requirements of the selected strategy. When for a specific technology, the time required to discover, connect, and transmit is higher than the available time of a device within range of a neighbour, it is set to sleep mode.

6.3.2 *Solution-dependent Settings*

Our proof-of-concept provides a basic implementation of a message application to exchange data in an opportunistic manner using our framework.



(1):
- Register to the framework.
- Send and request messages to/from the framework.

(2):
- Monitor, collect and analyze context data.
- Update the strategy and start the discovery process.

(3):
- Establish connection and data exchange.

Figure 6.4: Integration of SIESTA by third-party apps.

6.3.2.1 *Configurable Properties*

We define the following properties as configurable:

- **Technology:** determines the communication channel to be used, e. g., only Bluetooth, only Wi-Fi Direct or both.
- **Scheme:** represents the selected ND scheme that is required for the discovery process.
- **User preference:** fixes the limit of the variable E to define the trade-off between power consumption and discovery performance (only for the SIESTA ND scheme).

6.3.2.2 *Integration Into Other Applications*

The SIESTA service is encapsulated inside a dedicated proxy library.

The SIESTA *service* is implemented as a standalone Android application running in its process and encapsulated inside a dedicated proxy library (=SIESTA *library*). This encapsulation allows third-party applications to communicate with our service simply and directly. Figure 6.4 shows the data flow between two devices using our framework.

6.4 SIMULATION

We investigate the performance and energy consumption of the proposed ND scheme by means of simulation using the ONE [10].

6.4.1 *Simulation Setup*

We investigate the performance and energy consumption of SIESTA-ND by means of simulation using the ONE.

Detailed simulation settings for the ONE are provided in Table 6.1. The experiment runs for 24 hours, and nodes exchange their data every 30 seconds, if in proximity. The plots show the experiment results with seven different strategies: Constant, Hess, and SIESTA with five different values of E [1.0, 0.75, 0.5, 0.25, 0.10]. In addition, for each strategy, we use three different mobility models: Random Waypoint Mobility model (*RWP*), the map-based RWP model (*Map*), and finally, we use the real-world traces from a large-scale field test (*smarter*)[2] and included it in the ONE. Each run is seeded with numbers from the interval [1,20], resulting in a total of 420 runs. We analyze the energy consumption and the performance of the ND schemes using different mobility models.

Table 6.1: SIESTA simulation settings

Parameter	**Value(s)**
Dimensions *w x h*	8500 x 7500 [m]
Simulation duration	24 [h]
Number of nodes	300
Mobility Model	*RWP, Map, smarter*
Speed	0.5, 1.5 [m/s]
Experiments	21 (7 strategies $\times$ 3 mobility models)
Runs	20 per experiment
Message size	100 KB
Message TTL	360 min
Message interval	25 -35 sec
Routing Algorithm	Epidemic
Buffer size	100 [MB]
Transmit speed	2 [Mbps]
Transmission range	44 [m]

Table 6.2: Average power consumption on Nexus 5 smartphones

Source	Mode	Power consumption in [mW]
Bluetooth	On	3.53
	Listening	3.53
	Discovery	116.73
Wi-Fi	On	43.04
	Discovery	316.81
Activity recognition	each 5 seconds	21.78

6.4.2 *Evaluation Metrics*

We analyze the power consumption and the performance of our implementation.

We analyze the power consumption and the performance of our implementation by considering the following metrics: the number of beacons sent per hour, the effective energy consumption, the neighbour discovery rate, and the message delivery rate. With the exception of the message delivery rate plot, all other plots show the median values and omit the confidence intervals, which are small and would hamper readability.

6.4.2.1 *Power Consumption*

We measure the power consumption based on two aspects: *(i)* the number of beacons sent per hour and *(ii)* the effective energy consumption.

- **Number of beacons sent per hour:** This metric indicates the total number of beacons that were actively sent per hour. A high number of beacons sent per hour implies that the device stayed in the probing mode for a long time.
- **Effective energy consumption:** We measure the power consumption of single actions related to the ND process in a mobile device (see Table 6.2). We connect a Nexus 5 to the Monsoon Power Monitor[3] and perform different activities on the device for one minute. During the measurements, the display is on, and the unused communication technologies are off. We only present a relative energy consumption during the ND process. To calculate the overall power consumption, it is necessary to include the power consumption for transferring data packets.

2 https://smarter-projekt.de/demonstrator/
3 https://www.msoon.com/LabEquipment/PowerMonitor/

6.4.2.2 *Performance*

We choose the neighbour discovery rate and the message delivery rate as the performance metrics.

- **Neighbour discovery rate:** This metric represents the percentage of discovered neighbour devices during the simulation. It is compared against a truth data, i. e., when the device is permanently in the scan mode.
- **Message delivery rate:** The message or packet delivery rate defines the percentage of messages delivered successfully from all sent messages.

6.4.3 *Results*

The main goal of the simulation was to measure the energy consumption of different ND schemes as well as to analyze their performance. Therefore, we compare these schemes using different mobility models.

6.4.3.1 *Power Consumption*

Although devices in the probing mode can find more neighbours, they also require more energy. That means, *(i)* a high number of beacons sent per hour indicates a high energy consumption. Moreover, *(ii)* we calculate the energy consumption of the system with Equation 6.4.

$$E = E_{discovery} + E_{listening} + E_{actrec} \tag{6.4}$$

Where:

- $E_{discovery} = t_{discovery} * P_{discovery}$
- $E_{listening} = t_{listening} * P_{listening}$
- $E_{actrec} = t_{actrec} * P_{actrec}$

The last part of the equation is zero for discovery schemes without activity recognition. Figure 6.5 visualizes the energy consumption per node in joules (J).

As shown in Figure 6.6, SIESTA-ND sends a minimal number of beacons per hour in comparison with the other two schemes. Without any mobility awareness, devices send a high number of beacons (*Constant* scheme). Even though the *Hess* scheme adapts the interval of sending beacons according to speed, it is slightly better. *Hess* can be more efficient in static scenarios. However, OPPNET needs a high node mobility to exchange data opportunistically with other devices.

SIESTA-ND sends a minimal number of beacons per hour in comparison with the other two schemes.

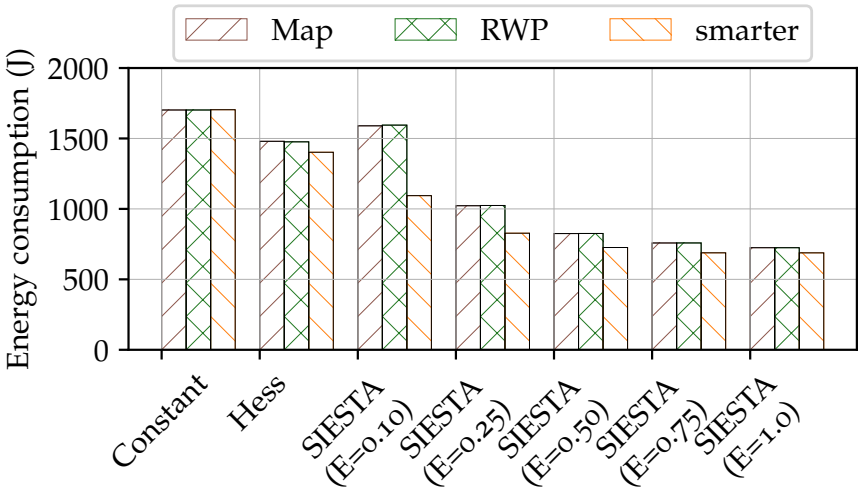


Figure 6.5: Energy consumption per node.

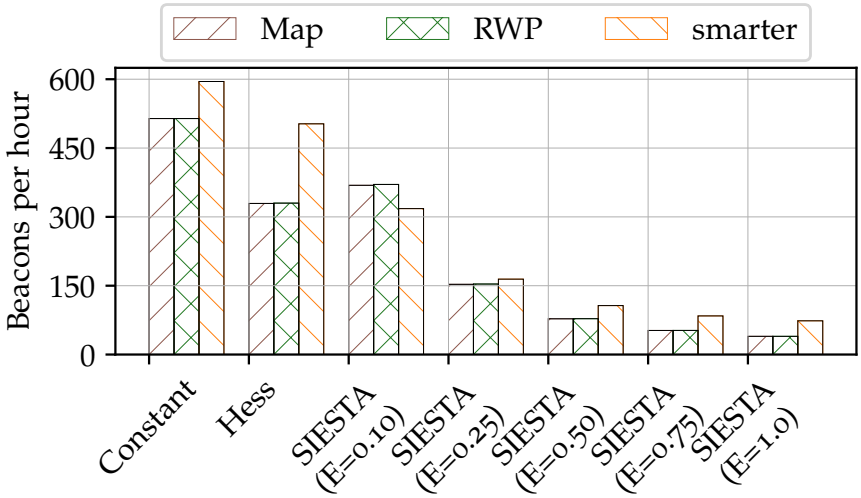


Figure 6.6: Number of beacons sent per hour.

6.4.3.2 *Performance*

The performance of SIESTA decreases for a high value of E. *However, it still allows discovery success comparable with the other two schemes.*

We evaluate the performance of our scheme using the neighbour discovery rate and the message delivery rate. Figure 6.7 visualizes the number of detected neighbours against the ground truth data, i. e., by continuous discovery. Figure 6.8 shows the message delivery rate for each ND scheme with three different mobility models.

The performance of SIESTA decreases for a high value of E. However, it still allows discovery success comparable with the other two schemes.

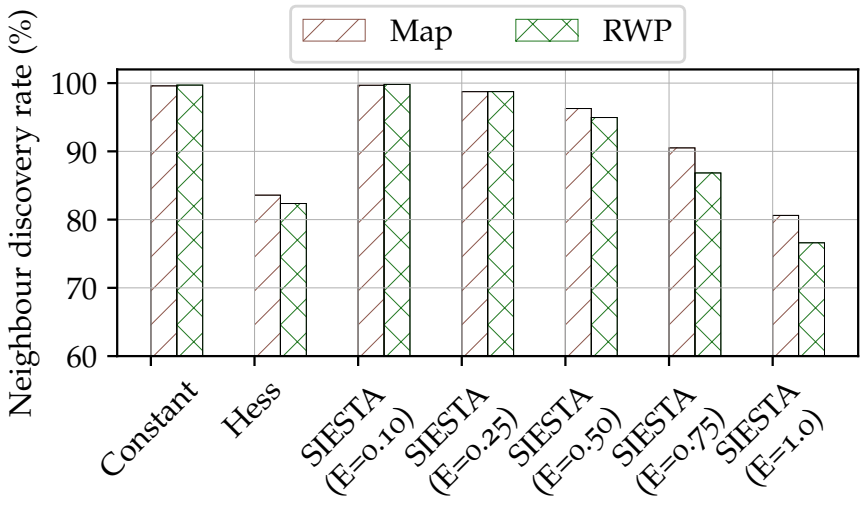


Figure 6.7: Number of detected neighbours.

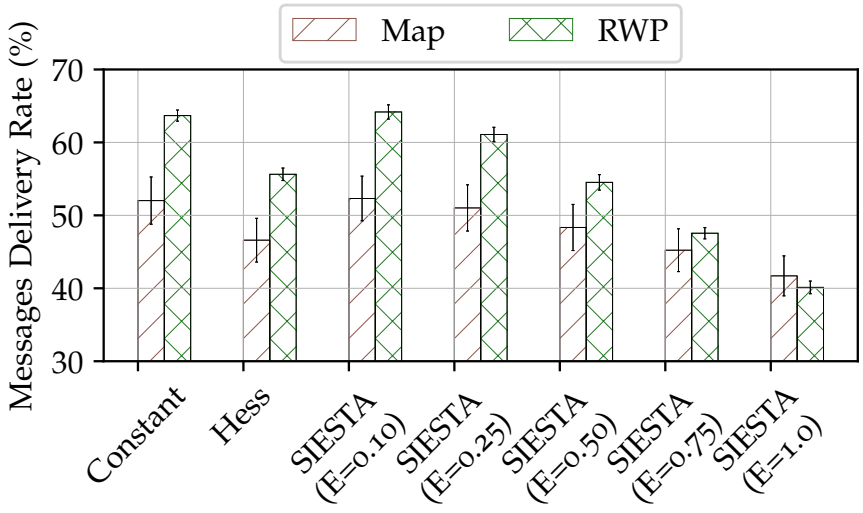


Figure 6.8: Delivery rate for all ND schemes with different mobility models.

6.5 EXPERIMENTAL EVALUATION

A mobile application was developed as proof-of-concept for Android-based smartphones.

A proof-of-concept for SIESTA was implemented on Android-based smartphones to demonstrate the feasibility of our framework on real devices.

6.5.1 *Experimental Setup*

Our proof-of-concept provides a basic implementation of a messaging application to exchange data in an opportunistic manner using our framework. Moreover, it enables additional utility functions, which allow logging information about established connections and number

Table 6.3: SIESTA proof-of-concept settings

Metric	Constant	Hess	SIESTA25	SIESTA50
Number of beacons sent	42	34	38	22
Neighbour discovery (%)	75	75	75	75
Avg. connection time (s)	69.52	68.51	55.42	60.13

Our scenario implies one stationary device A and a second device B carried by a participant.

of discoveries. Our scenario implies one stationary device A and a second device B carried by a participant. The initial distance between device A and B is 100 m. Device A moves in the direction of device B and stops after 200 m. After a short waiting period, device A turns around and returns to his initial position. We repeat this experiment four times. We use Bluetooth as the communication technology. In this experiment, we count the discoveries performed per device A, i. e., the number of beacons sent. We also check if on each round device A discovers device B.

6.5.2 *Results*

The number of beacons sent is comparable to the results of our simulation.

Table 6.3 summarizes our real-world experiment results. All schemes have the same neighbour discovery rate; thus they successfully discovered the other devices three of the four times. The number of beacons sent is comparable to the results of our simulation. However, as the walking speed and duration time of each experiment differs slightly on each run, we can not use these values to determine any performance difference between the schemes.

6.6 RELATED WORK

Existing energy-efficient neighbour discovery mainly use two forms of adaption: (i) optimizing the probing and listening properties or, (ii) performing changes in the discovery process.

The field of energy-efficient ND in opportunistic networking has been intensively studied using analytic as well as experimental methods. Existing ND researches [39–42] focus on saving energy for D2D using smartphones. Most of them mainly use two forms of adaption: *(i)* optimizing the probing and listening properties or, *(ii)* performing changes in the discovery process. On the one hand, by adjusting the scan and listen intervals, a discovery process can reduce energy consumption significantly. For example, the *probing frequency*, which indicates how often a device broadcasts a hello message per hour, can be adapted to save energy. However, any change on this property impacts the performance of the discovery process directly as well by decreasing the number of discovered devices. On the other hand, instead of broadcasting continuously, a device can deactivate the broadcasting mode completely and listen to the channel for signals

from other devices. Bluetooth Low Energy (BLE), for example, uses only three advertisement channels to scan for other BLE devices.

Furthermore, most of these approaches use the device context information to identify which properties can be adapted for improving the discovery process. For instance, several approaches utilize a certain threshold of speed for adapting the neighbour discovery while devices are moving, e. g., by deactivating the active probing, [41], by adapting the Wi-Fi activation [172]. Other approaches use real-world observations [173], e. g., based on the assumption that it is likely to find more devices in the vicinity of an already found device or maintain a database of past encounters. Using this information, it is possible to predict future devices encounters [174]. By defining a battery threshold value, a device can switch between different routing mechanisms to extend the lifetime of a device [175]. The communication technology used is also an option for choosing the adaptation of the discovery process. That means a device can switch between available technologies to connect to other devices, and also to save energy during communication [176].

