Dipl.-Ing. Christian Raffelsberger, Bakk-techn.

ANALYZING AND IMPROVING WIRELESS NETWORKING PROTOCOLS AND SERVICES FOR EMERGENCY RESPONSE SCENARIOS

DISSERTATION

submitted in fulfillment of the requirements for the degree of
Doktor der technischen Wissenschaften

Alpen-Adria-Universität Klagenfurt
Fakultät für Technische Wissenschaften

Advisor/1st Evaluator
Univ.-Prof. Dipl.-Ing. Dr. Hermann Hellwagner
Alpen-Adria-Universität Klagenfurt
Institut für Informationstechnologie

2nd Evaluator
Prof. Dr. Lionel Brunie
Institut National des Sciences Appliquées de Lyon
Laboratoire d'Informatique de l'Image et des Systèmes d'Information

Klagenfurt, July 2015

Affidavit

I hereby declare in lieu of an oath that

- the submitted academic paper is entirely my own work and that no auxiliary materials have been used other than those indicated;
- I have fully disclosed all assistance received from third parties during the process of writing the paper, including any significant advice from supervisors;
- any contents taken from the works of third parties or my own works that have been included either literally or in spirit have been appropriately marked and the respective source of the information has been clearly identified with precise bibliographical references (e.g. in footnotes);
- to date, I have not submitted this paper to an examining authority either in Austria or abroad and that
- the digital version of the paper submitted for the purpose of plagiarism assessment is fully consistent with the printed version.

I am aware that a declaration contrary to the facts will have legal consequences.

Signature:

Klagenfurt, 23 July 2015

Acknowledgments

I would like to thank my supervisor Prof. Hermann Hellwagner for giving me the opportunity to work at ITEC and his constant support and guidance throughout this thesis. I would also like to thank Prof. Lionel Brunie for his willingness to act as a reviewer and his feedback concerning this work.

I would also like to thank my colleagues from ITEC. It has been a pleasure to be part of this team and I really appreciate the support that I have received from all of you. In particular, I would like to express my gratitude to my office mate Benjamin Rainer for his support with the DASH encoder and all the discussions that helped to improve my work.

I would like to thank all partners from the BRIDGE project. I would like to point out Amro Al-Akkad for the great collaboration within BRIDGE, which resulted in several publications and successful demonstrations in the course of the project. I would also like to thank Daniela Pohl for her support in many project matters.

Last but definitely not least, I would like to deeply thank my family. My wife for always being there for me, for her patience and for motivating me to stick to my goals. I would also like to thank my son for helping me to remember what the most important things are in life.

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no 261817, the BRIDGE project (www.bridgeproject.eu), and was partly performed in the Lakeside Labs research cluster at Alpen-Adria-Universität Klagenfurt.

Abstract

Emergency response operations are highly collaborative efforts that usually involve different first responder organizations. Establishing and maintaining communication as well as disseminating information are critical and complex tasks in such operations, in order to allow the involved organizations to effectively cope with the situation at hand. Since fixed communication infrastructures may be destroyed or overloaded in the course of a disaster, wireless mobile ad-hoc networks (MANETs) are a promising solution to provide the means to communicate and manage information at a disaster scene. Most existing MANET routing protocols assume that an end-to-end path between source and destination can be established. However, this assumption may not hold in networks established during emergency responses. In particular, the wireless networks may provide diverse connectivity characteristics which imposes some challenges, especially on routing. Routing protocols need to take transmission errors, node failures and even the partitioning of the network into account.

This thesis aims to improve wireless networking for emergency response scenarios by proposing to use routing algorithms that provide mechanisms from delay-/disruption-tolerant networking (DTN) in order to cope with network disruptions, but at the same time are as efficient as MANET routing protocols in connected parts of the network. We make several contributions to achieve this goal. First, we describe how to model emergency response operations in a realistic way and analyze the specifics of such scenarios in terms of wireless connectivity. Based on the analysis of two realistic emergency response scenarios, it can be stated that networks offer diverse connectivity characteristics. In particular, in some parts of a disaster area the connectivity between first responders is good whereas other parts are not well connected. We show shortcomings of existing routing protocols from the MANET and the DTN domains and that a combination of these two approaches is beneficial in emergency response scenarios. In particular, we propose two routing algorithms that apply DTN mechanisms on top of MANET routing in order to cope with disruptions of the network. The algorithms are evaluated in different simulation-based experiments and compared with existing MANET and DTN routing protocols. The evaluation results show that the combined schemes provide a good tradeoff between delivery ratio and resource usage. Furthermore, we show that the combined approaches are applicable to a wide range of scenarios, from low to well-connected networks. For instance, in partitioned networks the combined approaches offer packet delivery ratios similar to state-of-the-art DTN routing schemes while using less resources concerning bandwidth and storage. Additionally, we propose a multimedia delivery system that provides another means of communication in emergency response scenarios. The design of the system takes the aforementioned challenges, such as network disruptions into account and also the specific requirements of the emergency response domain. In particular, we have selected HTTP Adaptive Streaming (HAS) for multimedia delivery but use a modified version of HTTP that supports data delivery despite network disruptions. Results from a simulation-based evaluation in a chemical incident scenario show that the multimedia delivery system can deliver videos with a high probability and acceptable delays, even in networks that offer low connectivity, especially in combination with the aforementioned combined MANET/DTN routing approaches.

Contents

CHAPTER 1 Introduction

In recent years, the usage of small, portable computing devices, such as smartphones or tablets, has dramatically increased around the world. Many people use mobile devices to access the Internet in order to consume services such as social networks, multimedia streaming, navigation or email, and to perform other tasks which have been previously performed mainly via fixed personal computers. This type of use is also referred to as *mobile computing*. The improvements of mobile devices and wireless communication technologies have made it possible that mobile computing is nowadays integrated into many people's everyday life. Similarly, mobile computing has also found its way into the public safety and disaster response domains, respectively it has the potential to improve future public safety and disaster response efforts. For instance, people who are affected by a natural disaster such as a hurricane or earthquake, may use social networks to inform relatives and friends of their well-being or to get information about where to get medical support. As a consequence, emergency response organizations have started to use social networks, either for getting information from affected people, or to inform them about the ongoing response [52, 70, 95, 118]. Additionally, mobile computing has the potential to support first responders on the incident scene by providing communication services that complement traditional radio communication. For instance, there are several examples that show how mobile computing applications can support the work of firefighters [23, 58, 80].

Public safety and emergency response scenarios are very promising application domains for wireless networks. One of the most important demands in an emergency response operation is a working communication network. Usually, disaster operations are led from a local control post that is located near the incident site. The incident commander that is located at the local command post has to get an overview of the disaster situation and available resources. Furthermore, the incident commander has to give tasks to other teams of different first responder organizations on the field. Thus, several first responder organizations need to collaborate in order to effectively cope with the disaster situation at hand. However, communication networks for emergency response operations have to operate in harsh environments. Existing fixed infrastructures such as cellular networks may be unavailable since they got destroyed by the disaster itself or get overloaded in the aftermath of the disaster. Thus, first responders may greatly benefit from wireless networks that are deployed at the incident scene, or opportunistic networks that are formed by devices carried by first responders. In particular, today's mobile devices (such as smartphones or tablets) offer ad-hoc communication interfaces (e.g., Bluetooth or Wi-Fi) and also provide the computing resources to perform complex tasks.

As mentioned before, emergency response scenarios could greatly benefit from ad-hoc wireless networks. On the other hand, this application domain is very challenging for networking. First responders, carrying devices that are connected via ad-hoc networks, are usually mobile which causes constant changes in the network topology. This means that new wireless links are established, existing links break and the quality of wireless links constantly changes due to the mobility of nodes. Obstacles that are present on the disaster scene have similar effects on the wireless network, since they may attenuate or completely block wireless signals which also affects the topology of the network. Such dynamic networks that are formed in the case of emergencies are also referred to as hastily formed networks [41]. Concerning the technical dimension, one challenge of hastily formed networks for emergency response is that the networks may get partitioned. A partitioned network does not provide end-to-end paths between all devices that are connected to the network. However, many traditional routing and transport protocols for mobile ad-hoc networks (MANETs) make the assumption that end-to-end connectivity can always be established. Thus, these protocols may not be able to provide communication in partitioned networks. As a result, new communication paradigms have been designed that do not make any assumptions about end-to-end connectivity. In particular, delay-/disruption-tolerant networking (DTN) addresses environments where continuous end-to-end connectivity is not available. However, DTN routing protocols often assume that the network is very sparse and consequently contacts between nodes are very rare. Thus, many protocols use replication to increase the chance that data can be delivered. On the other hand, replication reduces the performance in dense networks because it may cause network congestion.

We believe that routing protocols for emergency scenarios need to be able to work well in a broad range of networking scenarios, ranging from well-connected scenarios to sparse scenarios. Similarly, routing protocols need to be able to efficiently work in networks where some parts are well connected, whereas other parts are only intermittently connected. Thus, hybrid protocols that combine end-to-end routing and DTN routing may be necessary to route data in emergency scenarios.

The overall goal of this thesis is to improve mobile wireless networks that are used in emergency response scenarios. Hence, an important goal of this thesis is to analyze the specific challenges that are imposed by this application domain and to create routing algorithms or application level services that can cope with these challenges. Our research objectives in this context are described in the next section in more detail.

1.1 Research Objectives

The main goal of this thesis is to improve wireless networks and services that use these networks in emergency response operations. In order to achieve this goal, this thesis first analyzes existing wireless technologies that could be potentially used in the emergency response domain. In order to evaluate the performance of wireless technologies, an important task is to analyze the specifics of emergency response scenarios and to model these scenarios in a realistic way. Modeling is a very important tool since the nature of a disaster makes it hard to evaluate technologies under real-world settings. In particular, in an ongoing disaster situation, first responders will only use well-established and tested technologies that they have been trained with beforehand. Based on the modeled emergency scenarios, we develop and evaluate new routing protocols that are more suitable than current state-of-the-art routing algorithms. However, besides the network level there are also requirements towards new application level services that improve the work of first responders. In particular, we present a multimedia delivery system that can be used in emergency response scenarios that are prone to disruptions. The system allows first responders to exchange multimedia data despite the lack of end-to-end paths, which is not supported by current multimedia systems which usually assume end-to-end connectivity between the multimedia source and its consumers.

The research objectives of this thesis are:

- to analyze the specifics of emergency response scenarios and model them in a realistic way;

- to evaluate the performance of state-of-the-art routing protocols in emergency response scenarios;
- to analyze strengths and weaknesses of state-of-the-art routing protocols in such scenarios;
- to develop routing protocols that are better suited for communication in emergency scenarios and hence outperform state-of-the-art approaches in such scenarios;
- to evaluate the developed routing protocols in realistic emergency response scenarios;
- to design and develop a multimedia delivery system that provides another means of communication for emergency response scenarios; and
- to evaluate the multimedia system in realistic emergency response scenarios.