6.7 SUMMARY

In this chapter, we presented SIESTA, an adaptive neighbour discovery scheme for saving energy during D2D communications in self-organizing networks. We also introduce a cross-application neighbour framework for opportunistic networks. Our approach is mainly energy efficient in scenarios with a high number of static phases, where devices stay in listening mode. In turn, devices constantly moving with only short stationary phases imply continuous activity recognition, i. e., a high energy consumption. We evaluated SIESTA by means of a real-world proof-of-concept implementation and simulation. Our results indicate the trade-offs between energy-efficiency and performance for D2D neighbour discovery: we deliver 40% energy savings in return for only a 3% reduction in neighbour discovery efficiency.

We proposed an energy efficient ND process which adapts the probing interval depending on device mobility. We also include user preferences and battery level to calculate the probing interval.

7

USING BLUETOOTH MESH SOLUTIONS FOR MEDIATING EMERGENCY COMMUNICATION SYSTEMS

Previous chapters have presented solutions to improve the resilience of post-disaster systems by providing mechanisms to deal with: *(i)* basic security services such as authentication or key management, and *(ii)* saving energy consumption during the neighbour discovery phase. Building post-disaster networks based purely on smartphones, however, remains a challenging task, and, as of today, no practical solutions exist. This chapter proposes the Bluetooth Mesh emErgency (BlueMergency), a solution to mediate D2D communication in post-disaster scenarios by harnessing the Internet of Things (IoT) devices that remain operational following disaster. This chapter is based on our work previously published in [6].

The remainder of this chapter is organized as follows. We first introduce our motivating scenario in Section 7.1. Then, we briefly provide an overview of the new Bluetooth standard and its terminology in Section 7.2. In Section 7.3 we detail our BlueMergency concept. Our proof-of-concept implementation is described in Section 7.4 and the results of the experimental evaluation are presented in Section 7.5. We summarize related work in Section 7.6. Finally, Section 7.7 concludes this chapter, discussing several points for future work.

7.1 MOTIVATION AND CONTRIBUTION

Building post-disaster networks based purely on smartphones remains a challenging task, and, as of today, no practical solutions exist.

The usage of the IoT has proliferated in recent years [177, 178]. It is estimated that by 2025, the installed bases of IoT connected devices grow to almost 75 billion sensing devices. The IoT concept covers a wide range of solutions [20]. Smart offices [179] and smart homes [180] represent a prominent IoT use case. Smart office solutions aim to provide a more comfortable and energy-efficient workspace, where sensors adjust the light or heat according to the current measurement of an office [181, 182]. Smart home systems integrate and connect conventional home devices such as lighting, heating, a refrigerator, to offer an automated environment in which many house features can be controlled and monitored locally as well as remotely [180]. However, these smart environments mainly require the Internet to enable communication and interaction between smart objects.

On July 19, 2017, the Bluetooth Special Interest Group (SIG) presented Bluetooth Mesh (BT Mesh) [55, 56]: a protocol that allows devices to communicate in a mesh-based network topology. By en-

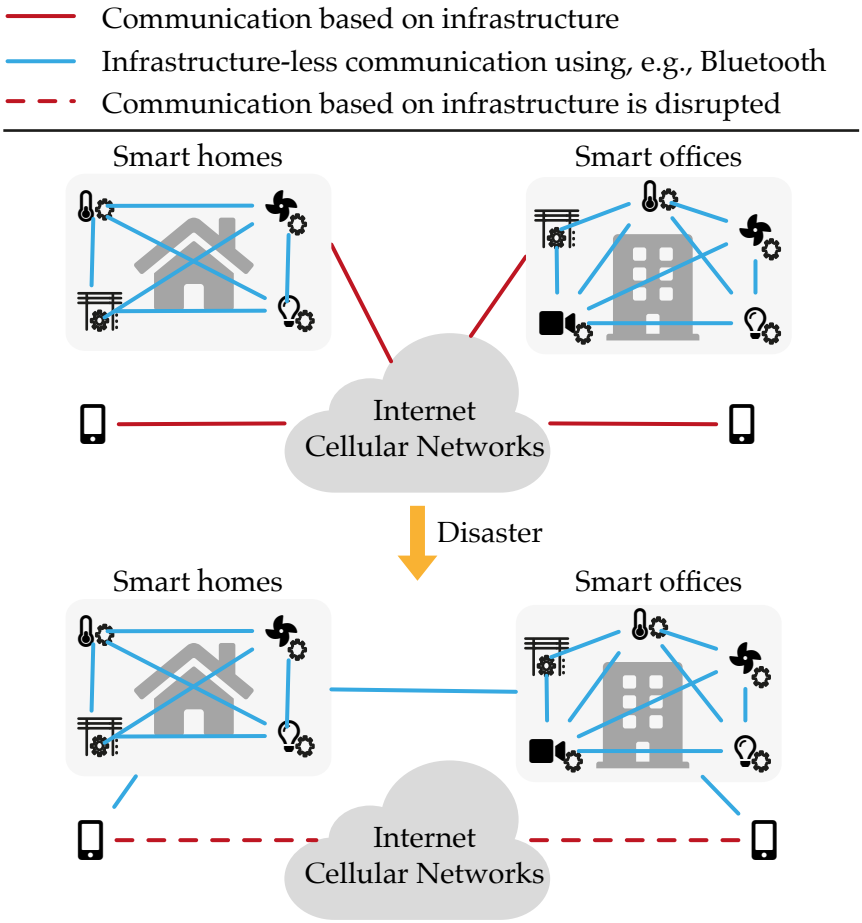


Figure 7.1: Integration of IoT solutions into post-disaster emergency communication systems.

abling hundreds of devices to communicate with each other, BT MESH becomes a technical solution for enabling communication post-disaster. The integration of mobile devices into these mesh networks opens up new possibilities for building post-disaster Emergency Communication Systems (ECSs) as depicted in Figure 7.1.

By including mobile devices into BT MESH networks it is possible to build self-organizing distributed wireless networks by leveraging the parts of digital cities that remain operational.

In this context, we propose BLUEMERGENCY: A new concept based on BT MESH that integrates IoT solutions into post-disaster systems. The key idea behind this concept is to provide a more resilient system by leveraging the parts of digital cities that remain operational. First, since BT MESH allows many-to-many communications, there is not a single point of failure. Second, the mesh devices are typically sensors with an integrated power source (e. g., battery), i. e., most of them remain functional even during a blackout or if the electrical grid is severely impaired. Third, the backward compatibility facilitates the connection of existing Bluetooth devices to an existing mesh network without the need for additional hardware or significant software changes. Finally, by including mobile devices, it is possible to build self-organizing distributed wireless networks by leveraging the parts of digital cities

that remain operational, thus enabling the population to communicate without relying on a centralized infrastructure.

7.2 BLUETOOTH MESH

In the last decade, Bluetooth and especially BLE have risen to become one of the most used communication technologies for the IoT [183]. The key idea behind this standard is to allow existing and new devices to build large-scale multi-hop sensor networks. The standard also provides backward compatibility, i. e., mobile devices compatible with Bluetooth 4.0 or later may also send messages in a BT MESH network. This section briefly introduces the key features and capabilities of BT MESH technology and details the underlying concept.

The key idea behind Bluetooth Mesh is to allow existing and new devices to build large-scale multi-hop sensor networks.

7.2.1 *Technical Background*

BT MESH is a flooding-based network that uses the publish/subscribe model for the data exchange, i. e., devices can send (*publish*) and receive (*subscribe*) certain information according to their interests. These networks can support up to 32767 devices, and a maximum of 127 hops are possible. An unsegmented message has a maximal size of 29 bytes, with the maximum application data payload size being 11 bytes. The standard includes two different bearers: *(i) advertising bearer:* is a non-connectable advertisement bearer which uses a new type of BLE advertisement packet to communicate, and *(ii) Generic Attribute Profile (*GATT*) bearer:* is a connection-oriented bearer, that provides backwards compatibility, i. e., it allows any Bluetooth device compatible with GATT to also be part of a mesh network. This bearer utilizes the Proxy Protocol [55] to exchange data between two devices using a GATT connection.

Bluetooth Mesh is a flooding-based network that uses the publish/subscribe model for the data exchange.

7.2.1.1 *Network Elements*

The devices need to be provisioned in order to build a BT MESH network. During the provisioning process a device—known as a ***provisioner***—distributes necessary security material to an unprovisioned device that wants to join the network. A provisioned device—also called a ***node***—can send and receive mesh messages. Mesh nodes can support one or more additional features:

Mesh nodes can support one or more additional features: relay, proxy, low power, or friend.

- **Relay nodes:** can also retransmit received mesh messages using the advertising bearer.
- **Proxy nodes:** can communicate using both communication bearers: GATT and Advertising.
- **Low Power nodes:** are limited power nodes that scan the communication channel at a reduced duty cycle.

- **Friend nodes:** stores messages addressed to Low Power nodes and retransmits them to those nodes later.

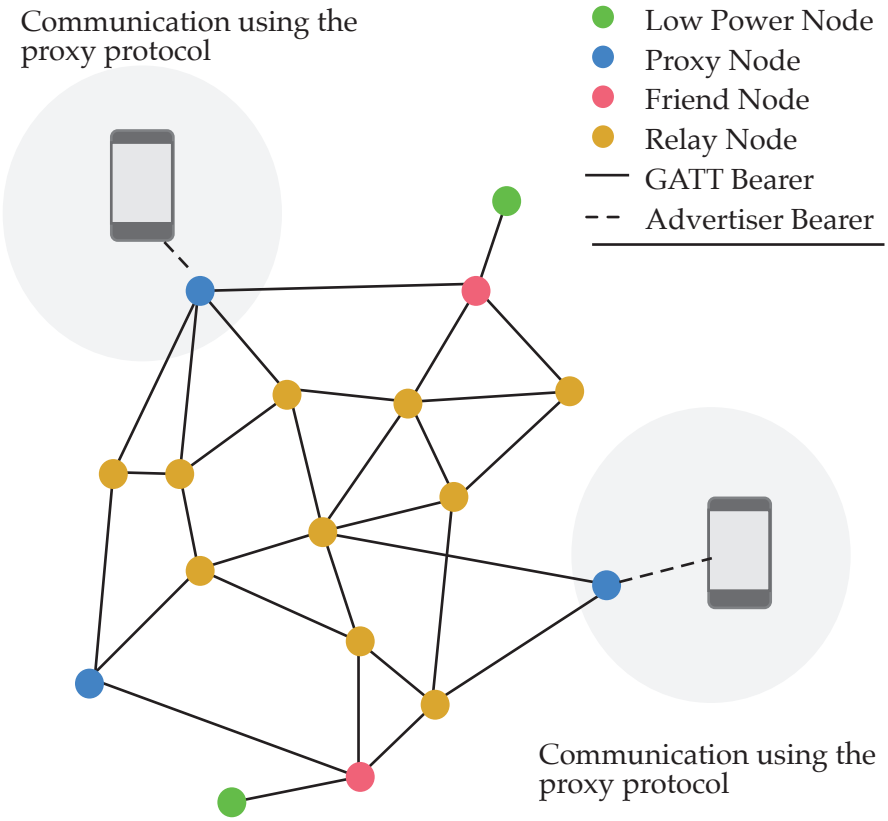


Figure 7.2: Bluetooth Mesh concept.

Figure 7.2 shows a possible BT Mesh network configuration with several nodes and all features supported by a mesh node. For communication, these nodes can either use an advertising or a GATT bearer. Additionally, mobile devices that do not support BT Mesh can communicate with the network using an additional communication protocol—known as ***proxy protocol***—specified in [55].

7.2.1.2 *Elements and Models*

Multiple services define the basic functionality of nodes, which can be generic or vendor specific.

Each mesh node has at least one element. The number of elements does not change during the time that a node is part of a network. Every element has an unique unicast address, and consists of one or multiple services as shown in Figure 7.3. These multiple services define the basic functionality of nodes. Services—also called ***models***—can be generic or vendor-specific. A model is identified by 16-bit (generic) or 32-bit ID (vendor-specific). A model is conformed by a set of states, messages, state transitions and behaviors. The generic models are specified in the standard. Vendor models can be designed and implemented freely. In most cases, generic and vendor models are

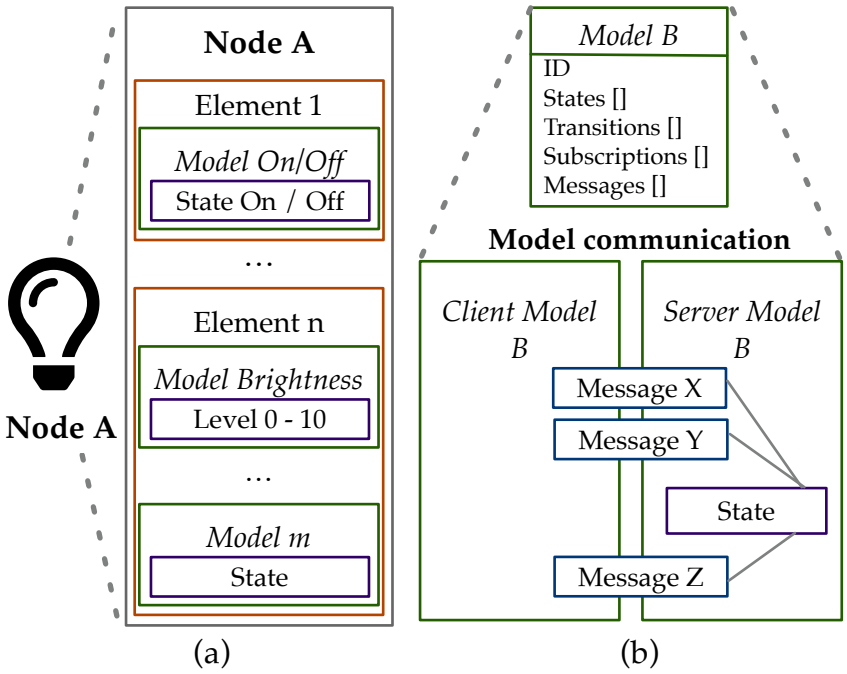


Figure 7.3: An example of Bluetooth Mesh elements and models: (a) mesh node composition, (b) client-server model communication.

implemented using the client/server concept: a server model provides a service, and a client model consumes this service. The client model does not have state. Figure 7.4 visualizes the generic On/Off model, a typical example of a generic model where a state can be set to on or off.

7.2.1.3 *Security*

Bluetooth Mesh considers security as mandatory.

The BT Mesh specification also considers security as mandatory, so all messages exchanged between devices on the network must be encrypted. The standard defines two keys used to secure messages, namely, network keys *NetKey* and application keys *AppKeys*. The *NetKey* allows devices to participate in one or more subnets, as well as in different mesh networks. The *AppKeys* enable devices to receive or to send messages related to a given application domain. Regarding privacy, the standard recommends the implementation of network PDU obfuscation to prevent the tracking of nodes in a mesh network.