1.2 Outline of this Work

Chapter 2 describes the technical background that is relevant for this thesis. In particular, it describes several wireless technologies that are suitable for disaster situations. Additionally, it introduces two different networking approaches, namely mobile ad-hoc networks (MANETs) and delay-/disruption-tolerant networking (DTN). Afterwards, Chapter 2 introduces a research project called BRIDGE which aims to improve the interoperability of first responders in large-scale emergency management. In particular, the networking architecture that has been developed within that project is described. This network architecture provides the context for some concepts of this thesis. Finally, models for creating realistic emergency response scenarios are described.

Chapter 3 describes how to model realistic emergency response scenarios. First, the modeling framework is introduced. Afterwards, two concrete scenarios are modeled. The first scenario describes an emergency response after an incident in a chemical facility. The second scenario models a real-world full-scale exercise. For both scenarios, we analyze the connectivity characteristics of the resulting wireless networks. Additionally, an evaluation of several state-of-the-art MANET routing protocols is performed in order to show the capabilities and limits of this type of routing in emergency response scenarios.

Chapter 4 describes approaches that combine MANET and DTN routing to tackle the challenging networking environment of emergency response scenarios. The chapter first gives an overview and classification of existing approaches. Afterwards, it introduces two approaches that we developed in the course of this thesis. Both approaches assume that a MANET routing protocol is used to retrieve information about the current state of the network and combine this protocol with DTN mechanisms to cope with disruptions. The first approach provides packet buffering on top of MANET routing in order to bridge temporary disruptions of the network. The second approach enhances the first approach by providing a mechanism to bridge permanent partitions by opportunistically selecting relay nodes, based on information collected by the MANET routing protocol.

Chapter 5 includes simulation-based evaluation studies of the aforementioned combined MANET/DTN approaches and a comparison with existing MANET and DTN routing algorithms. Additionally, it presents an evaluation in a generic scenario that shows that these approaches may also be useful in other domains, where wireless networks are diverse in terms of connectivity.

Chapter 6 describes a multimedia delivery system for emergency response scenarios that can cope with disruptions of the network. The multimedia delivery system is also an application domain for the routing algorithms that have been presented in Chapter 4. The delivery is based on MPEG Dynamic Adaptive Streaming over HTTP (MPEG-DASH) but uses a modified version of HTTP that supports delivery despite network partitioning. Furthermore, the chapter presents evaluation results of the system in the aforementioned chemical incident scenario and also describes a prototype implementation for Android devices.

Finally, Chapter 7 concludes the thesis and discusses open issues and possible future work.

CHAPTER 2

Background

This chapter presents the technical background for the main topics of this thesis. First, Section 2.1 gives an overview of wireless communication standards for different types of wireless networks that may be used in the context of emergency response scenarios. Afterwards, Section 2.2 introduces the end-to-end routing concept that is usually used in mobile ad-hoc networks and state-of-the-art protocols that follow this approach. Section 2.3 introduces the concept of delay-/disruption-tolerant networking (DTN) and state-of-the-art routing protocols that follow this concept. DTN routing is an alternative routing approach to end-to-end routing. Section 2.4 presents different types of networking architectures for emergency response scenarios. Furthermore, it presents the network architecture that has been developed in the course of the BRIDGE project to provide telecommunication services in disaster scenarios. Finally, Section 2.5 gives on overview of existing state-of-the-art approaches in terms of mobility and wireless modeling.

2.1 Wireless Communication Standards

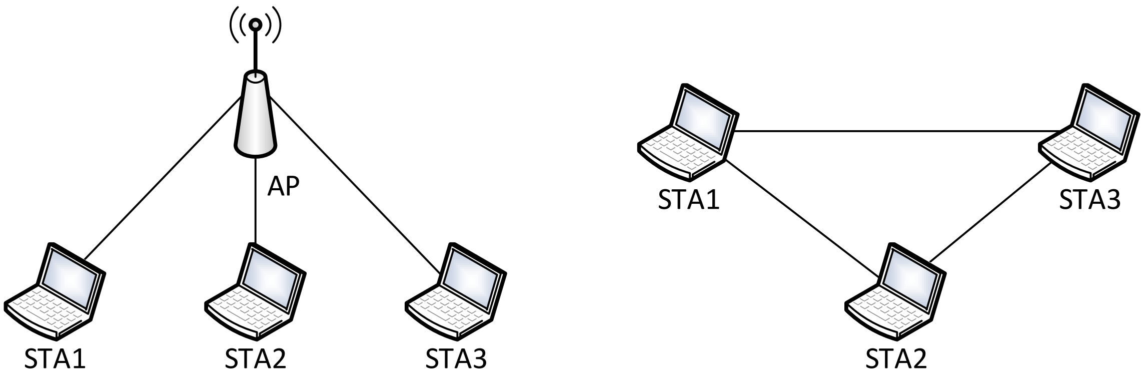
Traditionally, voice communication via analog radios was the most used form of communication in emergency responses. In recent years, many analog systems were replaced by digital services. For instance, Terrestrial Trunked Radio (TETRA) has replaced analog radio systems in many European countries as a standard for public safety communications. TETRA is mainly used for voice communication and brings several improvements compared to analog radio systems. For instance, it supports several communication modes such as one-to-one, one-to-many, or many-to-many. TETRA also provides data services, although its bandwidth is rather constrained compared to other wireless technologies such as Wi-Fi or modern cellular networks. Thus, such high bandwidth wireless technologies provide new opportunities for communication and data services beyond voice (e.g., multimedia services such as live video feeds or pictures from the incident scene). The main focus of this thesis is to improve data delivery on the incident scene by the use of modern wireless technologies. Such wireless networks may be created opportunistically by devices that are carried by the first responders or are deployed by them. Hence, this section focuses on wireless technologies that are supported by a broad range of mobile devices and provide high data rates, in order to support communication beyond voice.

The Institute of Electrical and Electronics Engineers (IEEE) has issued several widely used wireless communication standards in its IEEE 802 protocol family. The set of standards covers different types of wireless networks such as wireless personal networks (WPANs), wireless local area networks (WLANs) and wireless metropolitan area networks (WMANs). The different types provide different ranges and bandwidths and hence have different application areas.

WPANs are networks that are mainly used to interconnect devices that are within a few meters of each other. WPANs are often used as a replacement of cables and often focus on low energy consumption instead of high data rates. WPANs are covered by the IEEE 802.15 protocol family. For instance, IEEE 802.15.1 is the basis for the well-known Bluetooth standard, IEEE 802.15.4 is the basis for ZigBee and also used by 6LoWPAN to transport IPv6 packets in low-energy personal area networks. There are several use cases for WPANs in emergency response scenarios. For instance, WPANs based on the ZigBee protocol have been used to support the triage process by using electronic triage bracelets [57]. Mayer and Fritsche [78] presented a system that integrates wireless sensor networks based on 6LoWPAN with the Internet in order to support emergency management.

WLANs are networks that interconnect devices that are in the range of a few meters up to a few hundred meters. The main purpose of WLANs is to augment or replace wired local area networks in buildings or other local sites such as campuses or company sites. The best known standard for WLANs is the IEEE 802.11 standard and its amendments. In fact, today nearly all mobile devices such as laptops, tablets or smartphones are equipped with an IEEE 802.11 compatible wireless interface (e.g., 802.11 b/g/n). WLANs that are based on an IEEE 802.11 standard are often referred to as Wi-Fi networks. In the following, we will use Wi-Fi as a synonym for WLANs that are based on an IEEE 802.11 standard [53].

The most basic building block of any Wi-Fi network is the so called basic service set (BSS). A BSS consists of at least two wireless devices that are in range of each other. A device that supports the IEEE 802.11 standard is also referred to as a station (STA).



(a) infrastructure BSS

(b) independent BSS

Figure 2.1: Basic Wi-Fi operation modes.

Wi-Fi networks can be operated in one of two basic modes. The first mode is called infrastructure mode (or infrastructure BSS) and the second one is called ad-hoc mode (or IBBS, for independent BSS). In infrastructure mode there is at least one access point (AP) which creates the network and relays data for client devices connected to the access point. Usually, the AP provides its clients access to other networks such as another local area network or the Internet. Wi-Fi networks that operate in infrastructure mode always form a star topology as depicted in Figure 2.1a. Since the AP is used as a relay, clients cannot communicate with each other if the AP fails. The ad-hoc or IBSS mode does not include any infrastructure such as a dedicated AP. Instead, the nodes in the network form a dynamic network and communicate in a peer-to-peer manner to exchange data between each other. An example is shown in Figure 2.1b. This mode has the advantage that the network is more robust since node outages only affect parts of the network.

WLANs are very useful in emergency response scenarios since they provide transmission ranges that suffice in many scenarios and also provide data rates that allow many different services. For instance, 802.11 Wi-Fi networks offer theoretical data rates of up to several hundred Mbit/s and theoretical ranges of up to several hundred meters. Even though the theoretical values are usually not achieved in real emergency response scenarios, Wi-Fi is a very promising technology to support first responders. For instance, Section 2.4.2 presents a Wi-Fi based wireless network that can be used as a communication backbone on a disaster site. The Wi-Fi network is created by deploying wireless routers that form an ad-hoc network or by first responders carrying mobile devices (e.g., smartphones). Additionally, deployed wireless routers also provide wireless access points to connect devices that do not support the ad-hoc mode (i.e., IBSS).

For communication over longer distances, WMAN technologies such as IEEE 802.16 which is the basis for WiMAX networks or wireless cellular networks may be used (e.g., 3G or LTE networks). The architecture of these networks is based on fixed base stations that provide access to fixed and mobile users. Thus, the use of this type of networks is often disturbed in disaster scenarios, since the fixed infrastructure may get damaged or overloaded. On the other hand, WMANs often play an important role in post disaster tasks, since mobile base stations that are deployed after the incident may provide a communication backbone between organizations that operate on the scene and off-site organizations [107].

2.2 Routing for Mobile Ad-hoc Networks

Routing for mobile ad-hoc networks, in the following referred to as *MANET routing*, assumes the existence of an end-to-end path between the source and the destination. Such an end-to-end path may include intermediate nodes which forward data in order to increase the overall communication range. A simple example for MANET routing is illustrated in Figure 2.2. A source node S needs to transfer data to a destination node D. Since S and D are not within transmission range of each other, the data is relayed via an intermediate node I.

The main two tasks of any routing protocol are to find the shortest end-to-end path between a source and a destination and to forward packets via this path. However, finding a path between a source and destination pair is a challenging task in MANETs. The reason is that MANETs are much more dynamic, compared to wired networks where the network topology is more static and link breaks are less frequent. Network topology changes are mainly caused by the mobility of nodes which creates new wireless links and causes existing links to break. Furthermore, disruptions of wireless links caused by obstacles may affect the network topology. Another factor which may prevent nodes from communicating are packet collisions if two or more nodes try to access the wireless shared medium at the same time. MANET routing protocols need to be able to adapt to these topology changes in a distributed manner since no central control unit exists.

MANET routing protocols can be basically classified into proactive, reactive, and hybrid approaches [94, 106]. Proactive MANET routing protocols are very similar to traditional routing protocols for fixed networks and periodically exchange information about (parts of) the network topology. Based on this information, every node builds and maintains a

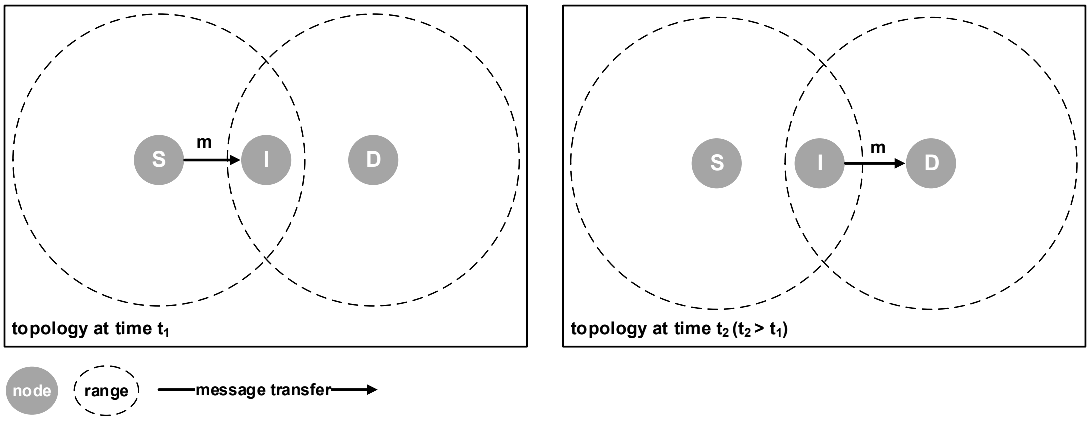


Figure 2.2: Example for mobile ad-hoc routing via a multi-hop path.

routing table that contains paths to other nodes in the network. Hence, proactive protocols are also referred to as table-driven protocols. Routing table entries have to include at least the destination address (e.g., an IPv4 or IPv6 address), the address of the next hop to reach the destination and a path cost metric (e.g., number of hops).

Proactive routing protocols can be further divided into distance-vector and link-state protocols [94]. In a distance-vector protocol only direct neighbors exchange their routing tables. Thus, nodes are only aware of links to their 1-hop neighbors and have no information about the topology of the network. On the other hand, link-state protocols broadcast information about the status of links in the entire network. As a result, every node is aware of the complete topology of the network and can independently calculate the routing table based on this information.

The main advantage of proactive routing is that each node maintains route information about every other node in the network. Hence, packets can be sent instantly when they arrive at the network layer. However, constantly maintaining routing tables imposes some overhead and limits the scalability of proactive routing approaches. Additionally, routing information may become invalid due to topology changes or lost topology update information. If the topology changes too fast (i.e., the network topology changes faster than the link information can be distributed in the network), a proactive routing protocol may not be able to converge. This may cause temporary routing loops because different nodes have a diverse view of the network topology.

Reactive protocols only calculate routes when they are needed. Hence, they are also referred to as on-demand protocols. If a node needs to send data to another node for which it has no route information, a route finding process is initiated by the reactive routing protocol. The route request is flooded in the entire network until the destination, or optionally an intermediate node that already has a route to the destination, replies to this request. As this route finding process may take some time, applications experience an initial delay before the data transfer can start. However, reactive protocols may produce less overhead than proactive protocols since routing control messages are only exchanged when routes are actually needed. Especially when only a subset of the nodes communicate with each other, the control overhead is low compared to proactive routing. Hence, reactive protocols may scale better than proactive protocols. However, if the network topology changes too fast, reactive protocols may produce broadcast storms [85] because of frequent route requests.

Besides proactive and reactive protocols, there are also hybrid protocols that try to combine the advantages of proactive and reactive routing (e.g., the Zone Routing Protocol [50]). The basic idea is that every node proactively calculates routes to a subset of the nodes in the network (e.g., to nodes that are within a certain hop limit) and calculates other routes only when needed. Usually, such hybrid protocols divide the network into different parts. Nodes that are in the same part of the network proactively maintain routes to each other. Routes between nodes that are in different parts are calculated on-demand. The performance of hybrid routing protocols is good if such an organization of the network into different parts reflects the communication demands of the nodes. This means that it is possible to segment the network in a way that nodes from the same segment often communicate with each other and only occasionally contact nodes from other parts of the network.

Several studies have analyzed the performance (i.e., packet delivery ratio, end-to-end delay, routing overhead) of different reactive and proactive routing protocols under different network characteristics [25, 28]. In general, the decision which routing protocol performs best in a network is difficult, since it greatly depends on the concrete application scenario and also the parametrization of the protocol (e.g., update intervals for a proactive protocol). However, there are some basic network characteristics that affect the performance of all MANET routing protocols. First, the mobility of the nodes has a big impact on the routing performance. The different routing approaches perform better if the network is mostly static. In that context, static means that the movement of nodes does not cause many topology changes. In particular, the network topology is stable if the absolute or relative (in relation to their neighbors) node speed is low and thus link break/repair events are less frequent. On the other hand, if the topology changes frequently due to the high mobility of nodes, on-demand protocols flood the network with path requests and table-driven protocols cannot converge (i.e., routing table entries are not updated in time). Second, the network connectivity is an important aspect that determines the performance of MANET routing, since it defines the probability that end-to-end paths exist. Since MANET routing can only route data if an end-to-end path between source and destination node can be established, MANET routing only works well in networks where most of the nodes are connected to each other. Hence, the connectivity of the network has a direct impact on the performance of a MANET routing protocol in terms of the packet delivery ratio.

MANET routing has been an active research field for over one decade and hence many MANET routing protocols have been designed and discussed in the literature. The following subsections cover protocols that are important in the context of this thesis. In particular, we exclude MANET routing approaches such as geographic routing or multicast routing. In geographic routing it is assumed that the routing protocols are aware of the position of other nodes in the network and use this information to calculate routes to other nodes. Since the locations of first responders may not be available in many emergency response operations, we believe that geographic routing is not suited in this domain. Although there are some applications for multicast routing in emergency response scenarios, this thesis only focuses on unicast communication between a sender and a receiver, since we believe that this is the dominant communication paradigm in emergency response operations. A broader overview of existing MANET routing protocols and approaches (including geographic routing and multicast routing) can be found in the literature [1, 6, 26, 77, 106].

2.2.1 Ad-hoc On-demand Distance Vector (AODV) Routing Protocol

A well-known reactive routing protocol is the ad-hoc on-demand distance vector (AODV) [93] routing protocol. Similar to other reactive approaches, the main idea of AODV is that routes are only established if they are needed. In particular, if a route needs to be established, a node broadcasts a so called route request (RREQ) message. All AODV control messages contain a sequence number in order to determine if their information is up-to-date. This information is important to prevent routing loops and also prevents that a node re-broadcasts the same message more than once. Apart from the sequence number, the RREQ includes information about the issuer of the request (i.e., the originator address) and for which node a route is desired (i.e., the destination address). If a node receives a

RREQ and has no valid route to the destination, it re-broadcasts the RREQ to its neighbors. Additionally, the node also creates a temporary entry called reverse route entry that contains the previous hop from which it received the RREQ. This reverse route is later used to route responses back to the originator of the RREQ. If the destination node receives the RREQ, it replies with a route reply (RREP) message. Similarly, intermediate nodes that already have a valid route to the destination, may issue a RREP if they receive the RREQ. If a node receives a RREP, it creates a so called forward route entry to the destination (i.e., it sets the node from which it received the RREP as next hop for the destination) and forwards the RREP using its reverse route entry. In this way routes between the issuer and destination of the RREQ can be established. If the node that originally issued the RREQ message does not receive information about a route to the destination, it repeats the discovery process after a certain timeout. If discovery fails several times, the source drops all packets for that destination and informs the application that no route is available.

In many cases a two-way communication between nodes is needed (e.g., to establish a TCP connection). Hence, AODV includes a mechanism to create two-way routes. In particular, if an intermediate node replies to a RREQ with a RREP, it may also issue a so called gratuitous RREP to the destination of the RREQ so that the destination also has a valid route to the originator of the RREQ.

Apart from finding new routes, it is also important to check the state of existing routes. Hence, nodes also monitor the link state of the next hops of active routes and inform other nodes by issuing a route error (RERR) message if a route gets invalid (e.g., because a next hop moved out of communication range). The RERR message includes the destinations that are affected by the link break and are no longer available via the previously announced route. If a node receives a RERR, it removes routes that include the nodes contained in the RERR. If this causes more nodes to get unavailable, the node adds these nodes to the RERR before broadcasting it. In this way information about topology changes is distributed in the network.

2.2.2 Dynamic MANET On-demand (DYMO) Routing Protocol

Based on previous experiences with reactive routing protocols, both from research and practical implementations, the dynamic MANET on-demand (DYMO) [34] routing protocol has been developed. Since DYMO incorporates many ideas from AODV, DYMO is referred to as AODVv2 in more recent versions of the protocol. It is important to note that DYMO (AODVv2) is still under development by the IETF MANET working group and hence details about the protocols change constantly. The description found here describes the basic idea behind the protocol but does not include details such as which information is stored in control messages, since that information may change in future versions of the protocol.

Similarly to AODV, RREQ and RREP messages are used to find and establish routes in the network. The main difference to AODV is that RREQ and RREP messages do not only contain information about the origin and destination of a request or reply but also about intermediate nodes. Hence, whenever a node receives a routing control message, it adds information about itself (e.g., its IP address) to the control message before forwarding it. In addition, each node puts the routing information that is contained in a received RREQ or RREP message to its routing table. In this way each node learns about routes to intermediate nodes that are on the route between the origin and the destination of the control message.

2.2.3 Optimized Link State Routing (OLSR) Protocol

Optimized link state routing (OLSR) [36] is a proactive link state routing protocol. Nodes exchange routing information periodically and every node maintains a path to all other nodes in the network. Like other link state protocols, all nodes have a complete view of the network. The main difference of OLSR to traditional link state routing protocols for wired networks is the concept of multipoint relay (MPR) nodes. In particular, every node selects a subset of its 1-hop neighbors to be MPRs. The MPR set is the minimum set of nodes that are needed to reach all 2-hop neighbors of a node. Only nodes that are contained in the MPR set of a node need to forward routing control messages and issue link updates. Similarly, only links to MPRs are considered in the route calculation process. Hence, the concept of MPRs reduces the routing overhead and processing complexity compared to traditional link state protocols.

OLSR has several types of control messages. First, every node periodically broadcasts HELLO messages. HELLO messages are never forwarded but only exchanged between direct neighbors. HELLO messages are used for neighbor detection, link sensing and also for the selection of MPR sets. However, the packet format of HELLO messages supports extensions. For instance, HELLO messages are also used for the calculation of the expected transmission count (ETX) metric [38] that is used in many practical implementations of OLSR, although the original IETF specification of OLSR defines hop count as a metric. The second type of control messages are topology control (TC) messages which include link state information. Due to the MPR concept of OLSR, not all links are advertised by TC messages. Instead, OLSR performs two optimizations. First, only nodes that are selected by at least one other node as MPR will generate TC messages. Second, TC messages generated by a node only have to include links to nodes that have selected this node as MPR. This set of nodes is also called the MPR selector set. The first optimization reduces the number of generated link state messages since not all nodes generate them, whereas the second optimization reduces the size of the TC messages since fewer links are included. TC messages are broadcast regularly or whenever the MPR selector set of a node changes.