7.2.1.4 *Backward Compatibility*

Bluetooth devices compatible with Bluetooth 4.0 or later, which do not implement the Bluetooth Mesh stack, can communicate with nodes from a BT Mesh network using a GATT connection. To this end, these devices need to implement the proxy protocol. This protocol defines two node roles: server and client. The proxy server is a node support-

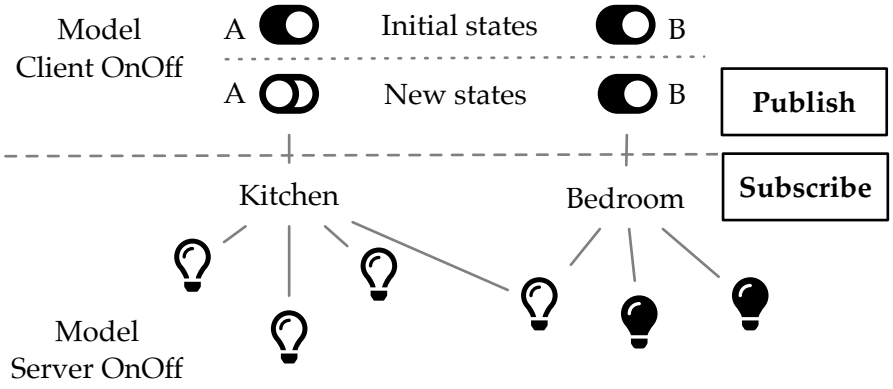


Figure 7.4: An example of a generic model.

Bluetooth devices without the Bluetooth Mesh stack but compatible with Bluetooth 4.0 or later can communicate in a BT MESH network using the proxy protocol.

ing both bearers, and a proxy client node supports only the GATT bearer. For example, mobile devices act as proxy clients to transmit and receive mesh network packets over the connection-oriented GATT bearer. Besides, a mesh node that supports the proxy feature can act as a proxy server, and relay mesh network packets from a proxy client to other nodes in the network.

7.3 THE BLUETOOTH MESH EMERGENCY COMMUNICATION CONCEPT

In this section, we introduce our post-disaster solution that includes devices from IoT solutions such as smart offices and smart homes to build emergency networks.

7.3.1 *Overview*

By considering IoT end devices from smart environments, we can build an emergency network to allow a D2D communication.

Natural or human-made disasters can occur at any time. A typical problem in the aftermath of a disaster is the damage of infrastructure, where mainly information and communication systems are affected and partially or totally unavailable. As a result, millions of people in need of help are isolated, especially during the crucial first hours. This disruption of communication also hinders the coordination of relief efforts.

But, if we consider IoT devices from smart offices and smart homes, we can build an emergency network to allow device-to-device communication. Typically, these end devices are constrained sensors with an integrated power source (e. g., battery), which allows them to be available even if a central power infrastructure is knocked out.

7.3.2 *Relevant Features*

BLUEMERGENCY is designed to complement existing self-organizing ECS. By utilizing the BT MESH networks, our solution fulfils the most representative requirements for emergency networks [18]. In general, we satisfy the following requirements:

BLUEMERGENCY fulfils the most representative requirements for emergency networks: resilience, basis emergency services, self-organizing, mobility and interoperability.

1. *Resilience:* An essential requirement for self-organizing emergency networks is the capability to provide an acceptable level of communication to cope in the absence of infrastructure. A system based on a mesh topology offers resilience, as there is not a single point of failure. In contrast, each device can communicate with other devices and also relay messages.
2. *Basis emergency services:* After a disaster, the communication needs focus mainly on the exchange of small but vital data, such as help messages or telling family and friends that you are safe. By implement a BT MESH vendor model, we can support services commonly used in emergencies [2].
3. *Self-organizing:* The self-organizing capability of BT MESH allows it to build a system that is easily adaptable and relocatable, which improves the reliability of a BT MESH based emergency network.
4. *Mobility:* The integration of mobile devices in BT MESH smart environments facilities the creation of networks with a variable topology.
5. *Interoperability:* One of the main limitations of existing emergency networks is the missing interoperability between the different implementations because of the lack of a common standard. In contrast, BLUEMERGENCY resolves this issue by proposing a solution based on an existing standard.

7.3.3 *Services*

We propose a BT MESH vendor model to facilitate the data exchange between mobile devices in the emergency network. Our implementation includes two functions: a server and a client model. We also support group subscriptions, i. e., nodes using our model can send and receive messages to/from a group. By supporting our model, a mobile device can act as server or client. Currently, we provide only two services commonly used in emergencies [2], namely: *SOS Emergency Messages*, and *I am Alive Notifications*. Table 7.1 summarizes the data structure of each packet using our model.

Our BT MESH vendor model facilitates the data exchange between mobile devices in the emergency network.

As mentioned in 7.2.1.2, a model can also define states. In our case, a mobile device that implements our emergency model can support four different states as summarized in Table 7.2.

Table 7.1: Data structure for the emergency model

Opcodes	Messages	Description
0xE1	0x0A	Message to request help.
0xE2	0x0B	Message to offer help.
0xE3	0x0C	Message to send user status.

Table 7.2: Node states using our vendor emergency model

State	Value	Description
STATE_OK_HELP	0x00	I am fine.
STATE_OFFER_HELP	0x01	I can offer help.
STATE_NEED_HELP	0x02	I need help.
STATE_NEED_OFFER	0x03	I need help and can offer help.

Because all mesh packets are encrypted, a node without the security credentials can neither join the mesh network nor send/receive data to other nodes. To address this, we integrate a QR-Code reader interface to get the minimum required security credentials to join the network. The QR-Code consists of a JavaScript Object Notation (JSON) format data that stores the security credentials needed to be part of the BT Mesh network. These credentials include the network key, application keys for the vendor model, and an index that is needed to identify the subnetwork. Figure 7.5 visualizes an example of using our vendor emergency model. The sensor nodes do not implement our vendor model, they only require to share the network key to relay our data.

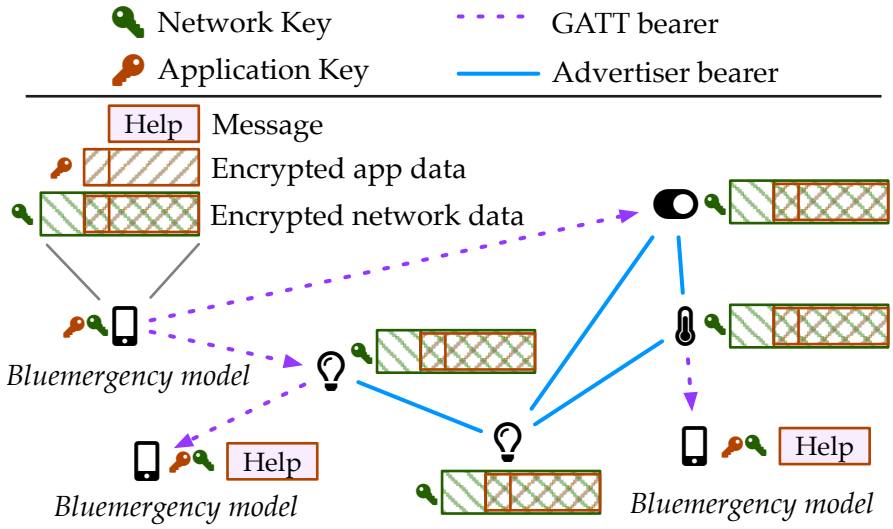
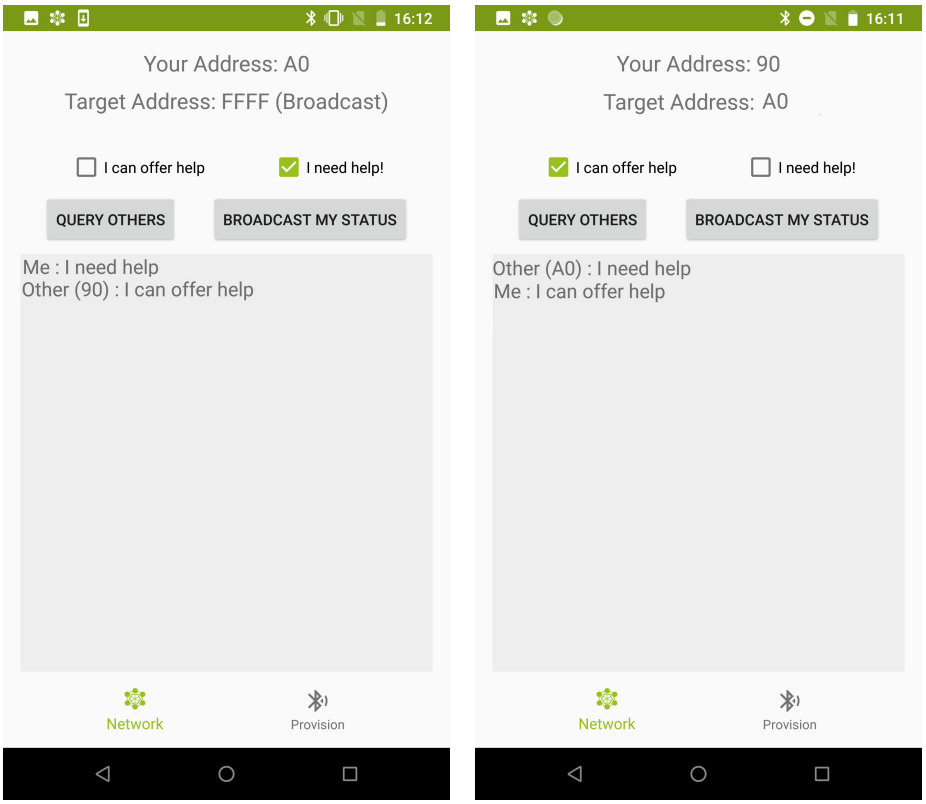


Figure 7.5: An example of using our vendor model.



(a) (b)

Figure 7.6: Screenshots of our Android application developed as proof-of-concept: (a) requesting help, and (b) offering help.

7.4 PROOF-OF-CONCEPT

In this section, we describe in detail our proof-of-concept implementation, as well as the hardware and software utilized. Figure 7.6 illustrates our Android application developed to test the feasibility of BLUEMERGENCY. We validate the communication between smartphone devices using a BT MESH network from two smart scenarios: *Scenario (A)* - smart offices, and *Scenario (B)* - the smart home.

We validate our concept in a smart office and a smart home scenario.

7.4.1 *Hardware Setup*

The testbed consists of RuuviTags [184] sensors based on the nRF52832 SoC from Nordic Semiconductor, Nordic Semiconductor nRF52840 USB Dongles [185], Raspberry Pi 3 Model B+ [186] nodes based on the Broadcom BCM2837B0 SoC and smartphones Nexus 6P running Android version 8.1.0.

The testbed consists of heterogeneous IoT devices and novel devices that integrate the BT MESH stack directly in the firmware,

Table 7.3 summarizes the node features configured on each device for both scenarios. Because of the Raspberry Pis support only the relay features, we use the proxy protocol with Nordic USB Dongles. For simplicity, an additional smartphone is initially used as *provisioner*.

Table 7.3: BT MESH node features supported by the devices in the testbed. We consider following notation: ● fully fulfils feature, ◑ fulfils, but not used, ○ does not fulfil feature.
* Pis were used only in the smart office scenario.

	RuuviTags/USB Dongles	Linux Pis*	Smartphones
Relay	●	●	○
Proxy	●	○	○
GATT Bearer	●	○	●
Adv. Bearer	●	●	○

7.4.1.1 *Scenario A: Smart Office*

Figure 7.7 visualizes the location of the nodes on scenario *A*. The nodes are distributed throughout an office building over two adjacent floors, each floor consists of offices and meeting rooms. Due to the high density of Wi-Fi access points as well as other equipment operating in the 2.4GHz band, the nodes have to cope with high interference. On the first floor, the nodes are arranged in an area of approximately 900 m^2, and on the 2nd floor, the overall facility measures approximately 180 m^2. The maximal distance between two nodes is approx. 10 m, and the minimal distance is close to 1 m.

Due to the high density of equipment operating in the 2.4GHz band, the nodes have to cope with high interference.

7.4.1.2 *Scenario B: Smart Home*

Figure 7.8 shows the proof-of-concept setup for scenario *B*. We distribute the nodes in a brick house with two floors in a residential area. The area covered by the smart home installation is approx 63 m^2 per floor. The maximal distance between two nodes is approx. 6.5 m, and the minimal distance is approx. 3 m.

The area covered by the smart home installation is approx 63 m^2 per floor.

7.4.2 *Software*

For our experiments, we use the SDK Softdevice version 6.1.0 [187] and the Mesh SDK version 3.1.0 [188], both developed by Nordic Semiconductor. The Android-nRF-Mesh library [189] is utilized for the initial setup configuration (provisioning phase). We build and extend the RuuviTag firmware from the Git repository [190] to integrate the mesh stack. For supporting mesh on the Raspberry Pis, BlueZ[191] version 5.50 was extended and rebuilt. Additionally, we integrate the Nordic library [189] to our smartphone application to support the proxy protocol as well as the proxy client on the smartphones.

We extend the RuuviTag firmware to integrate the mesh stack.

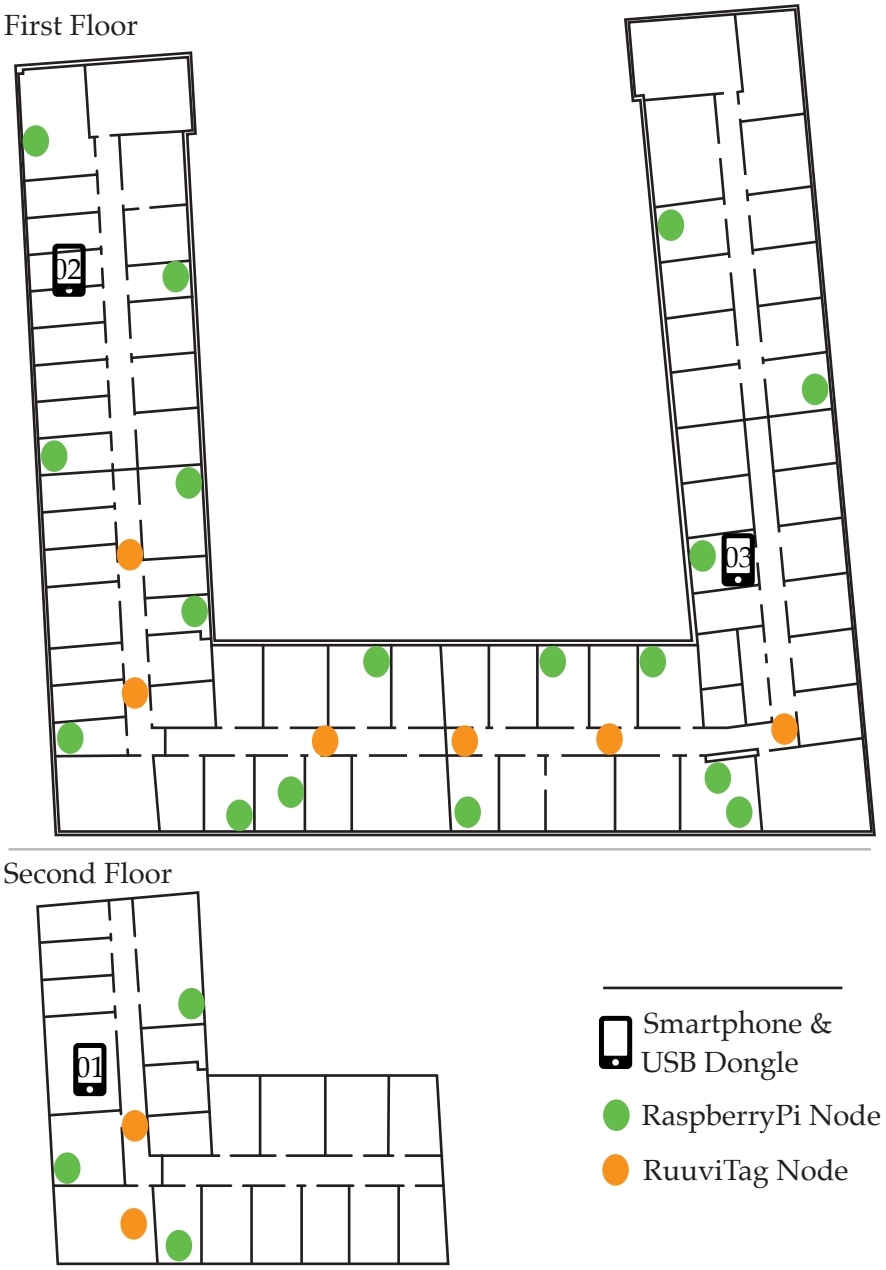


Figure 7.7: Proof-of-concept setup for the smart office experiments.