The remaining two types of control messages are used to support nodes with multiple interfaces and advertise links to external networks. Multiple interfaces declaration (MID) messages contain information about all interfaces of a node that runs OLSR. Hence, every node that runs OLSR on more than one interface has to generate these messages regularly. MID messages contain the addresses of the OLSR interfaces of a node and allow other nodes to determine routes to the OLSR networks that are connected via these interfaces. Finally, host and network association (HNA) messages are used to advertise routes to external networks that do not run OLSR. For instance, if an OLSR node also has an interface that provides access to the Internet, it can advertise this route via HNA messages. Similarly, if an OLSR node also provides a local access point it needs to generate HNA messages that allow other OLSR nodes to send packets to the nodes connected to that access point. The node issuing the HNA acts as a message relay and forwards packets from the OSLR network to the nodes connected to the AP.

2.2.4 Better Approach To Mobile Ad-hoc Networking (BATMAN) Routing Protocol

Another proactive routing protocol is the better approach to mobile ad-hoc networking (BATMAN) [61, 84]. The main design goal of BATMAN is to provide a simple routing protocol that is less complex than OLSR. The BATMAN protocol does not try to find the complete path between a source and a destination. Instead, every node only manages information about the best next hop towards each other node. This information is calculated by sending and receiving broadcast originator messages (OGM). OGMs are sent regularly by every node and include the address of the source (originator address), the address of the node forwarding the OGM, and a sequence number. The sequence number is used to determine if an OGM has already been received before and prevents forwarding the same message more than once. In a network with multiple routes, a node may receive an OGM multiple times via different neighbors. Depending on the quality of the links on a path, the network load etc., more OGMs will be received on good paths. If a node needs to forward data to another node, it uses the neighbor which forwarded most OGMs for that destination. Since wireless networks are dynamic and the quality of paths may change, this information is managed in a sliding window and only OGMs that have a sequence number within that sliding window are considered when calculating the best next hop.

BATMAN is not managed by the IETF MANET working group but by a team of developers that aimed to create an alternative to the OLSR routing protocol based on their experiences with implementing the Linux OLSR daemon (olsrd)[86]. BATMAN is still under active development and details about the protocol constantly change. The description above considers the BATMAN version III that is described in [61, 84] and has also been evaluated in the simulation study that is described in Section 3.4. The biggest change in more recent versions of the protocol is that BATMAN is implemented on the data link layer instead of the network layer. The implementation is called batman-adv. The main advantage is the reduction of the OGM size because no IP header is needed. On the other hand, performing routing on the data link layer breaks the fundamental separation of concerns design principle of IP networking. This results in some side effects. First, MAC layer routing creates a network that only supports a flat IP addressing scheme (i.e., all nodes in the network must use the same subnet mask). Second, from a network layer point of view, the network only consists of 1-hop neighbors since multi-hop routing is performed on the MAC layer. Evaluations have shown that there are no significant performance differences between the network and data link implementation of BATMAN [81]. Thus, it may be argued that the aforementioned disadvantages outweigh the advantages of a MAC layer implementation of the BATMAN routing protocol.

2.3 Routing for Delay-/Disruption-Tolerant Networking

Routing protocols for MANETs assume that a source-to-destination path can be established. In cases where this is not possible, a classical MANET routing protocol cannot deliver data to the destination. To cope with disruptions or the permanent partitioning of the network, routing protocols for delay- or disruption-tolerant networks (DTN) have been developed. Similarly to MANET routing, a message is forwarded by nodes in a hop-by-hop manner until it can be delivered to the destination. However, in contrast to MANET routing, DTN routing does not assume that the delivery is performed via a continuous end-to-end path between source and destination. Instead, DTN routing protocols assume that nodes offer buffers to store messages until there is an opportunity to deliver them to the final destination, or to forward the packets to other nodes in the network. This routing mechanism is called store-and-forward or store-carry-forward routing and is especially useful for sparse networks that only provide few contacts between nodes. An example is depicted in Figure 2.3. Since communication opportunities are very limited in sparse networks, many DTN routing protocols use message replication to increase the delivery probability, as well as to decrease the delivery delay, by utilizing multiple routes in parallel. Thus, DTN routing protocols can be classified into schemes that replicate messages (also called multi-copy schemes) and schemes that forward messages (also called single-copy schemes) [115]. Single-copy schemes do not use replication and delete messages from buffers once they have been successfully forwarded to another node. Multi-copy schemes can further be divided into unlimited and limited schemes. Unlimited schemes flood the network until all nodes have received a message. The number of replications depends on the size of the network and the opportunities to forward messages to neighboring nodes. This introduces a large overhead for storing and transmitting message copies. One way to reduce this overhead is to spread information about delivered messages in order to delete delivered messages from message buffers and prevent further replications. Another way is to limit the number of message copies. Limited-copy schemes define a maximum number of replications that are allowed for a message. This makes it possible to control the number of replications in order to reduce the bandwidth and storage overhead that is introduced by replication.

The main disadvantage of multi-copy schemes is that they do not scale well since they

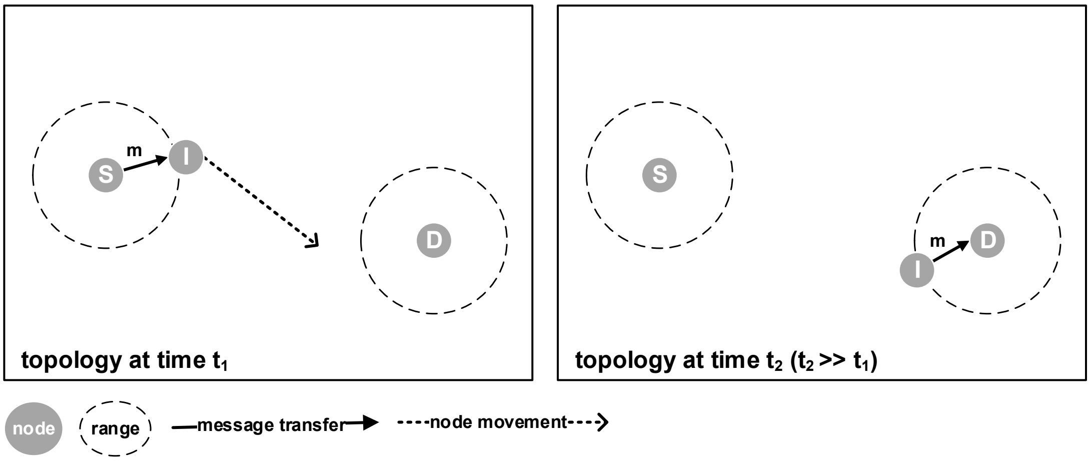


Figure 2.3: Example for store-carry-forward routing exploiting the mobility of nodes.

utilize more resources in terms of bandwidth and storage than single-copy schemes. Limited-copy schemes try to combine the advantages of single-copy and unlimited multi-copy approaches by limiting the number of replicas in the network. This limits the overhead that is introduced by replication. If the number of message copies is limited, it is important to distribute the available copies among those nodes that provide the highest delivery probability. Similarly, it may be beneficial to delay the transmission of certain messages if the current communication opportunity does not provide enough network resources to transmit all stored messages. As the future topology of the network is usually not known in advance, heuristics need to be applied in order to estimate the utility of a node to act as a message relay or to decide when to further keep a message in the buffer [115].

DTN routing protocols are mainly designed for sparse networks and may not perform as well as MANET routing protocols in dense networks. Especially the replication of packets imposes significant communication and storage overhead compared to MANET routing schemes. Thus, it is important to adapt the DTN routing scheme to the expected network density (e.g., by adjusting the maximum number of message copies).

The following subsections describe some DTN routing protocols that are important in the context of this thesis, in particular, the descriptions about the DTN routing protocols that have been used in the evaluations. A broader overview of DTN routing can be found in the literature [32, 132].

2.3.1 Epidemic Routing

Epidemic Routing [122] is a flooding-based scheme that aims to maximize the message delivery ratio and minimize delivery delay. In Epidemic Routing messages are sent to all nodes that have not already buffered the message. In order to determine which messages need to be exchanged between two nodes, nodes exchange so called summary vectors before they transfer any messages. A summary vector includes information about which messages are currently buffered by a node. A node only transfers those messages that are not included in the other node's summary vector. This mechanism avoids redundant message transfers and hence reduces the overhead.

If the bandwidth in the network allows nodes to perform all transmissions and the buffer capacity is sufficient to store all messages, Epidemic Routing minimizes the delivery delay and maximizes the packet delivery ratio, since it will exploit all available paths in the network. However, if resources are limited, Epidemic Routing suffers from the introduced transmission and storage overhead. In particular, it may suffer from message losses due to full buffers and network congestion. Hence, Epidemic Routing is especially useful in sparse networks where only a few communication opportunities exist.

2.3.2 Probabilistic Routing Protocol using History of Encounters and Transitivity

The probabilistic routing protocol using history of encounters and transitivity (PROPHET) [73] is a flooding-based scheme. However, instead of sending a message to all nodes that are encountered, nodes use the history of encounters to calculate if it is actually beneficial to forward a message. In particular, every node calculates the probability for meeting any other node, based on how often it met another node in the past. This metric is called delivery predictability. A node will forward a message only to nodes that offer a delivery predictability that is higher than the node's own one for the destination of the message.

The delivery predictability metric uses information about previous encounters in order to choose message relays. In particular, whenever a node A meets another node B, it updates the delivery predictability as follows:

$$P(A,B) = P(A,B)_{old} + (1 - P(A,B)_{old}) \cdot \alpha$$

The parameter α $(0 < \alpha < 1)$ has two purposes. First, it determines the initial value of $P(A, B)$ when the nodes A and B meet for the first time. Second, α also determines how fast the delivery predictability metric converges to 1 if two nodes meet frequently.

Every node needs to periodically recalculate the delivery predictability to update information about nodes that have not been met recently. This causes the delivery predictability to decrease over time if two nodes are not in contact. In particular, the following aging function updates the delivery predictability for a node B that is not in contact with another node A:

$$P(A, B) = P(A, B) \cdot \gamma$$

The parameter γ $(0 < \gamma < 1)$ determines how fast the delivery predictability converges to 0 if two nodes are not in contact.

Additionally, the delivery predictability is also transitively updated. The idea behind this mechanism is that if a node A does frequently meet another node B and B also frequently meets another node C, node A is also suited to deliver messages to C. In other words, a message destined for C may be delivered via the nodes A and B. Exploiting this transitive characteristic allows the protocol to connect different partitions that are mostly disjoint but are connected by some nodes that travel between the partitions. The transitive update function is as follows:

$$P(A, C) = P(A, C)_{old} \cdot (1 - P(A, C)_{old}) \cdot P(A, B) \cdot P(B, C) \cdot \beta$$

The parameter β $(0 \leq \beta \leq 1)$ is used to control the impact of transitivity. If it is set to 0 the delivery predictability does not include transitive relations but only direct contacts between nodes.

2.3.3 MaxProp

MaxProp [29] complements a flooding-based forwarding scheme with congestion control and buffer management strategies. MaxProp uses the meeting probability as a routing metric. For a network with n nodes, every node has to manage a vector of size $n - 1$ for storing the meeting probabilities with the other nodes in the network. Initially, every value in the vector is set to $\frac{1}{n-1}$. When a node meets another node, the vector is updated by incrementing the meeting probability with this node by 1 and then the entire vector is normalized so that the sum of probabilities is 1 again.