7.4.3 *Support for the Proxy Protocol*

We implement and integrate the proxy functionality into our Android application.

Currently, the Android Bluetooth stack does not provide the BT Mesh stack nor is the proxy protocol built-in. To address this, we integrate the Android-nRF-Mesh library [189] developed by Nordic Semiconductor into our smartphone application. The nRF-Mesh library supports the proxy protocol on Android devices only for the network configuration phase. To enable mobile devices to participate in an existing BT Mesh network, we implement and integrate the proxy functionality

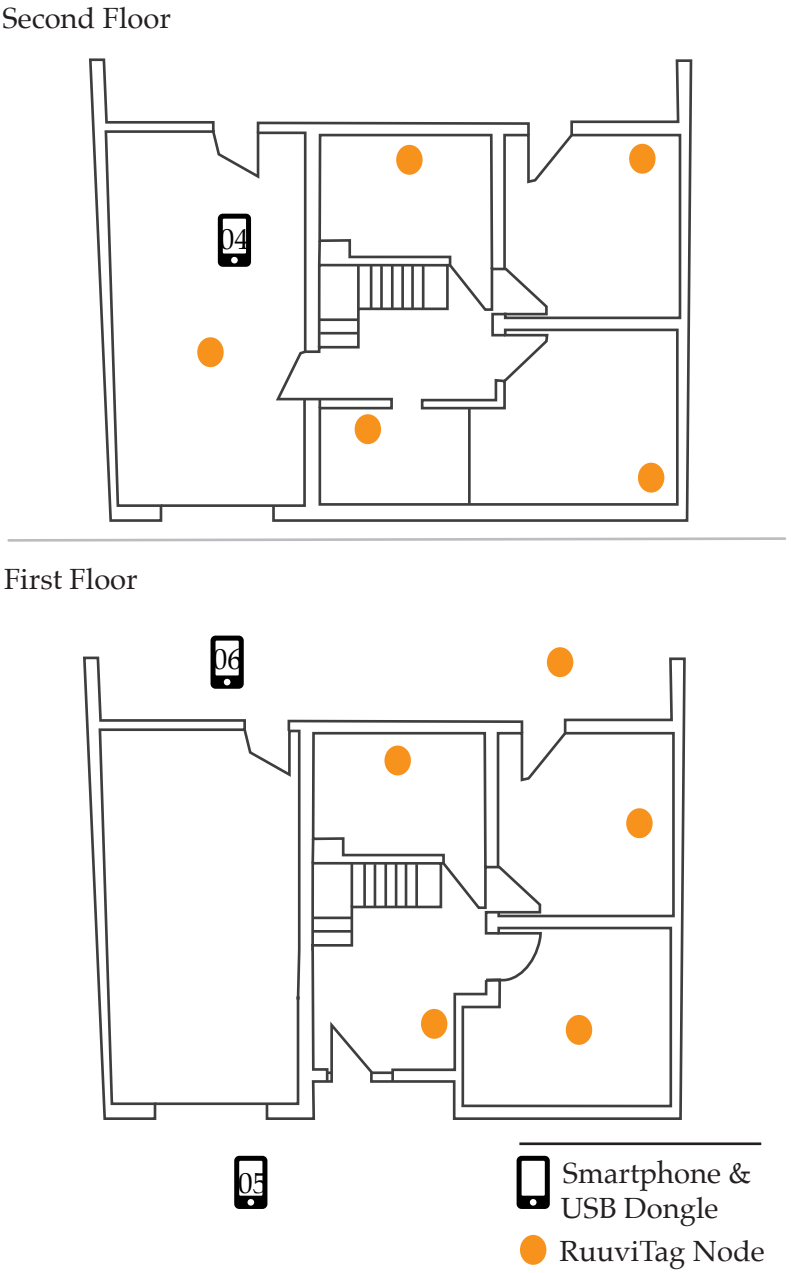


Figure 7.8: Proof-of-concept setup for the smart home experiments.

specified in the standard into our Android application. With these changes, a smartphone can receive and deal with BT Mesh messages.

7.4.4 *Network Configuration Phase*

The QR-code allows smartphone to be part of the existing network.

As mentioned before, a *provisioner* is responsible for the initial setup and any reconfiguration of the nodes in the network. For the experiments, we consider an already existing BT Mesh network, both in the smart home as well as in the smart office scenario. We also implement

a scanning QR-Code functionality, to allow smartphone devices to be part of the existing network by only scanning the required security materials.

7.4.5 *Network Services*

For the experiments, we consider the following configuration: each RuuviTag and Raspberry Pi implement and enable the relay feature. Because the Android application implements our vendor model, the smartphones can exchange messages between them using the existing BT MESH network. For simplicity, we set the destination address to predefined broadcast address. So each node that receives a message and implements our model can process it.

Each RuuviTag and Raspberry Pi implement and enable the relay feature.

7.5 EXPERIMENTAL EVALUATION

In this section, we show the feasibility of our solution that leverages smart environments to help form post-disaster communication networks. To this end, we implement a proof-of-concept application and test it in combination with the two outlined BT MESH scenarios using real devices.

A mobile application was developed as proof-of-concept for Android-based smartphones.

7.5.1 *Experimental Setup*

We perform a set of experiments to evaluate the performance of a BT MESH network regarding packet loss and response time. Each interaction from the experiments implies a variation of the number of messages sent: *(i)* first, we send 5 messages per minute, *(ii)* we increase the number of messages to 10 messages per minute, and finally, *(iii)* we send 20 messages per minute. Each experiment runs for 12 minutes. We repeat this procedure 5 times. Detailed experiment settings are provided in Table 7.4

7.5.1.1 *Scenario A: Smart Office*

We first configure ***01*** as the source node, which generates the BT MESH messages. It sends a help request message to all nodes in the network, in our case, to the other smartphones. As illustrated in Figure 7.7, ***01*** is located on the second floor, and the other nodes ***02, 03*** are located on the first floor. These nodes respond to the help request by confirming that they offer help.

The source node 01 sends a help request to all nodes in the network.

7.5.1.2 *Scenario B: Smart Home*

In addition to the smart office scenario, a smart home experiment was carried out. As depicted in Figure 7.8, node ***04*** was located inside

The source node 04 sends a help request to all nodes in the network.

Table 7.4: BLUEMERGENCY proof-of-concept settings

Scenario	Parameter	Value(s)
Office (A)	Dimensions w x h	85 x 65 [m]
	Number of relay nodes	28
	Distance between nodes (max, min)	(10, 1) [m]
Home (B)	Dimensions w x h	13.6 x 9.25 [m]
	Number of relay nodes	8
	Distance between nodes (max, min)	(6.5, 3) [m]
Both	Number of proxy servers	3
	Number of proxy clients	3
	Models	vendor emergency
	Number of msgs sent per minute	5 - Experiment I
		10 - Experiment II
		20 - Experiment III

the house, and nodes ***05, 06*** were located outside the house in close proximity. As a result, the smartphones outside the house were able to connect with the BT MESH network and to reach any device located inside the house.

7.5.2 *Evaluation Metrics*

We measure the performance of our system in a real-world environment, including external interference.

In our evaluation, we analyze two metrics: the response time and the packet loss rate.

7.5.2.1 *Response Time*

Is the time elapsed between the sending of a message and its reception in the destination. This latency should be as low as possible.

7.5.2.2 *Packet Loss Rate*

The proportion of packets lost during a transmission also represents an important factor for such a system. It indicates how reliable the network is in terms of packets delivered successfully to the destination.

7.5.3 *Results*

The main goal of the experiments was to measure the response time to a help request as well as the packet loss rate in a real-world environment, including external interference, i. e., BLE devices such as other

Table 7.5: BLUEMERGENCY experiment results

	Metric	Mean	Standard deviation	Median
	Number of hops	6.15	1.43	6.0
A	Response time [ms]	1053.13	453.20	1020.0
	Packet loss rate (%)	38.21	17.75	35.4
	Number of hops	3.11	0.32	3.0
B	Response time [ms]	995.53	349.60	827.5
	Packet loss rate (%)	8.5	4.67	11.2

smartphones, Wi-Fi devices. Table 7.5 summarizes the most important results from our experiments.

7.5.3.1 *Response Time*

The response time is in the order of one second for devices in proximity and increases to around 1.5 seconds for distant devices.

Figure 7.9 visualizes the response time to a help request in both smart environments. We can observe that the response time is directly influenced by the location of the nodes. As the distance between the nodes increases, the response time also grows. This is expected, as a message needs to traverse more hops to reach the destination. Furthermore, each node that relays a message implies additional processing time. The response time is in the order of one second for devices in proximity and increases to around 1.5 seconds for distant devices. While these latencies are considerably higher than latencies in infrastructure networks, we consider them to be acceptable in post-disaster scenarios, where the fact that communication and basic services are available at all can be considered paramount to minimizing latency.

7.5.3.2 *Packet Loss Rate*

The packet delivery is affected by the external interfering transmissions in the 2.4 GHz band.

Figure 7.10 shows the percentage of packet loss for each experiment. Although the packet loss rate for the smart home scenario indicates a similar pattern, it differs in the smart office scenario. This result is reasonable, as, during work hours, there are a lot of additional BLE and Wi-Fi devices such as notebooks, smartwatches, that generate interfering transmissions in the 2.4 GHz band.

7.6 RELATED WORK

So far, existing work in the field of BT MESH focuses mainly on the performance evaluation of such a network in smart environments, e. g., for building automation applications [192], proposing a smart-home architecture to demonstrate the feasibility of using this standard

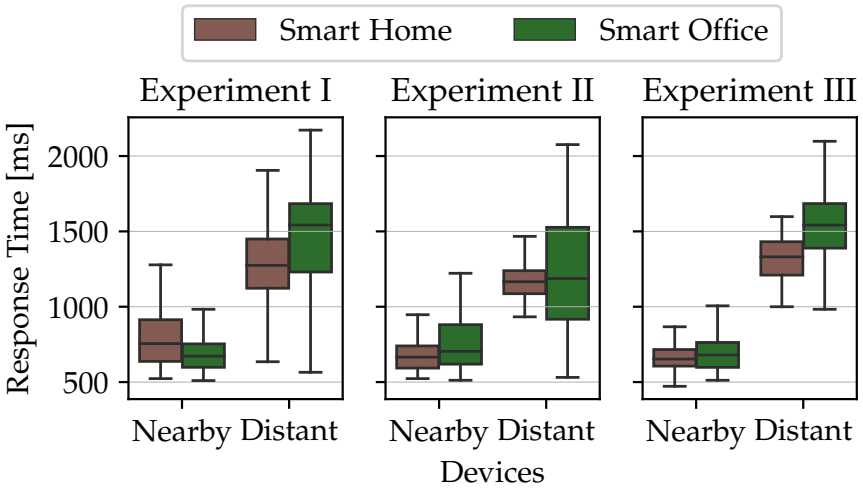


Figure 7.9: Response time to a help message in both scenarios.

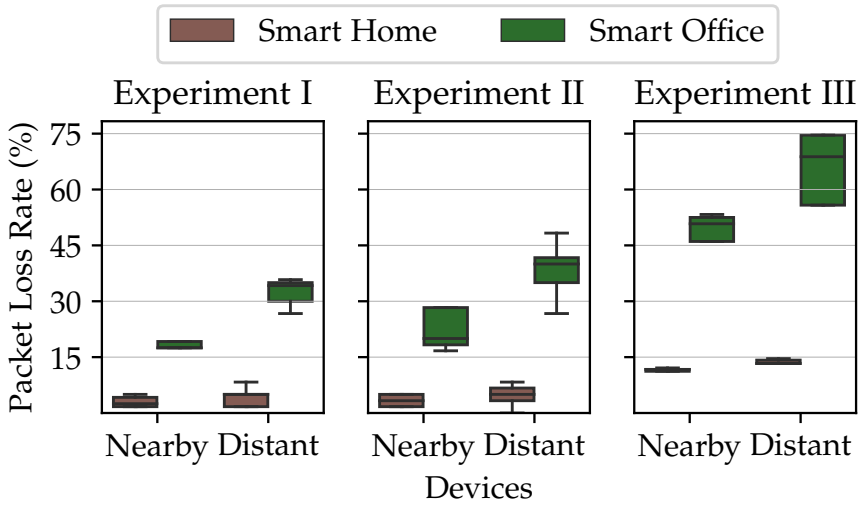


Figure 7.10: Packet loss rate in both scenarios.

Most of existing solutions for self-organizing emergency networks require either the installation of additional hardware or software modifications are necessary.

in smart home control systems [193], or for smart cities [194]. Our work aims at providing a solution to build self-organizing emergency networks without relying on central infrastructure.

The importance of self-organizing ad hoc networks after a disaster has been widely studied in recent researches. There are already several studies focusing on post-disaster systems based on self-organizing Mobile Ad Hoc Networks (MANETs) [2, 3, 88, 89, 195]. These solutions leverage MANETs or Delay Tolerant Networks (DTNs) technology to facilitate message routing/forwarding/spreading in the affected area. However, most of them either require the installation of additional hardware or software modifications are necessary, e. g., jail-breaking off-the-shelf devices, to enable mobile devices to be part of a wireless mesh network.

In contrast, this work proposes a solution based on the BT MESH standard to facilitate device-to-device communication in post-disaster scenarios. The proposed solution involves devices that typically remain functional after a disaster, i. e., by utilizing the infrastructure from smart environments. We present an experimental evaluation of such a system using well-known IoT application scenarios, namely, smart office and smart home. Our proof-of-concept considers heterogeneous devices, including devices that support the BT MESH stack, and devices which can communicate with the network without the need to implement the whole stack.

This work proposes a solution based on the BT MESH standard to facilitate a D2D communication in post-disaster scenarios.