To determine routes in the network, a graph is calculated where the costs of edges are based on the meeting probabilities. Based on this graph, nodes can calculate the costs for a path to a destination by summing up the costs of the edges (i.e., summing up the probabilities that each contact on the path does not occur) and send data via the shortest path (i.e., the path that offers the highest chance to deliver the packet to the destination).

MaxProp uses several additional mechanisms on top of the path-likelihood routing in order to increase the delivery probability and reduce delay. First, messages are sent in a particular order (e.g., control messages and new messages that have a low hop count are prioritized) that tries to better exploit available transmission opportunities and hence to increase the overall packet delivery ratio. Second, MaxProp also applies a buffer management mechanism that first drops packets that are less likely to increase the packet delivery ratio to better cope with buffer overflows.

2.3.4 Spray and Wait

Spray and Wait [113] is a replication-based protocol that limits the number of message copies in the network in order to reduce the transmission overhead compared to flooding-based schemes. Messages contain a replication counter that determines how often the message may be replicated in the network. Whenever a node meets another node that has not already a copy of the message, it hands over a fraction of its copies to this node (i.e., it reduces the replication counter and forwards the message to the other node). This is called the spray phase since message copies are spread in the network. If a node has buffered a message with a replication counter of 1, it is not allowed to forward the message to any other node but the destination. This phase is called the wait phase since the node has to wait until it meets the destination in order to forward the message.

In the following, we give a simple example of Spray and Wait routing. We assume that the initial number of message copies is four and that nodes hand over half of their message copies to other nodes. This spraying scheme is also referred to as *binary* Spray and Wait. First, a new message is created at node A with a replication count of 4. Node A can hand over two messages to the first node that it meets (node B) and one copy to the second node it meets (node C). Afterwards, node A and node C enter the wait phase. Node B, which received two copies, can forward the message once before it also enters the waiting phase. Hence, in total the message is transmitted three times during the spraying phase and four nodes have a message copy buffered that may be delivered to the destination of the message.

The initial number of message copies and the spraying scheme can be used to configure the routing algorithm. For instance, there may be use cases where it is beneficial to adapt the initial number of copies based on the importance of a message in order to improve the delivery probability for certain messages, or to adapt the number of forwarded message copies based on the probability that another node meets the destination.

2.4 Networking in Emergency Response Operations

This section describes different types of networking architectures for emergency response operations. Additionally, it presents a concrete networking system that has been developed in the course of a European research project called BRIDGE.

2.4.1 Types of Infrastructure in an Emergency Response

In an emergency response, several types of infrastructure can be identified [4]. First, *existing infrastructure* denotes infrastructure that is already available at the incident site and has survived the effects of the disaster. For instance, cell towers that are still intact and provide access to a mobile network or public Wi-Fi hotspots that provide Internet connectivity. Similarly, a TETRA network may provide voice communication for first responders. However, existing infrastructure is often severely affected by disasters, either because it is destroyed by the disaster itself, or because the remaining infrastructure gets overloaded in the aftermath of a disaster. Thus, first responders or other organizations may deploy communication equipment at the incident scene, so called *deployable infrastructure*. One example are mobile TETRA base stations that can be used to coordinate emergency response personnel at an incident location. Another example is the BRIDGE mesh network that is described in Section 2.4.2. It is very important to integrate the deployment of networking equipment into the standard procedures of first responders. For instance, Wolff and Wietfeld [128] suggest to integrate wireless routers in the couplings of fire hoses in order to automatically create a wireless ad-hoc network while firefighters deploy a fire hose. Similarly, Ramirez et al. [102] describe the use of small, deployable network devices, called landmarks, that can support the indoor navigation of firefighters. The third type of infrastructure is *opportunistic infrastructure* that refers to the use of devices and resources such as smartphones to support emergency response. For instance, the Help Beacons [5] and Local Cloud [4] systems use this type of networking approach. The Help Beacons system consists of an application for Android smartphones that can be used by victims of a disaster to send a distress signal (called help beacon). In particular, the Help Beacons system utilizes the ability of Android smart phones to create Wi-Fi networks in infrastructure mode in order to put SOS messages into the SSID of the created Wi-Fi network. These SOS messages can be retrieved by first responders using the Help Beacons seeker Android application. No additional infrastructure is needed since the system creates wireless networks in an opportunistic manner. The Local Cloud application [4] is another example for the use of opportunistic communication in a disaster situation. It allows users to exchange Twitter messages via their Android smartphones in a hop-by-hop manner, until one of the users can access the Internet in order to post collected messages to the Twitter servers. Like the Help Beacons application, it uses Wi-Fi networks that are created by the smartphones themselves. In the case of first responders, it can be assumed that such applications are pre-installed and hence are available when needed. However, it may be challenging to install these applications during a disaster, since today's application repositories for smartphones usually require Internet access. Hence, it is still an open issue how to provide such applications for the public in disaster situations. In [3] we presented and assessed some means to distribute and install applications without requiring Internet access.

The different types of infrastructure can be used in different phases of an emergency response. Opportunistic networks may be the most prominent type in the immediate aftermath of a disaster since they do not depend on any additional infrastructure. Such opportunistic networks may be created by first responders or even victims and bystanders that carry mobile devices. Even though these networks will probably not cover the entire disaster area and also be prone to disruptions and partitioning, they may already prove to be useful for the initial response.

After the initial first responder teams have arrived at the disaster scene and coped with the most immediate tasks, they may start to deploy wireless routers that provide a wireless network such as the one that is described in the next section (cf. Section 2.4.2). Thus this type network is not immediately available but it can be assumed that it is installed within the first few hours of a disaster. Similarly, mobile network operators could deploy portable base stations that re-establish the cellular network in the areas that are affected by the incident. Usually a large scale disaster also affects other infrastructure such as streets or the power grid, which makes it a very challenging logistical task to bring and deploy such mobile stations to the disaster scene. Hence, it can be assumed that it takes days or even weeks before such equipment is available. However, this initial reconstruction of local infrastructure is still useful for coordinating post-disaster recovery. For instance, it took nearly three months after the 2011 Great East Japan Earthquake to rebuild the communication and power infrastructure of some severely affected regions [107]. The aforementioned deployment of temporary infrastructure is useful in such cases.

This thesis focuses on opportunistic networks that are created on the incident scene and provide a local communication network for first responders. Chapter 3 presents two such scenarios. It is important to note that while we did not explicitly model off-site communication, it can be assumed that the incident command post that is established at the disaster scene provides a gateway to other networks such as the Internet that makes a communication between the disaster scene and off-site organizations possible.

2.4.2 The BRIDGE Networking Infrastructure

BRIDGE [27] is a collaborative project, funded by the European Union in its 7th Framework Programme. The main goal of the BRIDGE project is to improve crisis and emergency management in EU member states by providing a system that supports technical and social interoperability in large-scale emergency relief efforts. Interoperability between different stakeholders is a key issue that determines the effectiveness and success of an emergency response operation. Thus, the BRIDGE system supports the flexible assembly of emergency response systems, both legacy systems and systems created within the BRIDGE project. At the networking level, BRIDGE develops a networking infrastructure that facilitates system and network interoperability by using common wireless technologies.

The goal of the BRIDGE network infrastructure is to provide a communication and networking platform that can be used if the existing infrastructure is not operational anymore. This is important since disruptions of the networking infrastructure are common in disaster situations. In the following, this BRIDGE networking infrastructure is described.

The BRIDGE mesh network (also referred to as BRIDGE Mesh) is a WLAN that can be deployed by first responders on the incident site. The BRIDGE Mesh needs to be able

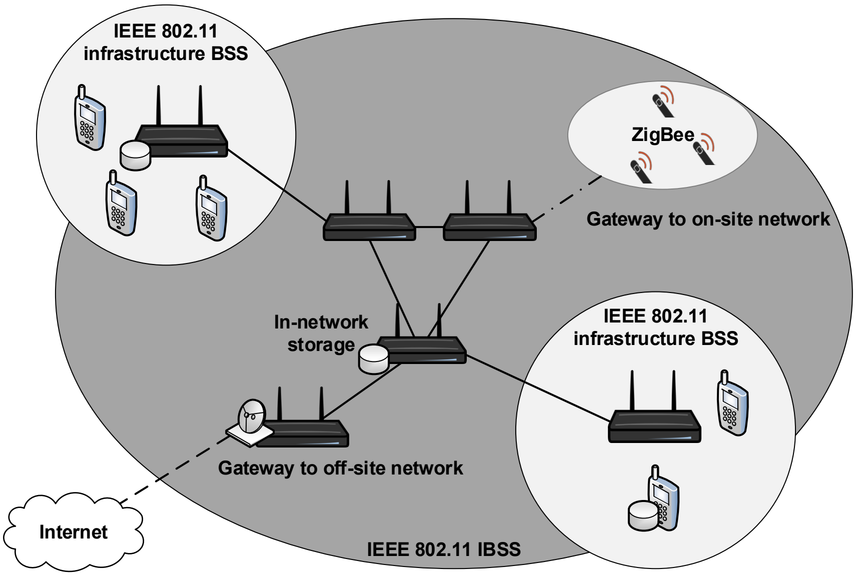


Figure 2.4: BRIDGE Mesh network.

to connect heterogeneous devices, both in terms of hardware and supported wireless standards, into one uniform networking infrastructure. In order to provide a communication backbone, the BRIDGE Mesh uses IEEE 802.11 in ad-hoc mode (i.e., IBSS mode) to interconnect routers on the disaster site. In particular, every router needs to support IEEE 802.11g on a 2.4 GHz channel and may optionally also provide IEEE 802.11n (either on a 2.4 GHz or a 5 GHz channel). IEEE 802.11 has been chosen since it is a well-known and widespread standard. Additionally, it offers a good trade-off between wireless range and bandwidth. Besides the Wi-Fi interface to interconnect routers, a BRIDGE Mesh router may also provide additional interfaces and act as a gateway to other wireless or wired networks. For instance, routers may also provide an AP in order to connect client devices such as smartphones, notebooks or tablets with the BRIDGE Mesh. Similarly, a router may also provide interfaces to WPANs and WANs. For instance, a router may include a ZigBee interface in order to allow wireless sensors to transmit data, or a 3G modem to provide access to the Internet via a mobile network. Figure 2.4 shows an example of a BRIDGE network, consisting of different types of devices.

Depending on the functionality of a BRIDGE Mesh network device, one can differentiate between different device types. The simplest network elements in a BRIDGE Mesh are wireless repeaters that extend the range of the wireless network. Since the location of the incident command post and different hotspots at the incident site may be far away from each other, these devices may need to be deployed to provide wireless communication between the different locations on the incident site. The second type of network elements are gateways which provide access to existing off-site networks, in general the Internet. This connects the local network on the incident scene with networks from higher level organizations, which are situated in off-site emergency operations centers. Usually, such a gateway device will be located very near to the incident command post (e.g., directly on an incident command truck) since the command post itself usually needs connectivity to external networks. The third type of network elements are gateways between different wireless technologies on the incident site. For instance, the BRIDGE electronic triage bracelets that support the process of determining the priority of treatment of patients on the site, use ZigBee to transfer collected data. A gateway device that sends the collected triage data via the IEEE 802.11 based mesh network to the incident command post needs to be deployed near the triage area. Similarly, gateway devices could connect sensor networks that are based on 6LoWPAN with the BRIDGE Mesh. Finally, there are network elements that provide in-network storage of data when the network gets partitioned and data cannot be instantly forwarded. These devices provide a large amount of storage on the order of gigabytes and use the bundle protocol [110] for communication.