7.7 SUMMARY

As mentioned above, building post-disaster networks based purely on smartphones remains a challenging task, e. g., due to the limited communication range, scalability, etc. The rapidly growing IoT technology, however, offers the possibility to improve this situation. For instance, IoT devices can help to relieve congestion or build a backup network in case of cyber-attacks. In this chapter, we showed that smart environments, as found in today's and future digital cities, can contribute to establishing post-disaster networks. In particular, we showed that the novel BT MESH standard, which is supported by a wide range of IoT solutions, can be used to mediate post-disaster device-to-device communication, even using most of today's smartphones. We demonstrate the feasibility of such a system on common off-the-shelf devices by designing and implementing our BLUEMERGENCY proof-of-concept system. To this end, an Android application implements the proxy protocol specified in the standard. Additionally, we propose an emergency model to enable smartphones to exchange data using existing IoT devices. We show the feasibility and performance of our solution in two BT MESH realistic scenarios, namely a smart office and a smart home scenario. For the performance evaluation, we utilized heterogeneous IoT devices, i. e., linux-based devices, and novel devices that integrate the BT MESH stack directly in the firmware, together with regular Android smartphones that do not offer native BT MESH support. By utilizing BT MESH as mediating technology, we can address the lack of direct communication between nearby mobile devices without the need to modify such devices, e. g., jail-breaking a device to support Wi-Fi in ad hoc mode. Finally, our experiments facilitate a first performance analysis of such a system.

Smart environments as found in today's and future digital cities can contribute in establishing post-disaster networks.

Part IV

CONCLUSIONS AND OUTLOOK

This part summarizes the results of this thesis, provides conclusions and gives an outlook.

8

CONCLUSIONS

8.1 SUMMARY AND CONCLUSION

In this thesis, we have proposed a comprehensive suite of solutions that contribute to facilitating secure device-to-device communication for emergency responses. Building post-disaster networks for enabling civilians to communicate using smartphones also involves new and challenging scenarios, especially improving the resilience of such systems while considering real-world human behaviour. In this context, we focused on two key research directions to solve these challenges. First, we have analyzed existing mechanisms and approaches that facilitate population communications using smartphone-based emergency communication systems. Existing solutions mainly consider traces gathered in everyday activities for the simulation models or only include the input and behaviour of professional disaster relief personnel or other organizations. We have focused on involving civilians, i. e., spontaneous volunteers, and their requirements into the design and deployment of post-disaster systems. Regarding the second research direction, we have provided mechanisms to improve the resilience of smartphone-based emergency communication systems. Within the scope of this thesis, we have mainly contributed as follows.

In the first part, we summarized common factors regarding communication issues, population needs, from representative disaster scenarios from the last decade. Then, we investigated and analyzed existing post-disaster solutions focusing mainly on smartphone-based solutions. With this information, we identified relevant civilian requirements that such systems should fill. Besides, we defined the communication services required after disasters. Using these requirements and services from our analysis as a basis, we conducted a large-scale field test of a scripted disaster scenario with 125 participants. By collecting data about user mobility, user interaction with the emergency services, and smartphone sensor readings, we gained insights from civilians' behaviour when utilizing a smartphone-based post-disaster system.

In the second part, we focused on improving the resilience of such systems. For doing so, we specifically proposed mechanisms to deal with the security services in a decentralized way, to save energy during neighbour discoveries for opportunistic encounters, and finally to compensate for scarce infrastructure after a disaster.

Regarding decentralized bootstrapping security, we presented Sea of Lights (SoL), a lightweight scheme for bootstrapping Device-to-Device

(D2D) security and wirelessly spreading it to enable secure distributed self-organizing networks. SoL was implemented in a two-layer fashion architecture: *(i)* Trust Management and *(ii)* Key Management. The Trust Management layer based on a simplified version of the Web-of-Trust (WoT) paradigm. This layer covers the bootstrapping and establishment of mutual trust as well as the synchronization and update of the local trust repository. The Key Management layer focused on the generation and protection of the key material. It controls and manages access to the keys. Besides, this layer is responsible for choosing appropriate key storages. We tested the feasibility of our solution using Android devices. Also, we evaluated the performance of SoL by means of simulation. By doing so, we were able to provide a solution for bootstrapping security associations between mobile devices in partially disconnected networks in a decentralized way.

Furthermore, we investigated mechanisms that allow saving energy consumption for opportunistic encounters. In this context, Neighbour Discovery (ND) represents one of the leading energy consumers. Thus, we developed SavIng Energy in STAtic Phases (SIESTA), an adaptive and efficient neighbour discovery scheme for self-organizing networks. SIESTA was developed for saving energy during static phases while adapting the discovery parameters if the devices were moving. We evaluated the performance of SIESTA through a proof-of-concept implementation and simulations. Hence, we provided an opportunistic networking framework for mobile devices that also optimizes the neighbour discovery process to save energy-consumption in D2D communications.

Finally, we proposed Bluetooth Mesh emErgency (BlueMergency), a novel emergency network concept that uses the Internet of Things (IoT) technology and the Bluetooth Mesh (BT Mesh) standard for mediating emergency communication systems. We sought to consider communication tools that ordinary civilians can use, i. e., without requiring the installation of additional hardware or significant software modifications. In particular, we showed that smart environments could contribute to establishing post-disaster networks without relying on central communication infrastructures. In addition, we implemented an Android application as a proof-of-concept to show the feasibility of such a system on conventional off-the-shelf devices.

8.2 OUTLOOK

The contributions of this thesis raise opportunities for optimizing secure D2D communication for emergency response systems. There are new research directions and challenges that still need to be addressed. We see for the need for more real-world datasets gathered of the evaluation of D2D emergency communication systems considering human behaviour during disasters. Even though it is impractical to cover all

imaginable disaster scenarios, the collection of these datasets opens up new possibilities for understanding real-world human behaviour in disasters. Thus, it allows for developing more realistic systems for such situations.

Concerning security, an important aspect remains the implementation of methods focused on the revocation of compromised keys in decentralized networks. Indeed, key revocation plays an important role in keeping security in a network as a compromised key can affect the trust of the system partially or totally. However, as summarized in [196], there is no one-for-all key revocation scheme which deals with all the security issues and requirements of such networks. For example, many of them assume the existence of a central authority or a prior knowledge of the network topology, which is not always possible, especially in real-world mobile systems, where devices can join and leave the network arbitrarily. Several schemes rely on the information provided by the devices in the network to deal with misbehaving users. However, this can also be used by malicious users to affect the network and to disable legitimate devices.

Although our experiments show the feasibility of the proposed BlueMergency concept, we envision several improvements in future work. Hence, the proposed emergency services could be enriched by location information to help the discovery of persons in need. Since BT Mesh was not designed for emergency use, several other challenges remain. While security is a mandatory BT Mesh feature, i. e., without the corresponding security credentials, a device can neither join a mesh network nor exchange data with other nodes; it still lacks usability during emergencies. For practical applicability, easy to use D2D security solutions could be integrated into our BlueMergency concept. Finally, to ensure that smartphone-based post-disaster solutions become real helpful tools during disasters, we need a cross-platform D2D technology solution for supporting interoperability between most of the conventional smartphones used by the population.

BIBLIOGRAPHY

[1] Flor Álvarez, Matthias Hollick, and Paul Gardner-Stephen. "Maintaining both Availability and Integrity of Communications: Challenges and Guidelines for Data Security and Privacy During Disasters and Crises." In: *Global Humanitarian Technology Conference*. IEEE, 2016, pp. 62–70. DOI: 10.1109/GHTC.2016.7857261.

[2] Patrick Lieser, Flor Álvarez, Paul Gardner-Stephen, Matthias Hollick, and Doreen Boehnstedt. "Architecture for Responsive Emergency Communications Networks." In: *Global Humanitarian Technology Conference*. IEEE, 2017, pp. 1–9. DOI: 10.1109/GHTC.2017.8239239.

[3] Flor Álvarez, Lars Almon, Patrick Lieser, Tobias Meuser, Yannick Dylla, Björn Richerzhagen, Matthias Hollick, and Ralf Steinmetz. "Conducting a Large-scale Field Test of a Smartphone-based Communication Network for Emergency Response." In: *Proceedings of the 13th Workshop on Challenged Networks*. ACM, 2018, pp. 3–10. DOI: 10.1145/3264844.3264845.

[4] Flor Álvarez, Max Kolhagen, and Matthias Hollick. "Sea of Lights: Practical Device-to-Device Security Bootstrapping in the Dark." In: *Proceedings of the 43rd Conference on Local Computer Networks*. IEEE, 2018, pp. 124–132. DOI: 10.1109/LCN.2018.8638102.

[5] Flor Álvarez, Tobias Schultes, and Matthias Hollick. "SIESTA: Smart Neighbor Discovery for Device-to-device Communications." In: *International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. (Submitted). IEEE. 2020.

[6] Flor Álvarez, Lars Almon, Hauke Radtki, and Matthias Hollick. "Bluemergency: Mediating Post-disaster Communication Systems using the Internet of Things and Bluetooth Mesh." In: *Global Humanitarian Technology Conference*. IEEE. 2019, pp. 62–70.

[7] Yannick Dylla. "Aufbereitung und Evaluation des SMARTER Feldversuchs über Verzögerungstolerante Netzwerke im Katastrophenfall." MA thesis. Technische Universität Darmstadt, 2018.

[8] Max Kolhagen. "Utilizing Secure Elements to Establish Authentication in Mobile Ad-hoc Networks." MA thesis. Technische Universität Darmstadt, 2016.

[9] Tobias Schultes. "A Framework for Adaptive Energy-Efficient Neighbor Discovery in Opportunistic Networks." MA thesis. Technische Universität Darmstadt, 2016.

[10] Ari Keränen, Jörg Ott, and Teemu Kärkkäinen. "The ONE Simulator for DTN Protocol Evaluation." In: *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*. ICST, 2009, 55:1–55:10. DOI: 10.4108/ICST.SIMUTOOLS2009.5674.

[11] Dan Wang, Zheng Xiang, and Daniel R. Fesenmaier. "Smartphone Use in Everyday Life and Travel." In: *Journal of Travel Research* 55.1 (2016), pp. 52–63. DOI: 10.1177/0047287514535847.

[12] IHS Statista 2019. *Forecast number of mobile devices worldwide from 2019 to 2023 (in billions)*. Accessed on 11.12.2019. URL: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/.

[13] Bin Guo, Zhiwen Yu, Xingshe Zhou, and Daqing Zhang. "From Participatory Sensing to Mobile Crowd Sensing." In: *International Conference on Pervasive Computing and Communication Workshops*. IEEE, 2014, pp. 593–598. DOI: 10.1109/PerComW.2014.6815273.

[14] Ellen Barry, The New York Times. *Earthquake Devastates Nepal, Killing More Than 1,900*. Accessed on 11.12.2019. 2015. URL: https://www.nytimes.com/.

[15] CNN Ray Sanchez. *Power outages: Post-Irma recovery includes turning on the lights*. Accessed on 11.12.2019. 2017. URL: http://edition.cnn.com/.

[16] Los Angeles Times. *Censors in China keep mainlanders in dark about Hong Kong protests*. Accessed on 11.12.2019. URL: http://www.latimes.com/.

[17] Erika Rosas, Nicolás Hidalgo, Veronica Gil-Costa, Carolina Bonacic, Mauricio Marin, Hermes Senger, Luciana Arantes, Cesar Marcondes, and Olivier Marin. "Survey on Simulation for Mobile Ad-Hoc Communication for Disaster Scenarios." In: *Journal of Computer Science and Technology* 31.2 (2016), pp. 326–349. DOI: 10.1007/s11390-016-1630-x.

[18] Karen Miranda, Antonella Molinaro, and Tahiry Razafindralambo. "A Survey on Rapidly Deployable Solutions for Post-Disaster Networks." In: *Communications Magazine* 54.4 (2016), pp. 117–123. DOI: 10.1109/MCOM.2016.7452275.

[19] Kamran Ali, Huan X. Nguyen, Purav Shah, Quoc-Tuan Vien, and Even Ever. "Internet of Things (IoT) Considerations, Requirements, and Architectures for Disaster Management System." In: *Performability in Internet of Things*. Springer, 2019, pp. 111–125. DOI: 10.1007/978-3-319-93557-7_7.

[20] IHS Statista. *Internet of Things (IoT) connected devices installed worldwide from 2018, 2025 and 2030 (in billions)*. Accessed on 11.12.2019. 2019. URL: https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/.

[21] Ejaz Ahmed, Ibrar Yaqoob, Abdullah Gani, Muhammad Imran, and Mohsen Guizani. "Internet-of-Things-based Smart Environments: State of the Art, Taxonomy, and Open Research Challenges." In: *Wireless Communications* 23.5 (2016), pp. 10–16. DOI: 10.1109/MWC.2016.7721736.

[22] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. "Internet of Things for Smart Cities." In: *IEEE Internet of Things Journal* 1.1 (2014), pp. 22–32. DOI: 10.1109/JIOT.2014.2306328.

[23] Fadi Shrouf, Joaquin Ordieres, and Giovanni Miragliotta. "Smart Factories in Industry 4.0: A Review of the Concept and of Energy Management Approached in Production Based on the Internet of Things Paradigm." In: *International Conference on Industrial Engineering and Engineering Management*. IEEE, 2014, pp. 697–701. DOI: 10.1109/IEEM.2014.7058728.

[24] Leysia Palen and Sophia B Liu. "Citizen Communications in Crisis: Anticipating a Future of ICT-Supported Public Participation." In: *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*. ACM. 2007, pp. 727–736. DOI: 10.1145/1240624.1240736.

[25] Muhammad Azizi Mohd Ariffin, Angelos K Marnerides, and Andreas U Mauthe. "Multi-level resilience in networked environments: concepts & principles." In: *14th Annual Consumer Communications & Networking Conference*. IEEE. 2017, pp. 272–275. DOI: 10.1109/CCNC.2017.7983118.

[26] Andreas Mauthe, David Hutchison, Egemen K Cetinkaya, Ivan Ganchev, Jacek Rak, James PG Sterbenz, Matthias Gunkelk, Paul Smith, and Teresa Gomes. "Disaster-resilient communication networks: Principles and best practices." In: *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*. IEEE. 2016, pp. 1–10. DOI: 10.1109/RNDM.2016.7608262.

[27] Manon Jurgens and Ira Helsloot. "The effect of social media on the dynamics of (self) resilience during disasters: A literature review." In: *Journal of Contingencies and Crisis Management* 26.1 (2018), pp. 79–88. DOI: 10.1111/1468-5973.12212.

[28] Simon Dobson, David Hutchison, Andreas Mauthe, Alberto Schaeffer-Filho, Paul Smith, and James PG Sterbenz. "Self-Organization and Resilience for Networked Systems: Design

Principles and Open Research Issues." In: *Proceedings of the IEEE* 107.4 (2019), pp. 819–834. DOI: 10.1109/JPROC.2019.2894512.

[29] Marco Conti and Silvia Giordano. "Mobile Ad Hoc Networking: Milestones, Challenges, and New Research Directions." In: *Communications Magazine* 52.1 (2014), pp. 85–96. DOI: 10.1109/MCOM.2014.6710069.

[30] Abraham Martín-Campillo, Jon Crowcroft, Eiko Yoneki, and Ramon Martí. "Evaluating opportunistic networks in disaster scenarios." In: *Journal of Network and computer applications* 36.2 (2013), pp. 870–880. DOI: https://doi.org/10.1016/j.jnca.2012.11.001.

[31] Daniel Reina, J.M.L. Coca, M. Askalani, Sergio L. Toral, Federico Barrero, Eleana Asimakopoulou, Stelios Sotiriadis, and Nik Bessis. "A Survey on Ad Hoc Networks for Disaster Scenarios." In: *International Conference on Intelligent Networking and Collaborative Systems*. IEEE, 2014, pp. 433–438. DOI: 10.1109/INCoS.2014.28.

[32] Osnat Mokryn, Dror Karmi, Akiva Elkayam, and Tomer Teller. "Help Me: Opportunistic Smart Rescue Application and System." In: *11th Annual Mediterranean Ad Hoc Networking Workshop*. IEEE, 2012, pp. 98–105. DOI: 10.1109/MedHocNet.2012.6257129.

[33] Allan Goncalves, Carlos Silva, and Patricia Morreale. "Design of a Mobile Ad Hoc Network Communication App for Disaster Recovery." In: *28th International Conference on Advanced Information Networking and Applications Workshops*. IEEE, 2014, pp. 121–126. DOI: 10.1109/WAINA.2014.26.

[34] Konstandinos Koumidis, Panayiotis Kolios, Christos Panayiotou, and Georgios Ellinas. "ProximAid: Proximal adhoc networking to Aid emergency response." In: *2nd International Conference on Information and Communication Technologies for Disaster Management*. IEEE. 2015, pp. 20–26. DOI: 10.1109/ICT-DM.2015.7402031.

[35] Marco Di Felice, Luca Bedogni, and Luciano Bononi. "The Emergency Direct Mobile App: Safety Message Dissemination over a Multi-Group Network of Smartphones Using Wi-Fi Direct." In: *Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access*. ACM, 2016, pp. 99–106. DOI: 10.1145/2989250.2989257.

[36] Milan Schmittner. "Scalable and secure multicast routing for mobile ad-hoc networks." MA thesis. Technische Universität, 2014.

[37] Li Li, Xiaoxiong Zhong, and Yang Qin. "A secure routing based on social trust in opportunistic networks." In: *International Conference on Communication Systems*. IEEE, 2016. DOI: 10.1109/ICCS.2016.7833575.

[38] Sacha Trifunovic, Andreea Picu, Theus Hossmann, and Karin Anna Hummel. "Adaptive Role Switching for Fair and Efficient Battery Usage in Device-to-device Communication." In: *SIGMOBILE Mobile Computing Communication Review* 18.1 (2014), pp. 25–36. DOI: 10.1145/2581555.2581560.

[39] Lorenzo Bracciale, Pierpaolo Loreti, and Giuseppe Bianchi. "The Sleepy Bird Catches More Worms: Revisiting Energy Efficient Neighbor Discovery." In: *Transactions on Mobile Computing* 15.7 (2016), pp. 1812–1825. DOI: 10.1109/TMC.2015.2471299.

[40] Mathew Orlinski and Nick Filer. "Neighbour discovery in opportunistic networks." In: *Ad Hoc Networks* 25.PB (2015), pp. 383–392. DOI: 10.1016/j.adhoc.2014.07.024.

[41] Andrea Hess, Esa Hyytiä, and Jörg Ott. "Efficient Neighbor Discovery in Mobile Opportunistic Networking using Mobility Awareness." In: *Sixth International Conference on Communication Systems and Networks*. IEEE, 2014, pp. 1–8. DOI: 10.1109/COMSNETS.2014.6734890.

[42] Wenjie Hu, Guohong Cao, Srikanth V. Krishanamurthy, and Prasant Mohapatra. "Mobility-Assisted Energy-Aware User Contact Detection in Mobile Social Networks." In: *33rd International Conference on Distributed Computing Systems*. IEEE, 2013, pp. 155–164. DOI: 10.1109/ICDCS.2013.40.

[43] Gokce Gorbil. "No Way Out: Emergency Evacuation With No Internet Access." In: *International Conference on Pervasive Computing and Communication Workshops*. IEEE. 2015, pp. 505–511. DOI: 10.1109/PERCOMW.2015.7134089.

[44] Nils Aschenbruck, Aarti Munjal, and Tracy Camp. "Trace-based mobility modeling for multi-hop wireless networks." In: *Computer Communications* 34.6 (2011), pp. 704–714. DOI: 10.1016/j.comcom.2010.11.002.

[45] Iain Parris, Fehmi B. Abdesslem, and Tristan Henderson. "Facebook or Fakebook? The effects of simulated mobile applications on simulated mobile networks." In: *Ad Hoc Networks* 12 (2014), pp. 35–49. DOI: 10.1016/j.adhoc.2012.05.008.

[46] Injong Rhee, Minsu Shin, Seongik Hong, Kyunghan Lee, Seong J. Kim, and Song Chong. "On the Levy-Walk Nature of Human Mobility." In: *IEEE/ACM Transactions on Networking* 19.3 (2011), pp. 630–643. DOI: 10.1109/TNET.2011.2120618.

[47] Mirco Musolesi, Mattia Piraccini, Kristof Fodor, Antonio Corradi, and Andrew T. Campbell. "Supporting Energy-Efficient Uploading Strategies for Continuous Sensing Applications on Mobile Phones." In: *International Conference on Pervasive Computing*. Springer. 2010, pp. 355–372. DOI: 10.1007/978-3-642-12654-3_21.

[48] Murray Turoff. "Past and Future Emergency Response Information Systems." In: *Communications of the ACM* 45.4 (2002), pp. 29–32. DOI: 10.1145/505248.505265.

[49] Jacob N Shapiro and David A Siegel. "Coordination and security: How mobile communications affect insurgency." In: *Journal of Peace Research* 52.3 (2015), pp. 312–322. DOI: 10.1177/0022343314559624.

[50] John Burgess, George Dean Bissias, Mark D Corner, and Brian Neil Levine. "Surviving attacks on disruption-tolerant networks without authentication." In: *Proceedings of the 8th International Symposium on Mobile Ad Hoc Networking and Computing*. ACM, 2007, pp. 61–70. DOI: 10.1145/1288107.1288116.

[51] Fai C. Choo, Mun C. Chan, and Ee-Chien Chang. "Robustness of DTN against Routing Attacks." In: *Second International Conference on COMmunication Systems and NETworks*. IEEE, 2010, pp. 1–10. DOI: 10.1109/COMSNETS.2010.5432014.

[52] *SMARTER dataset*. Accessed on 11.12.2019. URL: https://github.com/tu-fmaz/smarter_traces_field_test.

[53] *SOL source code*. Accessed on 11.12.2019. URL: https://github.com/tu-fmaz/sea_of_lights.

[54] *SIESTA source code*. Accessed on 11.12.2019. URL: https://github.com/tu-fmaz/siesta.

[55] Bluetooth SIG. *Bluetooth Mesh Profile Specification 1.0.1*. Accessed on 11.12.2019. 2017. URL: https://www.bluetooth.com/specifications/mesh-specifications.

[56] Bluetooth SIG. *Bluetooth Mesh Model Specification 1.0.1*. Accessed on 11.12.2019. 2017. URL: https://www.bluetooth.com/specifications/mesh-specifications.

[57] Louise K. Comfort and Thomas W. Haase. "Communication, Coherence, and Collective Action: The Impact of Hurricane Katrina on Communications Infrastructure." In: *Public Works management & policy* 10.4 (2006), pp. 328–343. DOI: 10.1177/1087724X06289052.

[58] Hannah Ritchie and Max Roser. *Natural Disasters - Empirical View*. Accessed on 11.12.2019. URL: https://ourworldindata.org/natural-disasters.

[59] Yan Ran. "Considerations and Suggestions on Improvement of Communication Network Disaster Countermeasures after the Wenchuan Earthquake." In: *Communications Magazine* 49.1 (2011), pp. 44–47. DOI: 10.1109/MCOM.2011.5681013.

[60] Fabio Ricciato, Angelo Coluccia, and Alessandro D'Alconzo. "A review of DoS attack models for 3G cellular networks from a system-design perspective." In: *Computer Communications* 33.5 (2010), pp. 551–558. DOI: 10.1016/j.comcom.2009.11.015.

[61] AL-Saraireh Ja'afer, Sufian Yousef, and Mohammad AL Nabhan. "Analysis and Enhancement of Authentication Algorithms in Mobile Networks." In: *Journal of Applied Sciences* 6.4 (2006), pp. 872–877. DOI: 10.3923/jas.2006.872.877.

[62] William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. "Exploiting Open Functionality in SMS-Capable Cellular Networks." In: *Proceedings of the 12th Conference on Computer and Communications Security*. ACM, 2005, pp. 393–404. DOI: 10.1145/1102120.1102171.

[63] *The status of the 2G/3G network sunset*. Accessed on 11.12.2019. URL: https://nae.global/en/the-status-of-the-2g-3g-network-sunset/.

[64] Yongsuk Park and Taejoon Park. "A Survey of Security Threats on 4G Networks." In: *Globecom Workshops*. IEEE. 2007, pp. 1–6. DOI: 10.1109/GLOCOMW.2007.4437813.

[65] Anastasios N Bikos and Nicolas Sklavos. "LTE/SAE Security Issues on 4G Wireless Networks." In: *Security & Privacy* 11.2 (2013), pp. 55–62. DOI: 10.1109/MSP.2012.136.

[66] Jin Cao, Maode Ma, Hui Li, Yueyu Zhang, and Zhenxing Luo. "A Survey on Security Aspects for LTE and LTE-A Networks." In: *Communications Surveys & Tutorials* 16.1 (2014), pp. 283–302. DOI: 10.1109/SURV.2013.041513.00174.

[67] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information." In: *26th Annual Network and Distributed System Security Symposium*. 2019. DOI: https://dx.doi.org/10.14722/ndss.2019.23442.

[68] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. "New Vulnerabilities in 4G and 5G Cellular Access Network Protocols: Exposing Device Capabilities." In: *12th Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2019, pp. 221–231. DOI: 10.1145/3317549.3319728.

[69] *Hong Kong Takes Symbolic Stand Against China's High-Tech Controls*. Accessed on 11.12.2019. URL: https://www.nytimes.com/2019/10/03/technology/hong-kong-china-tech-surveillance.html/.

[70] Washington (AFP). *10 countries cited for extreme media censorship: watchdog*. Accessed on 11.12.2019. URL: https://www.france24.com/en/20190910-10-countries-cited-for-extreme-media-censorship-watchdog.

[71] Sec Schneider. *Iridium System Hacking*. Accessed on 11.12.2019. 2015. URL: https://fahrplan.events.ccc.de/congress/2014/Fahrplan/system/attachments/2559/original/Iridium-Talk-Komplett.pdf.

[72] Santamarta Ruben. *A Wake-up Call for SATCOM Security*. Accessed on 11.12.2019. 2014. URL: https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf.

[73] Anne Nelson, Ivan Sigal, Dean Zambrano, and S John. *Media, Information Systems and Communities: Lessons from Haiti*. Accessed on 11.12.2019. 2010. URL: https://www.alnap.org/help-library/media-information-systems-and-communities-lessons-from-haiti.

[74] Dave Yates and Scott Paquette. "Emergency knowledge management and social media technologies: A case study of the 2010 Haitian earthquake." In: *International Journal of Information Management* 31.1 (2011), pp. 6–13. DOI: 10.1016/j.ijinfomgt.2010.10.001.

[75] Brett D.M. Peary, Rajib Shaw, and Yukiko Takeuchi. "Utilization of Social Media in the East Japan Earthquake and Tsunami and its Effectiveness." In: *Journal of Natural Disaster Science* 34.1 (2012), pp. 3–18. DOI: 10.2328/jnds.34.3.

[76] Fujio Toriumi, Takeshi Sakaki, Kosuke Shinoda, Kazuhiro Kazama, Satoshi Kurihara, and Itsuki Noda. "Information Sharing on Twitter During the 2011 Catastrophic Earthquake." In: *22Nd International Conference on World Wide Web*. ACM, 2013, pp. 1025–1028. DOI: 10.1145/2487788.2488110.

[77] Chi Zhang, Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang. "Privacy and Security for Online social Networks: Challenges and Opportunities." In: *IEEE Network* 24.4 (2010), pp. 13–18. DOI: 10.1109/MNET.2010.5510913.

[78] Homeland Security FEMA. *National Preparedness Report*. accessed: 17.11.2019. 2013. URL: https://www.fema.gov/media-library/assets/documents/32509.

[79] Scott Campbell. *Facebook Safety Check: Fury as users who aren't in Nepal mark themselves safe from quake*. Accessed on 11.12.2019. 2015. URL: http://www.express.co.uk/news/uk/576844/Facebook-Safety-Check-Nepal-earthquake-marked-declared-quake.

[80] ProteGear Far Out and Still Safe. *inReach (DeLorme)*. Accessed on 11.12.2019. 2016. URL: https://www.protegear.de/produkte-tarife/inreach-se/.

[81] Sandy Clark, Travis Goodspeed, Perry Metzger, Zachary Wasserman, Kevin Xu, and Matt Blaze. "Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System." In: *Proceedings of the 20th USENIX Security Symposium*. USENIX Association, 2011, pp. 8–12.

[82] Stephen Glass, Vallipuram Muthukkumarasamy, Marius Portmann, and Matthew Robert. "Insecurity in Public-Safety Communications: APCO Project 25." In: *Security and Privacy in Communication Networks*. Springer Berlin Heidelberg, 2011, pp. 116–133. DOI: 10.1007/978-3-642-31909-9_7.

[83] Martin Pfeiffer, Jan-Pascal Kwiotek, Jiska Classen, Robin Klose, and Matthias Hollick. "Analyzing TETRA Location Privacy and Network Availability." In: *6th Workshop on Security and Privacy in Smartphones and Mobile Devices*. ACM, 2016, pp. 117–122. DOI: 10.1145/2994459.2994463.

[84] A Kannammal and S Sujith Roy. "Survey on Secure Routing in Mobile Ad-hoc Networks." In: *International Conference on Advances in Human Machine Interaction*. IEEE. 2016, pp. 1–7. DOI: 10.1109/HMI.2016.7449197.

[85] *FreiFunk*. Accessed on 11.12.2019. URL: https://freifunk.net//en/.

[86] Tobias Hardes. "Performance analysis and simulation of a Freifunk Mesh network in Paderborn using B.A.T.M.A.N Advanced." Accessed on 11.12.2019. MA thesis. 2015. URL: http://thardes.de/wp-content/uploads/2016/03/thesis.pdf.

[87] *Commotion Wireless*. Accessed on 11.12.2019. URL: https://commotionwireless.net/.

[88] Paul Gardner-Stephen. *The Serval Project: Practical Wireless Ad-hoc Mobile Telecommunications*. Accessed on 11.12.2019. 2011. URL: http://developer.servalproject.org/files/CWN_Chapter_Serval.pdf.

[89] Paul Gardner-Stephen, Jeremy Lakeman, Romana Challans, Corey Wallis, Ariel Stulman, and Yoram Haddad. "MeshMS: Ad Hoc Data Transfer within Mesh Network." In: 5.8 (2012), pp. 496–504. DOI: 10.4236/ijcns.2012.58060.

[90] Paul Gardner-Stephen, Andrew Bettison, Romana Challans, and Jeremy Lakeman. "The Rational Behind The Serval Network Layer For Resilient Communications." In: *Journal of Computer Science* 9.12 (2013), p. 1680. DOI: 10.3844/jcssp.2013.1680.1685.

[91] Paul Gardner-Stephen, Romana Challans, Jeremy Lakeman, Andrew Bettison, Dione Gardner-Stephen, and Matthew Lloyd. "The Serval Mesh: A Platform for Resilient Communications in Disaster & Crisis." In: *Global Humanitarian Technology Conference*. IEEE. 2013, pp. 162–166. DOI: 10.1109/GHTC.2013.6713674.