The BRIDGE Mesh network has been tested in several real world demonstrations and emergency response exercises. During a full-scale emergency response exercise in the Risavika harbor near Stavanger in Norway, several routers have been deployed in order to provide access to the Internet on the incident location, and to provide a gateway for the data collected by other components within the BRIDGE system. For instance, the in-network storage devices have been used to store distress calls collected by the Help Beacons application (see Section 2.4.1) until they could be forwarded via the BRIDGE Mesh to an incident command post. Figure 2.5 shows two deployment examples. In another exercise, the BRIDGE Mesh has been used to provide a local communication network in a tunnel fire scenario.

The findings of this thesis contribute to the goals of the BRIDGE project. First, this thesis provides insights into specifics and challenges of networking in emergency response scenarios (cf. Chapter 3). Based on this initial investigation, routing algorithms that can better cope with the identified challenges than state-of-the art approaches are developed (cf. Chapter 4). The focus of this work are local networks on the incident site that are used by different organizations involved in the emergency response in order to communicate

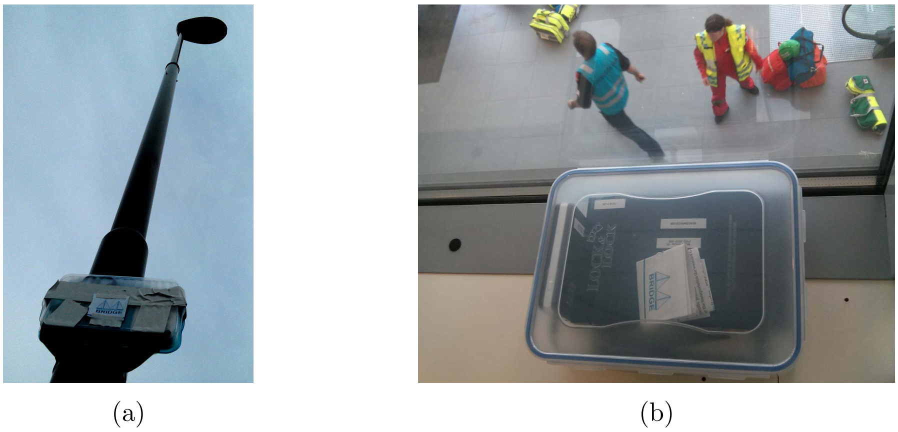

(a) (b)

Figure 2.5: BRIDGE Mesh prototypes deployed in full-scale emergency response exercise.

and exchange information. It is important to note that this work does not deal with off-site inter-organizational information exchange. Another contribution of this thesis towards the goals of the BRIDGE project is to investigate how multimedia services can be used on the disaster site (cf. Chapter 6). Multimedia communication is a challenging task in such environments since the communication networks on the incident site may be prone to disruptions. On the other hand, the BRIDGE project acts as source of requirements for the algorithms and systems that are presented in this thesis.

2.5 Mobility and Wireless Modeling

Emergency response is a challenging domain for research and application development. One of the reasons is that disasters are sudden events and usually researchers are not able to perform measurements on a disaster scene. For instance, it is usually not possible to test and evaluate a wireless communication system during a real-world emergency response operation. This is also true for collecting data that helps to evaluate systems in simulated environments. For instance, it is relatively easy to equip students with smartphones or other devices that can record their movements while they are on campus since that is an everyday situation in a partly controlled environment. However, collecting traces from first responders during an emergency response is usually not possible. One alternative is to gather traces during emergency response exercises which are planned in advance. However, realistic exercises are also stressful events that require first responders to fully concentrate on their tasks. For instance, in the course of the BRIDGE project it was planned to gather GPS logs during the full-scale exercise in the Risavika harbor in Norway. About 30 first responders were equipped with smartphones that could log their locations during the exercise. However, when analyzing the collected data it became clear that some first responders had forgotten to activate the provided smartphone, left it at the fire station or that some responders exchanged their phones which made it impossible to correctly match the mobility trace with their actual task. Thus, only a fraction of the traces remained usable, which was too small to be used for evaluation purposes. Although it would have been technically possible to correct some of the flaws during the exercise (e.g., activate GPS on smartphones), the scale and nature of the exercise made it impossible to perform such changes while the exercise was running.

For the reasons described above, modeling is the most practicable way to create disaster scenarios that can be used for evaluations. Thus, this approach has also been chosen to evaluate the algorithms that are described in this work. Creating scenarios that model the specifics of emergency response scenarios in a realistic way has still been an important issue. Hence, realistic assumptions about the movements of first responders on the scene and their working environment have been made. In the following, we present state-of-the-art approaches for mobility modeling and wireless modeling.

2.5.1 Mobility Modeling

The mobility of the nodes is an important property of every wireless network since it influences the connectivity characteristics of the network. Thus, it is important to use mobility models that mimic the behavior of the nodes in a realistic way. Many different mobility models have been designed that describe different movement patterns of nodes.

Synthetic models are the most widely used type of models. They calculate the movement of nodes based on pre-defined rules and some pseudo-random factors. Apart from using these synthetic models for evaluation purposes, it is also possible to gather movement traces from nodes in real-world networks. Usually, such traces are collected by equipping devices with sensors that track their positions during a certain period of time. Another possibility to create movement traces is to log to which Wi-Fi hotspots or cell towers the devices of the tracked users have been connected over time. Such traces make it possible to use more realistic movement patterns in evaluations but usually they are less generic, since they only capture a certain use case over a limited period of time. There are also approaches to combine the advantages by creating synthetic models that are based on mobility traces.

Generic Mobility Models

One of the most widely used synthetic mobility models is the random waypoint model (RWP) [31]. In the RWP model every node performs the following three steps independently from every other node:

1. Choose a random location from the available area. Additionally, choose a random movement speed from a uniformly distributed random variable constrained by a minimum and a maximum value.
2. Move to the chosen location with the chosen movement speed.
3. Choose a random waiting time, also uniformly distributed between a minimum and a maximum value and repeat the procedure starting at the first step after this time has passed.

Although all nodes move independently from each other and all waypoints are chosen randomly, it has been shown that the RWP model produces clusters of nodes around the center of the simulation area. This is due to the fact that it is very likely that nodes choose waypoints that cause them to travel through the center of the simulation area [21]. Variations of the RWP model do not suffer from this clustering. Examples are the random direction model and the random walk model [31].

The random direction model is similar to the RWP model in the sense that all nodes move randomly. However, for each movement, nodes choose a random direction instead of a random location. This modification prevents the clustering of nodes at the center of the simulation area [18]. A node moves into the chosen direction until it reaches the border of the area where it bounces off or appears at the opposite side of the simulation area.

The random walk model is similar to the random direction model. However, instead of moving until hitting a border, each movement is restricted either by a maximum distance or a maximum movement time, after which the node performs the next decision. The parameters of the model are speed, direction, travel time and/or travel distance. The maximum values for the travel time and the distance may be fixed or randomly chosen from a certain interval. For instance, the random walk implementation which has been used in the evaluation described in Chapter 5 supports random speeds, distances and travel times.

Generic mobility models offer a simple way of modeling the movements of nodes. However, the main problem of generic models is that in reality nodes in a network usually do not move in a random manner. Hence, these models may be useful to assess some generic properties of a protocol or system but may not reflect its performance under real-life settings. This is also true for the mobility of first responders. The following sections present models that are better suited for describing the mobility in emergency response scenarios.

Event-driven, Role-based Disaster Mobility

Nelson et al. [83] describe a role-based and event-driven mobility model for emergency response. The model defines three entities which are object, role, and event. An *object* represents a node that has a certain location and velocity. Additionally, every object has a certain *role*. For instance, a node can represent a victim or a first responder. The role of the node determines its general mobility behavior, since each role has a certain mobility pattern assigned to it. Additionally, the model defines *events*, which represent the most complex entity of the model. Basically, events impact the generic mobility pattern of nodes that are near to the event. In particular, an event attracts or repels nodes depending on several parameters, such as the role of the node, or the location and intensity of the event. For example, nodes that are within the so called *disaster radius* are immobilized, which represents the direct impact of the disaster. Nodes that are within the so called *event horizon* adapt their movements immediately. For instance, victims flee from the event while first responders approach it. Nodes that are within the so called *relevant radius* react after a *radio contact time*. This represents first responder units that are dispatched to the event's location.

The event-driven, role-based model is flexible and supports modeling a broad range of disaster scenarios. On the other hand, it offers many parameters which have to be configured. For instance, in order to define an event, one has to set several radii that influence how the event impacts its environment. It is rather hard to find realistic values for these parameters, since these parameters may not have a correlation with effects of real disaster events. Unfortunately, Nelson et al. [83] do not describe how to find reasonable values for the parameters, nor do they describe the effects of certain parameters.

Post-Disaster Mobility Model

The post-disaster mobility (PDM) model [121] simulates large-scale emergency response operations in urban environments. It especially focuses on large-scale disasters such as hurricanes or earthquakes. Although the name of the model suggests that it only covers situations after a disaster, there are also disasters where the emergency response starts before the disaster hits. For instance, hurricanes usually do not strike suddenly but people get warned and evacuation procedures start beforehand. The post-disaster mobility model can also capture such evacuation procedures that are happening before a disaster.

The PDM model targets urban environments where different neighborhoods are affected by a disaster and need to be evacuated. The model supports to define a certain number of neighborhoods that are connected via roads. Every neighborhood has a certain radius and includes a number of houses and people. Thus, the nodes are clustered in the simulation area based on the position and size of the different neighborhoods. When an evacuation is started, a node may either move to the nearest evacuation center after a random waiting time, or ignore the evacuation (depending on a random variable that defines the probability of evacuation). Evacuated nodes return to their designated houses after a designated random waiting time, whereas nodes that ignored the evacuation move randomly within their neighborhood.

Apart from the evacuation centers, there are a few other types of centers that define the movement of first responder nodes. For instance, according to the PDM model every scenario needs to have at least one main coordination center. Other examples for available centers are medical centers and hospitals, police and fire stations. There are also several types of first responder nodes available, for instance, supply vehicles that carry relief goods between main centers and evacuation centers, police cars that patrol neighborhoods, ambulances, and fire trucks that can react to randomly placed events such as fires. Additionally, the model supports rescue workers and volunteers that assist the evacuation.

Since the PDM model focuses on complete urban areas, it is a rather complex mobility model. In order to model a scenario, one has to select the number of neighborhoods, houses and inhabitants. Additionally, the position of the pre-defined centers such as fire and police stations and how many vehicles are available in these stations has to be modeled. The number of rescue workers that assist the evacuation has to be chosen as well.