[92] Roberto Di Pietro, Stefano Guarino, Nino V. Verde, and Josep Domingo-Ferrer. "Security in wireless ad-hoc networks – A survey." In: *Computer Communications* 51 (2014), pp. 1–20. DOI: 10.1016/j.comcom.2014.06.003.

[93] Christian Reuter and Marc-André Kaufhold. "Fifteen years of social media in emergencies: A retrospective review and future directions for crisis informatics." In: *Journal of Contingencies and Crisis Management* 26.1 (2018), pp. 41–57. DOI: doi.org/10.1111/1468-5973.12196.

[94] Yao-Nan. Lien, Hung-Chin Jang, and Tzu-Chieh Tsai. "A MANET Based Emergency Communication and Information System for Catastrophic Natural Disasters." In: *29th International Conference on Distributed Computing Systems Workshops*. IEEE, 2009, pp. 412–417. DOI: 10.1109/ICDCSW.2009.72.

[95] *Mobile App FEMA*. Accessed on 11.12.2019. URL: http://www.fema.gov/mobile-app.

[96] David Markenson and Laura Howe. "American Red Cross Digital Operations Center (DigiDOC): An Essential Emergency Management Tool for the Digital Age." In: *Disaster medicine and public health preparedness* 8.05 (2014), pp. 445–451. DOI: 10.1017/dmp.2014.102.

[97] *Red Cross Person Finder*. Accessed on 11.12.2019. URL: http://familylinks.icrc.org/en/Pages/home.aspx.

[98] *KATWARN*. Accessed on 11.12.2019. URL: https://www.katwarn.de/.

[99] *NINA*. Accessed on 11.12.2019. URL: http://www.bbk.bund.de/DE/NINA/Warn-App_NINA.html.

[100] Noriyuki Suzuki, Jane L. F. Zamora, Shigeru Kashihara, and Suguru Yamaguchi. "SOSCast: Location Estimation of Immobilized Persons through SOS Message Propagation." In: *Fourth International Conference on Intelligent Networking and Collaborative Systems*. IEEE, 2012, pp. 428–435. DOI: 10.1109/iNCoS.2012.101.

[101] Amro Al-Akkad, Leonardo Ramirez, Alexander Boden, Dave Randall, and Andreas Zimmermann. "Help Beacons: Design and Evaluation of an Ad-Hoc Lightweight S.O.S System for Smartphones." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2014, pp. 1485–1494. DOI: 10.1145/2556288.2557002.

[102] *INKA: Professional integration of volunteers in crisis management and disaster control*. Accessed on 11.12.2019. URL: https://www.sifo.de/de/inka-professionelle-integration-von-freiwilligen-helfern-in-krisenmanagement-und-1963.html.

[103] *ENSURE: ENablement of urban citizen SUpport for crisis REsponse*. Accessed on 11.12.2019. URL: https://www.sifo.de/de/ensure-verbesserte-krisenbewaeltigung-im-urbanen-raum-durch-situationsbezogene-2064.html.

[104] Amro Al-Akkad, Christian Raffelsberger, Alexander Boden, Leonardo Ramirez, and Andreas Zimmermann. "Tweeting 'When Online is Off'? Opportunistically Creating Mobile Ad-hoc Networks in Response to Disrupted Infrastructure." In: *Proceedings of the 11th International Conference on Information Systems for Crisis Response and Management*. ISCRAM Association, 2014.

[105] *Project Rescuer*. Accessed on 11.12.2019. URL: http://www.rescuer-project.org.

[106] *Project VR2Market*. Accessed on 11.12.2019. URL: http://vitalresponder.inesctec.pt/index.php/project/.

[107] *Project EmerGent*. Accessed on 11.12.2019. URL: http://www.fp7-emergent.eu.

[108] Matthew Zook, Mark Graham, Taylor Shelton, and Sean Gorman. "Volunteered Geographic Information and Crowdsourcing Disaster Relief: A Case Study of the Haitian Earthquake." In: *World Medical & Health Policy* 2.2 (2010), pp. 7–33. DOI: doi.org/10.2202/1948-4682.1069.

[109] Morten Wendelbo, Federica La China, Hannes Dekeyser, Leonardo Taccetti, Sebastiano Mori, Varun Aggarwal, Omar Alam, Ambra Savoldi, and Robert Zielonka. "The Crisis Response to the Nepal Earthquake: Lessons Learned." In: *European Institute for Asian Studies* (2016).

[110] Patricia Henriquez-Coronel, Daniel Barredo-Ibanez, and Juan-Pablo Trampuz. "The role of media and emotions in crisis communication due to natural disasters. An experimental study about Twitter, Facebook and ELCOMERCIO.com during the 2016 earthqueake in Ecuador." In: *Revista Internacional de Relaciones Publicas* 8.16 (2018), pp. 187–206. DOI: 10.5783/RIRP-16-2018-11-187-206.

[111] Jennifer Gray Briony. "Building resilience in Small Island Developing States: social media during the 2017 Atlantic hurricane season." In: (2018).

[112] *Spanish Version, Hurricane Maria Communications Status Report for Nov. 17*. Accessed on 11.12.2019. URL: https://www.fcc.gov/document/hurricane-maria-communications-status-report-nov-17/spanish-version.

[113] Joshua Whittaker, Katharine Haynes, John Handmer, and Jim McLennan. "Community safety during the 2009 Australian'Black Saturday'bushfires: an analysis of household preparedness and response." In: *International Journal of Wildland Fire* 22 (2013), pp. 841–849. DOI: doi.org/10.1071/WF12010.

[114] Mitchell Bingemann. *Telstra says it's ready for the next Black Saturday*. Accessed on 11.12.2019. URL: http://www.theaustralian.com.au/business/technology/telco-says-its-ready-for-the-next-black-saturday/news-story/f48e065f14fa8614f2a18165c9b279b8.

[115] The Washington Post Cleve R. Wootson Jr. *The deadliest, most destructive wildfire in California's history has finally been contained*. Accessed on 11.12.2019. URL: https://www.washingtonpost.com/nation/2018/11/25/camp-fire-deadliest-wildfire-californias-history-has-been-contained/.

[116] A Malcolm Gill and Scott L Stephens. "Scientific and social challenges for the management of fire-prone wildland–urban interfaces." In: *Environmental Research Letters* 4.3 (2009). DOI: doi.org/10.1088/1748-9326/4/3/034014.

[117] Emergency Telecommunications Cluster. *Current Emergencies – South Sudan*. Accessed on 11.12.2019. URL: https://www.etcluster.org/countries/south-sudan.

[118] Lidia Mayner and Paul Arbon. "Defining disaster: The need for harmonisation of terminology." In: *Australasian Journal of Disaster & Trauma Studies* 19 (2015), pp. 21–26.

[119] The United Nations. *Terminology on disaster risk reduction, from United Nations International Strategy for Disaster Reduction*. Accessed on 11.12.2019. 2009. URL: https://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf.

[120] Donald J Patterson. "Haitian resiliency: A case study in intermittent infrastructure." In: *First Monday* 20.8 (2015). DOI: dx.doi.org/10.5210/fm.v20i8.6129.

[121] Bluetooth Special Interest Group. *Bluetooth Core Specification*. Accessed on 11.12.2019. URL: https://www.bluetooth.com/specifications/bluetooth-core-specification/.

[122] Apple. *Multipeer Connectivity*. Accessed on 11.12.2019. URL: https://developer.apple.com/documentation/multipeerconnectivity.

[123] Wi-Fi Alliance. *Wi-Fi Peer-to-Peer (P2P) Technical Specification v1.7*. Accessed on 11.12.2019. URL: https://www.wi-fi.org/discover-wi-fi/specifications.

[124] IEEE Association. "IEEE Standard for Information technology — Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." In: *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)* (2016), pp. 1–3534. DOI: 10.1109/IEEESTD.2016.7786995.

[125] Wi-Fi Alliance. *Neighbor Awareness Networking Specification*. Accessed on 11.12.2019. URL: https://www.wi-fi.org/discover-wi-fi/specifications.

[126] Milan Stute, David Kreitschmann, and Matthias Hollick. "One Billion Apples' Secret Sauce: Recipe for the Apple Wireless Direct Link Ad Hoc Protocol." In: *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. ACM, 2018, pp. 529–543. DOI: 10.1145/3241539.3241566.

[127] Google. *Google Nearby*. Accessed on 11.12.2019. URL: https://developers.google.com/nearby/connections/overview.

[128] David M Hollis. *Cyberwar case study: Georgia 2008*. Accessed on 11.12.2019. 2011. URL: http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

[129] Susannah Rosenblatt and James Rainey. *Katrina Takes a Toll on Truth, News Accuracy*. Accessed on 11.12.2019. 2005. URL: http://articles.latimes.com/2005/sep/27/nation/na-rumors27.

[130] King wa Fu, Chung hong Chan, and Michael Chau. "Assessing Censorship on Microblogs in China: Discriminatory Keyword Analysis and the Real-Name Registration Policy." In: *Internet Computing* 17.3 (2013), pp. 42–50. DOI: 10.1109/MIC.2013.28.

[131] Huadong Ma, Dong Zhao, and Peiyan Yuan. "Opportunities in Mobile Crowd Sensing." In: *Communications Magazine* 52.8 (2014), pp. 29–35. DOI: 10.1109/MCOM.2014.6871666.

[132] Oscar D. Lara and Miguel A. Labrador. "A Survey on Human Activity Recognition using Wearable Sensors." In: *Communications Surveys & Tutorials* 15.3 (2013), pp. 1192–1209. DOI: 10.1109/SURV.2012.110112.00192.

[133] Konrad Szocik. "An Axiological Aspect of Terrorism: Remarks on Scott Atran's Perspective." In: *Journal of Applied Security Research* 11.2 (2016), pp. 111–123. DOI: 10.1080/19361610.2016.1137172.

[134] Tamba Isaac. "An Economic Analysis of Boko Haram's Activities in the Chad-Cameroon-Nigeria Border Area." In: *Journal of Economic & Financial Studies* 3.01 (2015), pp. 24–29. DOI: 10.18533/jefs.v3i01.98.

[135] Pacific Disaster Center. *Disaster Alert*. Accessed on 11.12.2019. URL: http://www.pdc.org/solutions/tools.

[136] Nils Aschenbruck, Elmar Gerhards-Padilla, Michael Gerharz, Matthias Frank, and Peter Martini. "Modelling Mobility in Disaster Area Scenarios." In: *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems*. ACM. 2007, pp. 4–12. DOI: 10.1145/1298126.1298131.

[137] Sergio Cabrero, Roberto García, Xabiel G. Pañeda, and David Melendi. "Understanding Opportunistic Networking for Emergency Services: Analysis of One Year of GPS Traces." In: *Proceedings of the 10th Workshop on Challenged Networks*. ACM. 2015, pp. 31–36. DOI: 10.1145/2799371.2799381.

[138] Milan Stute, Max Maass, Tom Schons, and Matthias Hollick. "Reverse Engineering Human Mobility in Large-scale Natural Disasters." In: *Proceedings of the 20th International Conference on Modelling, Analysis and Simulation of Wireless and Mobile Systems*. ACM, 2017, pp. 219–226. DOI: 10.1145/3127540.3127542.

[139] Michael Doering, Sven Lahde, Johannes Morgenroth, and Lars Wolf. "IBR-DTN: An Efficient Implementation for Embedded Systems." In: *Proceedings of the Third Workshop on Challenged Networks*. ACM, 2008, pp. 117–120. DOI: 10.1145/1409985.1410008.

[140] Johannes Morgenroth, Sebastian Schildt, and Lars C Wolf. "A Bundle Protocol Implementation for Android Devices." In: *Proceedings of the 18th International Conference on Mobile Computing and Networking*. ACM, 2012, pp. 443–446. DOI: 10.1145/2348543.2348606.

[141] Patrick Lieser, Alaa Alhamoud, Hosam Nima, Björn Richerzhagen, Sanja Huhle, Doreen Böhnstedt, and Ralf Steinmetz. "Situation Detection based on Activity Recognition in Disaster Scenarios." In: *Proceedings of the 15th International Conference on Information Systems for Crisis Response and Management* (2018).

[142] Duncan J Watts and Steven H Strogatz. "Collective dynamics of 'small-world' networks." In: *Nature* 393.6684 (1998), pp. 440–442. DOI: 10.1038/30918.

[143] Samuel C. Nelson, Albert F. Harris III, and Robin Kravets. "Event-driven, Role-based Mobility in Disaster Recovery Networks." In: *Proceedings of the second Workshop on Challenged Networks*. ACM. 2007, pp. 27–34. DOI: 10.1145/1287791.1287798.

[144] Md Yusuf S. Uddin, David M. Nicol, Tarek F. Abdelzaher, and Robin H. Kravets. "A Post-Disaster Mobility Model for Delay Tolerant Networking." In: *Proceedings of the Winter Simulation Conference*. IEEE. 2009, pp. 2785–2796. DOI: 10.1109/WSC.2009.5429249.

[145] Alma Whitten and J. D. Tygar. "Why Johnny can't encrypt: A usability evaluation of PGP 5.0." In: *USENIX Security Symposium*. Vol. 348. 1999, pp. 169–184.

[146] Danny Dolev and Andrew C. Yao. "On the security of public key protocols." In: *Transactions on Information Theory* 29.2 (1983), pp. 198–208. DOI: 10.1109/TIT.1983.1056650.

[147] Kannan Govindan and Prasant Mohapatra. "Trust computations and trust dynamics in mobile adhoc networks: A survey." In: *Communications Surveys & Tutorials* 14.2 (2011), pp. 279–298. DOI: 10.1109/SURV.2011.042711.00083.

[148] Mikhail Fomichev, Flor Álvarez, Daniel Steinmetzer, Paul Gardner Stephen, and Matthias Hollick. "Survey and Systematization of Secure Device Pairing." In: *Communications Surveys & Tutorials* 20.1 (2017), pp. 517–550. DOI: 10.1109/COMST.2017.2748278.

[149] Al-Sakib Khan Pathan. *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016. ISBN: 978-1-4398-1920-3.

[150] *ZXing Project*. Accessed on 11.12.2019. URL: https://github.com/zxing/zxing.

[151] *SEEK for Android*. Accessed on 11.12.2019. URL: https://seek-for-android.github.io/.

[152] *YubiKey*. Accessed on 11.12.2019. URL: https://www.yubico.com/.

[153] Rounak Sinha, Hemant Kumar Srivastava, and Sumita Gupta. "Performance Based Comparison Study of RSA and Elliptic Curve Cryptography." In: *International Journal of Scientific & Engineering Research* 4.5 (2013), pp. 720–725.

[154] Sonja Buchegger and Jean-Yves Le Boudec. "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks." In: *Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing*. IEEE, 2002, pp. 403–410. DOI: 10.1109/EMPDP.2002.994321.

[155] Elhadi. Shakshuki, Nan Kang, and Tarek Sheltami. "EAACK — A Secure Intrusion-Detection System for MANETs." In: *Transactions on Industrial Electronics* 60.3 (2013). DOI: 10.1109/TIE.2012.2196010.

[156] Adnan Nadeem and Michael P. Howarth. "An intrusion detection & adaptive response mechanism for MANETs." In: *Ad Hoc Networks* 13 (2014), pp. 368–380. DOI: 10.1016/j.adhoc.2013.08.017.