Disaster Area Mobility Model

The disaster area mobility model [12] focuses on the process of recovering victims from a disaster site. In such operations, the rescue services usually separate the incident scene and its surroundings into several tactical areas. This tactic is also referred to as *separation of the room* [12]. In particular, there are designated areas where the treatment of victims takes place, ambulances and other transport units wait to pick up victims and an area where the incident command post is located. Based on their role in the recovery process, first responders move within or between these tactical areas. The disaster area mobility model is based on this concept of separating the incident site into tactical areas.

The disaster area mobility model defines five different types of areas:

- Incident Location (IL): the area where an incident happened and patients are located
- Patients Waiting For Treatment Area (PWFTA): the area where the triage takes place and patients that have been rescued from the incident location wait for initial treatment
- Casualties Clearing Station (CCS): the area where patients receive extended aid and are prepared to be picked up by an ambulance
- Ambulance Parking Point (APP): the area where ambulances park before they pick up patients
- Technical Operational Command (TOC): the area where the local incident command staff is located

Every tactical area has a certain size and shape and contains a certain number of nodes representing first responders. There are two types of nodes: so called transport nodes, which move between two different types of areas and so called stationary nodes, which do not leave their designated area. In addition to the aforementioned five tactical areas, the model also supports obstacles that restrict the movements of nodes between the areas. All transport nodes use the shortest available path between two tactical areas, while stationary nodes move randomly within their designated area.

The mobility of a node is based on its role (i.e., whether it is a transport or a stationary node) and the tactical area that it is assigned to. For example, nodes that are assigned to an IL move between this IL and the PWFTAs in the simulation area. This represents first responders who pick up patients[1] from a dangerous location on the incident site and bring them to a safer place where they wait for further treatment. Similarly, nodes assigned to a PWFTA transport patients to a CCS. PWFTAs and CCSs may also contain stationary nodes that represent medical personnel looking after patients. Transport nodes that are assigned to an APP represent ambulances that pick up victims from a CCS and bring them to a hospital. Every tactical area but the TOC have defined entry and exit points that are used for entering and leaving the area. Similarly, there are designated entry and exit points at the border of the simulation area where ambulances enter and leave the simulation. The TOC is the only area that is not directly involved in the transportation process but includes nodes that represent the command staff that supervises and manages the emergency response operation.

We have chosen the disaster area mobility model to simulate the mobility of first responder nodes. The main reason for that decision is that we are mainly interested in the characteristics of wireless networks on an incident scene. The disaster area mobility model focuses on the movement of first responder nodes at the incident scene itself. This distinguishes this model from the post-disaster mobility model and the role-based, event-driven mobility model that both focus on metropolitan areas. In the course of the BRIDGE project, several generic disaster scenarios were described that are based on real-world incidents, for instance, an incident in a chemical plant, or the detonation of a bomb in an airport terminal. Additionally, the BRIDGE project could also take part in a full-scale exercise in the Risavika harbor near Stavanger, Norway. For both cases, the disaster area mobility model was well suited. For instance, the separation of the room concept that is the basis of the disaster area mobility model has been observed in the Risavika exercise.

2.5.2 Wireless Modeling

In addition to the mobility of nodes, another factor that influences the performance of a wireless network is the propagation environment. We use a combination of two propagation models to capture the effects of mixed indoor/outdoor environments. This is a realistic assumption since in disaster scenarios first responders often have to temporarily work indoors

[1] Please note that the disaster area mobility model does not explicitly model patients but only includes first responder nodes. However, for the sake of clarity, this description of the mobility on the disaster area also includes patients.

which has severe effects on the wireless propagation and hence also on the connectivity characteristics of the wireless network. For instance, if a firefighter has to enter a building, his/her communication device may get disconnected from the rest of the network since walls may block wireless signals.

The reception power decreases with the distance between sender and receiver. This is expressed by the so called path loss which is the fraction of received power and transmitted power. If the sender and the receiver are in line of sight, the loss of power can be expressed using the free-space path loss model which is defined as follows [46, p.49]:

$$L_p(dB) = 20 \cdot \log \left(\frac{4\pi d}{\lambda} \right),$$

where d denotes the distance between sender and receiver and λ denotes the wavelength of the signal. For wireless signals $\lambda = \frac{c}{f}$, where c denotes the speed of light and f the frequency of the signal.

Additionally, we also use a wireless obstacle model to include the effects of first responders also working indoors and large obstacles that may obstruct the line-of-sight path between a sender and a receiver. In particular, a wireless obstacle model by Sommer et al. [112] is used. This model has been chosen as it is simple to configure but still suits our purpose of modeling static obstacles that attenuate wireless signals. According to this model, a signal is attenuated if an obstacle obstructs the line of sight path between the sending and the receiving node by applying the following loss:

$$L_o(dB) = \beta \cdot n + \gamma \cdot d_m,$$

where β denotes the attenuation in dB per border of the obstacle (e.g., the walls of a building), n denotes the number of intersections with the obstacle between sender and receiver, d_m denotes the distance the signal has to travel inside the obstacle and γ denotes the attenuation in dB/m that represents the inner structure of the obstacle. Every obstacle is defined based on its location, shape and the effect it has on the signal (i.e., β and γ). β represents the attenuation property of the obstacle material (e.g., the brick wall of a house). It has to be noted that the attenuation depends on the frequency of the signal and is in general very obstacle specific [112]. However, there exist some measurements concerning the attenuation properties of common building materials [14, 45, 105] which can be used to define a reasonable value for β. For instance, in the case of brick walls, attenuation values of 6 dB up to 25 dB have been reported, depending on the thickness of the wall and insulation. Based on the measurements of Sommer et al. [112], γ is usually less than 1 dB/m.

If other losses (e.g., the loss due to obstacles) are also present, they can be added as further factors, i.e. the overall loss L can be calculated as follows (cf. [46, p.49]): $L = L_p \cdot L_o$, or as: $L(dB) = L_p(dB) + L_o(dB)$, if the values are given in decibel. To calculate the received power P_r for a signal the following general calculation can be used (cf. [112]):

$$P_r(dBm) = P_t + G_t + G_r - L,$$

where P_t is the transmission power (in dBm), G_t and G_r denote the antenna gains of the transmitting and the receiving antenna (in dB) and L denotes the overall loss (in dB).

As mentioned before, we consider free-space path loss and the loss caused by obstacles. Hence, the receiving power is calculated as follows:

$$P_r = P_t + G_t + G_r - \underbrace{20 \cdot \log\left(\frac{4\pi d}{\lambda}\right)}_{\text{path loss}} - \underbrace{\beta \cdot n + \gamma \cdot d_m}_{\text{obstacle loss}},$$

Receivers can reconstruct the information that has been transmitted if the received power is higher than a certain threshold. This threshold is also referred to as the receiver sensitivity Θ and is an important antenna characteristic. So in other words, a signal can be received if $P_r \geq \Theta$. Based on the receiver sensitivity and the sending power, the maximum transmission range can be calculated. These two models are included in the evaluation framework that is described in the next chapter, We use a fixed frequency of 2.4 GHz as this is the most used frequency for Wi-Fi and assume that antennas to not provide any gain (i.e., $G_s = G_r = 0\, dB$). The sender power and the sensitivity of the receivers can now be set to achieve a certain wireless range (assuming no obstacles in the line-of-sight path). For instance, to achieve a maximum transmission range of $100m$ using a sender power of $3dBm$, the receiver sensitivity has to be set to $-77dBm$. Further details about the parameters that are used for simulations are found in the next chapter (cf. Section 3.2.2 and Section 3.3.2).

CHAPTER 3 Modeling and Evaluating Wireless Networks in Emergency Response Scenarios

Emergency response operations are complex scenarios requiring different organizations to work together in order to handle the situation at hand. Information is one of the key resources in an emergency response operation and the ability to exchange information is very important to achieve the goals of the response operation in a timely and effective manner. The type and size of the disaster determines which and how many organizations are involved in the emergency response. In small scale emergencies, most coordination takes place at the incident site and is handled by the incident commander that is on the scene. However, when a big disaster strikes, the emergency response gets larger which requires even more coordination efforts, also with organizations that are located off-site. Hence, there may also be a need to exchange data between the incident site and remote sites. Existing communication infrastructure, such as the Internet or telephone networks, can be used to coordinate the response off-site, since these networks are usually still available. Similarly, the interested public can use such infrastructure to get information about the disaster. However, at the incident site itself, the access to existing networks may be severely hampered. The existing infrastructure may be destroyed or overloaded which makes information exchange at the incident site a challenging task. As an alternative, first responders may deploy local wireless networks such as the BRIDGE Mesh (cf. Section 2.4.2) or rely on opportunistic networks. These types of networks provide the means to exchange information at the incident site itself and may also provide gateways to existing, off-site networks.

The contributions of this chapter are as follows: First, this chapter presents a modeling framework that supports creating realistic emergency response scenarios that can be used to evaluate wireless ad-hoc networks on a disaster scene. The framework is based on existing tools that are combined to model scenarios that include realistic mobility patterns of first responders and also the effects of obstacles on wireless links. Furthermore, this chapter presents two emergency response scenarios that have been modeled with the help of this framework. The first scenario describes an emergency response effort after an incident in a chemical facility. The second scenario models a real-world exercise that simulated a terror attack at a harbor. For both scenarios we evaluate the connectivity characteristics for different wireless transmission ranges. Additionally, this chapter presents the results of an evaluation of state-of-the-art MANET routing protocols in the chemical incident scenario. Please note that some parts of this chapter are based on previously published work. In particular, the connectivity evaluation of the chemical scenario has been partly published in [98] and the evaluation of the MANET routing protocols can be found in [96].

This chapter is organized as follows: Section 3.1 presents the modeling framework that has been used to model the two emergency response scenarios that are presented in Section 3.2 and Section 3.3. Additionally, Section 3.4 presents a simulation-based evaluation of the performance of several state-of-the-art MANET routing protocols in the chemical incident scenario. Finally, Section 3.5 concludes this chapter.

3.1 Modeling and Evaluation Framework

This section describes the modeling and evaluation framework that is used to create and evaluate realistic emergency response scenarios. The framework is mainly based on existing simulation frameworks and tools. This has the advantage that the soundness and comparability of the simulation results is improved, compared to using custom simulators and custom implementations of models and protocols. Based on these existing modeling and simulation tools, a modeling framework has been created that can be used to model emergency response scenarios and perform evaluations in these scenarios. Figure 3.1 shows an overview of this framework.