[157] Jan Seedorf, Dirk Kutscher, and Fabian Schneider. "Decentralised Binding of Self-Certifying Names to Real-World Identities for Assessment of Third-Party Messages in Fragmented Mobile Networks." In: *Conference on Computer Communications Workshops*. IEEE, 2014, pp. 416–421. DOI: 10.1109/INFCOMW.2014.6849268.

[158] Michael Farb, Yue-Hsun Lin, Tiffany Hyun-Jin Kim, Jonathan McCune, and Adrian Perrig. "Safeslinger: Easy-to-Use and Secure Public-Key Exchange." In: *Proceedings of the 19th International Conference on Mobile Computing and Networking*. ACM, 2013, pp. 417–428. DOI: 10.1145/2500423.2500428.

[159] Wenlong Shen, Weisheng Hong, Xianghui Cao, Bo Yin, Devu M. Shila, and Yu Cheng. "Secure Key Establishment for Device-to-Device Communications." In: *Global Communications Conference*. IEEE, 2014, pp. 336–340. DOI: 10.1109/GLOCOM.2014.7036830.

[160] Christoph Busold, Ahmed Taha, Christian Wachsmann, Alexandra Dmitrienko, Hervé Seudié, Majid Sobhani, and Ahmad-Reza Sadeghi. "Smart Keys for Cyber-Cars: Secure Smartphone-based NFC-enabled Car Immobilizer." In: *Proceedings of the Third Conference on Data and Application Security and Privacy*. ACM, 2013, pp. 233–242. DOI: 10.1145/2435349.2435382.

[161] Srdjan Capkun, Jean-Pierre Hubaux, and Levente Buttyan. "Mobility Helps Peer-to-Peer Security." In: *Transactions on Mobile Computing* 5.1 (2006), pp. 43–51. DOI: 10.1109/TMC.2006.12.

[162] Mario Cagalj, Srdjan Capkun, and Jean-Pierre Hubaux. "Key Agreement in Peer-to-Peer Wireless Networks." In: *Proceedings of the IEEE* 94.2 (2006), pp. 467–478. DOI: 10.1109/JPROC.2005.862475.

[163] Wei Sun, Zheng Yang, Xinglin Zhang, and Yunhao Liu. "Energy-efficient neighbor discovery in mobile ad hoc and wireless sensor networks: A survey." In: *Communications Surveys & Tutorials* 16.3 (2014), pp. 1448–1459. DOI: 10.1109/SURV.2013.012414.00164.

[164] Teemu Kärkkäinen, Mika Välimaa, Esa Hyytiä, and Jörg Ott. "Opportunistic Content Dissemination Performance in Dense Network Segments." In: *Proceedings of the 11th Workshop on Challenged Networks*. ACM, 2016, pp. 1–6. DOI: 10.1145/2979683.2979692.

[165] Teemu Kärkkäinen, Mika Välimaa, Shourov K. Roy, Esa Hyytiä, and Jörg Ott. "Practical opportunistic content dissemination performance in dense network segments." In: *Computer Communications* 123 (2018), pp. 65–80. DOI: 10.1016/j.comcom.2018.03.013.

[166] Mario Conti, Chiara Boldrini, Salil S. Kanhere, Enzo Mingozzi, Elena Pagani, Pedro M. Ruiz, and Mohamed Younis. "From MANET to people-centric networking: Milestones and open research challenges." In: *Computer Communications* 71.C (2015), pp. 1–21. DOI: 10.1016/j.comcom.2015.09.007.

[167] GSMA Intelligence. *Rural coverage: strategies for sustainability*. accessed: 17.11.2019. 2015. URL: https://www.gsmaintelligence.com/research/.

[168] Jihun Seo, Keuchul Cho, Wooseong Cho, Gisu Park, and Kijun Han. "A discovery scheme based on carrier sensing in self-organizing Bluetooth Low Energy networks." In: *Journal of Network and Computer Applications* 65.C (2016), pp. 72–83. DOI: 10.1016/j.jnca.2015.09.015.

[169] Huan Zhou, Huanyang Zheng, Jie Wu, and Jiming Chen. "Energy-Efficient Contact Probing in Opportunistic Mobile Networks." In: *22nd International Conference on Computer Communication and Networks*. IEEE, 2013, pp. 1–7. DOI: 10.1109/ICCCN.2013.6614135.

[170] A. Troël. "Prise en compte de la mobilité dans les interactions de proximité entre terminaux à profils hétérogènes." PhD thesis. Rennes 1, 2004.

[171] Briar Project. *Secure messaging, anywhere*. Accessed on 11.12.2019. 2018. URL: https://briarproject.org/.

[172] Kyu-Han Kim, Alexander W Min, Dhruv Gupta, Prasant Mohapatra, and Jatinder Pal Singh. "Improving energy efficiency of Wi-Fi sensing on smartphones." In: *INFOCOM*. IEEE. 2011, pp. 2930–2938. DOI: 10.1109/INFCOM.2011.5935133.

[173] Catalin Drula, Cristiana Amza, Franck Rousseau, and Andrzej Duda. "Adaptive energy conserving algorithms for neighbor discovery in opportunistic bluetooth networks." In: *Journal on Selected Areas in Communications* 25.1 (2007), pp. 96–107. DOI: 10.1109/JSAC.2007.070110.

[174] Wei Wang, Vikram Srinivasan, and Mehul Motani. "Adaptive Contact Probing Mechanisms for Delay Tolerant Applications." In: *13th Annual International Conference on Mobile Computing and Networking*. ACM, 2007, pp. 230–241. DOI: 10.1145/1287853.1287882.

[175] Hiroki Nishiyama, Masaya Ito, and Nei Kato. "Relay-by-Smartphone: Realizing Multihop Device-to-Device Communications." In: *Communications Magazine* 52.4 (2014), pp. 56–65. DOI: 10.1109/MCOM.2014.6807947.

[176] Trevor Pering, Yuvraj Agarwal, Rajesh Gupta, and Roy Want. "CoolSpots: Reducing the Power Consumption of Wireless Mobile Devices with Multiple Radio Interfaces." In: *4th International Conference on Mobile Systems, Applications and Services*. ACM, 2006, pp. 220–232. DOI: 10.1145/1134680.1134704.

[177] Vangelis Gazis. "A Survey of Standards for Machine-to-Machine and the Internet of Things." In: *Communications Surveys & Tutorials* 19.1 (2017), pp. 482–511. DOI: 10.1109/COMST.2016.2592948.

[178] Terence K.L. Hui, R. Simon Sherratt, and Daniel D. Sánchez. "Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies." In: *Future Generation Computer Systems* 76 (2017), pp. 358–369. DOI: 10.1016/j.future.2016.10.026.

[179] Iman Khajenasiri, Abouzar Estebsari, Marian Verhelst, and Georges Gielen. "A Review on Internet of Things Solutions for Intelligent Energy Control in Buildings for Smart City Applications." In: *Energy Procedia* 111 (2017), pp. 770–779. DOI: 10.1016/j.egypro.2017.03.239.

[180] Timothy Malche and Priti Maheshwary. "Internet of Things (IoT) for building Smart Home System." In: *International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*. IEEE, 2017, pp. 65–70. DOI: 10.1109/I-SMAC.2017.8058258.

[181] Sergio Munoz, Antonio F. Llamas, Miguel Coronado, and Carlos A. Iglesias. "Smart Office Automation Based on Semantic Event-Driven Rules." In: *5th International Workshop on Smart Offices and Other Workshops*. IOS Press BV, 2016, p. 3. DOI: 10.3233/978-1-61499-690-3-3.

[182] M. Narayana Murthy and P. AjaySaiKiran. "A Smart Office Automation System Using Raspberry Pi (Model-B)." In: *International Conference on Current Trends towards Converging Technologies*. IEEE. 2018, pp. 1–5. DOI: 10.1109/ICCTCT.2018.8550894.

[183] Mario Collotta, Giovanni Pau, Timothy Talty, and Ozan K. Tonguz. "Bluetooth 5: A Concrete Step Forward toward the IoT." In: *Communications Magazine* 56.7 (2018), pp. 125–131. DOI: 10.1109/MCOM.2018.1700053.

[184] Ruuvi Innovations Ltd (Oy). *Ruuvitag*. Accessed on 11.12.2019. URL: https://ruuvi.com/ruuvitag-specs/.

[185] Nordic Semiconductor. *nRF52840 Dongle*. Accessed on 11.12.2019. URL: https://www.nordicsemi.com/Software-and-Tools/Development-Kits/nRF52840-Dongle.

[186] Raspberry Pi Foundation. *Raspberry Pi 3 Model B+*. Accessed on 11.12.2019. URL: https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/.

[187] Nordic Semiconductor. *nRF5 Series SoCs*. Accessed on 11.12.2019. URL: https://www.nordicsemi.com/Software-and-Tools/Software/nRF5-SDK.

[188] Nordic Semiconductor. *Nordic nRF5-SDK for Mesh*. Accessed on 11.12.2019. URL: https://www.nordicsemi.com/Software-and-Tools/Software/nRF5-SDK-for-Mesh.

[189] Nordic Semiconductor. *Android nrF Mesh Library*. Accessed on 11.12.2019. URL: https://github.com/NordicSemiconductor/Android-nRF-Mesh-Library.

[190] Otso Jousimaa Ruuvi Innovations. *Git Repository Ruuvi Blog*. Accessed on 11.12.2019. URL: https://github.com/ruuvi/ruuvi.firmware.c/tree/ruuviblog.

[191] *Release of BlueZ 5.50*. Accessed on 11.12.2019. 2019. URL: http://www.bluez.org/release-of-bluez-5-50/.

[192] Caril Martínez, Leonardo Eras, and Federico Domínguez. "The Smart Doorbell: A proof-of-concept Implementation of a Bluetooth Mesh Network." In: *Third Ecuador Technical Chapters Meeting (ETCM)*. IEEE. 2018, pp. 1–5. DOI: 10.1109/ETCM.2018.8580325.

[193] Qing Wan and Jianghua Liu. "Smart-Home Architecture Based on Bluetooth mesh Technology." In: 322.7 (2018), p. 072004. DOI: 10.1088/1757-899x/322/7/072004.

[194] Adonay A. Veiga and Claudia J. B. Abbas. "Proposal and Application of Bluetooth Mesh Profile for Smart Cities' Services." In: *Smart Cities* 2.1 (2019), pp. 1–19. DOI: 10.3390/smartcities2010001.

[195] Himanshu Verma and Naveen Chauhan. "MANET Based Emergency Communication System for Natural Disasters." In: *International Conference on Computing, Communication & Automation*. IEEE. 2015, pp. 480–485. DOI: 10.1109/CCAA.2015.7148424.

[196] Mengmeng Ge, Kim-Kwang R. Choo, Huai Wu, and Yong Yu. "Survey on key revocation mechanisms in wireless sensor networks." In: *Journal of Network and Computer Applications* 63 (2016), pp. 24–38. DOI: 10.1016/j.jnca.2016.01.012.

AUTHOR'S PUBLICATIONS

CONFERENCE PAPERS

[1] Flor Álvarez, Matthias Hollick, and Paul Gardner-Stephen. "Maintaining both Availability and Integrity of Communications: Challenges and Guidelines for Data Security and Privacy During Disasters and Crises." In: *Global Humanitarian Technology Conference (GHTC)*. IEEE. 2016, pp. 62–70. DOI: 10.1109/GHTC.2016.7857261.

[2] Patrick Lieser, Flor Álvarez, Paul Gardner-Stephen, Matthias Hollick, and Doreen Boehnstedt. "Architecture for Responsive Emergency Communications Networks." In: *Global Humanitarian Technology Conference (GHTC)*. IEEE. 2017, pp. 1–9. DOI: 10.1109/GHTC.2017.8239239.

[3] Flor Álvarez, Max Kolhagen, and Matthias Hollick. "Sea of Lights: Practical Device-to-Device Security Bootstrapping in the Dark." In: *43rd Conference on Local Computer Networks (LCN)*. IEEE. 2018, pp. 124–132. DOI: 10.1109/LCN.2018.8638102.

[4] Lars Almon, Flor Álvarez, Laurenz Kamp, and Matthias Hollick. "The King is Dead Long Live the King! Towards Systematic Performance Evaluation of Heterogeneous Bluetooth Mesh Networks in Real World Environments." In: *44th Conference on Local Computer Networks (LCN)*. IEEE. 2019, pp. 124–132.

[5] Flor Álvarez, Lars Almon, Hauke Radtki, and Matthias Hollick. "Bluemergency: Mediating Post-disaster Communication Systems using the Internet of Things and Bluetooth Mesh." In: *Global Humanitarian Technology Conference (GHTC)*. IEEE. 2019, pp. 62–70.

WORKSHOP PAPERS

[1] Flor Álvarez, Lars Almon, Patrick Lieser, Tobias Meuser, Yannick Dylla, Björn Richerzhagen, Matthias Hollick, and Ralf Steinmetz. "Conducting a Large-scale Field Test of a Smartphone-based Communication Network for Emergency Response." In: *Proceedings of the 13th Workshop on Challenged Networks*. ACM, 2018, pp. 3–10. DOI: 10.1145/3264844.3264845.

[2] Flor Álvarez, Lars Almon, Ann-Sophie Hahn, and Matthias Hollick. "Toxic Friends in Your Network: Breaking the Bluetooth Mesh Friendship Concept." In: *5th Security Standardisation Research Workshop (SSR)*. ACM. 2019, pp. 1–12. DOI: 10.1145/3338500.3360334.

JOURNAL ARTICLES AND BOOK CHAPTERS

[1] Mikhail Fomichev, Flor Álvarez, Daniel Steinmetzer, Paul Gardner Stephen, and Matthias Hollick. "Survey and Systematization of Secure Device Pairing." In: *IEEE Communications Surveys & Tutorials* 20.1 (2017), pp. 517–550. DOI: 10.1109/COMST.2017.2748278.

[2] Lars Almon, Flor Álvarez, Patrick Lieser, Tobias Meuser, and Fabian Schaller. "Ad-Hoc-Kommunikation – Gesellschaftlich wünschenswert, rechtlich ungeregelt." In: *Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung*. Ed. by Alexander Roßnagel, Michael Friedewald, and Marit Hansen. Springer Fachmedien Wiesbaden, 2018, pp. 77–98. ISBN: 978-3-658-23727-1.

UNDER PEER REVIEW

[1] Flor Álvarez, Tobias Schultes, and Matthias Hollick. "SIESTA: Smart Neighbor Discovery for Device-to-device Communications." In: *International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. (Submitted). IEEE. 2020.

ERKLÄRUNG ZUR DISSERTATIONSSCHRIFT

gemäß § 9 der Allgemeinen Bestimmungen der Promotionsordnung der Technische Universität Darmstadt vom 12. Januar 1990 (ABI. 1990, S. 658) in der Fassung der 8. Novelle vom 1. März 2018

Hiermit versichere ich, Flor María Álvarez Zurita, die vorliegende Dissertationsschrift ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Eigenzitate aus vorausgehenden wissenschaftlichen Veröffentlichungen werden in Anlehnung an die Hinweise des Promotionsausschusses Fachbereich Informatik zum Thema „Eigenzitate in wissenschaftlichen Arbeiten“ (EZ-2014/10) in Kapitel „*Previously Published Material*“ auf Seiten xix bis xx gelistet. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen. In der abgegebenen Dissertationsschrift stimmen die schriftliche und die elektronische Fassung überein.

Darmstadt, 20. Dezember 2019

Flor María Álvarez Zurita