The first part of the framework is the BonnMotion tool [13]. BonnMotion supports the creation and the analysis of mobility scenarios. Moreover, it is possible to export mobility traces which provide information about the position of each node at a particular time. BonnMotion includes implementations of several mobility models, including the random waypoint model, the random walk model and the disaster area mobility model which have been described in Section 2.5.1. BonnMotion also provides an analysis component to calculate statistics about a given scenario, such as number of neighbors or network partitions. However, as depicted in Figure 3.1, BonnMotion has not been used to analyze the connectivity characteristics of the scenarios but only to create mobility traces. The reason is that BonnMotion does not support modeling the wireless characteristics of a network and

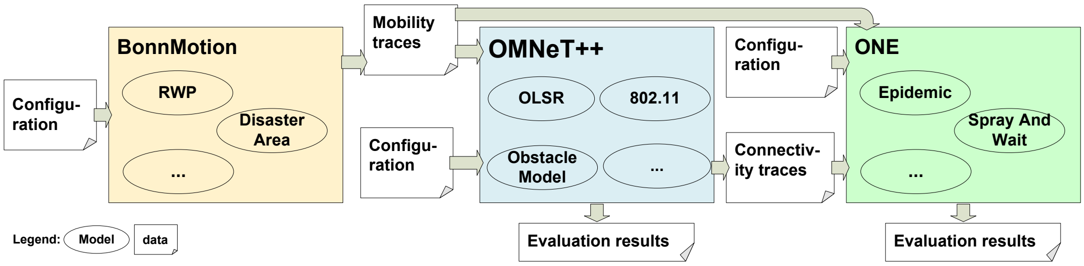


Figure 3.1: Overview of the modeling framework.

hence it is not possible to include the effects of wireless obstacles and more complex wireless transmission models in the connectivity analysis.

The second part of the framework is the OMNeT++ simulation framework [87]. It is a packet level simulator that provides physical models describing the propagation of wireless signals, such as the free-space path loss or the obstacle model that have been presented in Section 2.5.2. Additionally, there also exist implementations of several mobile ad-hoc routing protocols (e.g., OLSR, AODV). We used OMNeT++ to evaluate several state-of-the art MANET routing protocols (see Section 3.4) and to evaluate a hybrid MANET/DTN routing protocol that is described in Section 4.4. Additionally, OMNeT++ has been used to create connectivity traces that include information about which nodes are connected via wireless links. These connectivity traces also capture effects of wireless propagation in presence of obstacles that attenuate signals. The connectivity traces have been used to assess the characteristics of the two emergency response scenarios that are presented later in this chapter.

The third part of the framework is the ONE simulator [63]. This simulator is widely used to evaluate DTN scenarios and includes implementations of several well-known DTN protocols, including the protocols described in Section 2.2. Apart from using the ONE simulator to evaluate the performance of several state-of-the-art DTN routing protocols, we also implemented and evaluated the hybrid MANET/DTN protocol that is presented in Chapter 4. Compared to OMNeT++, the ONE simulator does not include detailed models about the physical and medium access control layers. However, the effects of these two layers are captured by the connectivity traces that are generated by OMNeT++. Hence, the presented framework exploits the advantages of OMNeT++ concerning realistic models for the lower layers as well as DTN routing protocol implementations within the ONE simulator.

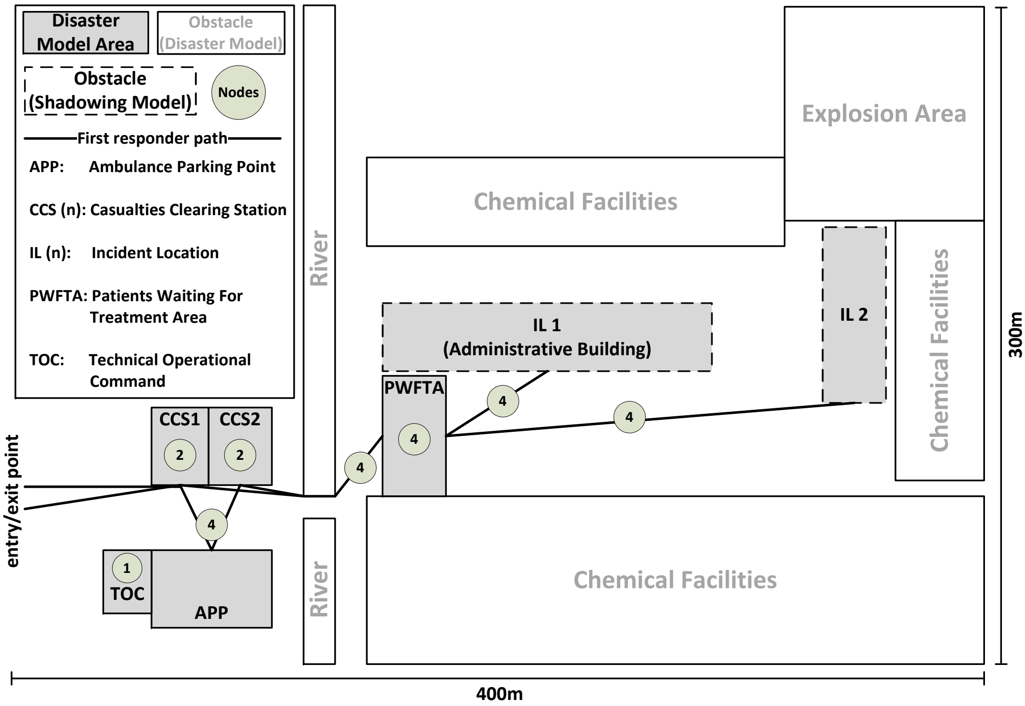

Disaster Model Area
Obstacle (Disaster Model)
Obstacle (Shadowing Model)
Nodes
First responder path
APP: Ambulance Parking Point
CCS (n): Casualties Clearing Station
IL (n): Incident Location
PWFTA: Patients Waiting For Treatment Area
TOC: Technical Operational Command
River
Explosion Area
Chemical Facilities
IL 1 (Administrative Building)
IL 2
PWFTA
CCS1
CCS2
TOC
APP
entry/exit point
1
2
4
300m
400m

Figure 3.2: Overview of the chemical incident scenario.

3.2 Chemical Incident Scenario

This section describes the modeling of an emergency response after an incident in a chemical factory. The scenario is roughly based on the CHEMCO scenario [116] that has been developed within the BRIDGE project. The CHEMCO scenario describes a large-scale incident in a chemical facility where an exploding truck inside the facility causes a major disaster. To reduce the complexity of the scenario, we scaled the scenario down concerning involved first responders and duration of the response operation. In particular, we focus on a search-and-rescue operation inside the chemical facility. In the scenario described in this section, an explosion in the facility has caused two buildings inside the facility to get damaged. Several first responder teams enter these buildings to rescue trapped people and bring them to safety. The mobility of the nodes is modeled according to the disaster area mobility model and the wireless environment that have been described in Section 2.5. The scenario is depicted in Figure 3.2.

3.2.1 Scenario Description

The scenario consists of 25 mobile nodes that represent first responders (e.g., firefighters, paramedics, ambulances) that carry a wireless device. Each first responder is assigned to a tactical area which is positioned in the simulation area (cf. Figure 3.2). In particular, the scenario includes two Incident Locations representing damaged buildings within the chemical facility. Since the two disaster areas are buildings, they also represent wireless obstacles. Each IL contains four nodes which are all transport nodes. Hence, in total eight nodes move between the ILs and the PWFTA. The PWFTA contains eight nodes. Four nodes do not leave the PWFTA, while four additional nodes transport victims to the two CCSs located in front of the facility. Each CCS contains two nodes that do not leave their designated area. Additionally, the scenario includes an APP where four ambulances wait to pick up victims from the CCSs and transport them to a hospital. The simulation area includes an entry and exit point at the left border of the simulation area that represents the location where ambulances arrive at or leave the scene. Finally, the TOC is located in front of the facility and contains one node representing an incident commander.

Since chemical facilities are usually secured against unauthorized access, it is assumed that the chemical facility can only be entered via one gate. This is modeled by placing two obstacles representing a river in front of the facility. Hence, all nodes enter or leave the facility via a bridge in front of the facility. The location of the two buildings (i.e., the incident locations) are set based on the CHEMCO scenario [42, 116]. The movement paths for the transport nodes are illustrated in Figure 3.2.

The chemical incident scenario has some specific properties, since the connectivity of a node depends on its role within the rescue and treatment process. On the one hand, some first responder nodes are very well connected with each other. For instance, the nodes that operate in the CCSs in front of the facility are quite close to the incident commander and only move within their designated area. Similarly, the nodes that are located in the PWFTA are very well connected to each other. On the other hand, the nodes that represent first responders moving inside the ILs are only intermittently connected with the rest of the nodes and may become isolated. Although this is mainly a result of the layout of the chemical facility and hence the arrangement of the tactical areas, such diversities in connectivity of first responders have also been observed during real-world emergency drills [35]. Thus, we argue that this scenario realistically illustrates connectivity problems which

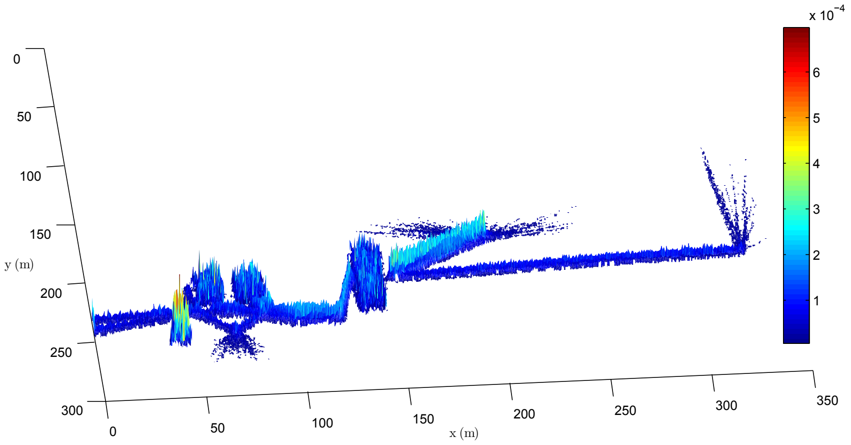


Figure 3.3: Normalized node distribution of the chemical incident scenario.

also regularly happen in in real emergency response scenarios. A more detailed analysis of the connectivity characteristics of the chemical incident scenario is presented in the next section.

The node distribution is visualized in Figure 3.3. The histogram is based on the so called dwell time that has been introduced by Bettstetter and Wagner [20]. The histogram is created by dividing the simulation area into equally sized cells (we use a cell size of 0.5 m x 0.5 m) and measuring the time that nodes are located in a certain cell. The height of a bar is determined by the total amount of time that nodes spent in the according cell. The histogram is normalized so that the sum of the heights of all bars is equal to 1. It can be seen that the TOC offers the highest dwell time, since the TOC area is relatively small and the node does not leave the area. Similarly, the two CCSs and the PWFTA offer a high dwell time. On the other hand, the ILs and the APP are less populated since they only contain transport nodes leaving these areas. The histogram also reveals the paths that are used by the transport nodes in order to move patients between different tactical areas.

3.2.2 Connectivity Characteristics

This section describes a simulation based study that has the goal to evaluate the connectivity characteristics of the chemical incident scenario.

Connectivity metrics

Several metrics are used to assess the connectivity characteristics of the scenario. The first metric is the *number of connected components* which shows how many partitions exist in the network. A connected component represents an 'island of connectivity' where nodes can communicate using end-to-end paths but are separated from other islands. In a connected network only one connected component exists that includes all nodes of the network. If the number of partitions is greater than one, not all nodes can communicate via end-to-end paths. A variation of this metric omits isolated nodes and only counts connected components with at least two nodes.

The *largest connected component (LCC)* is another metric for the connectivity of a network. It represents the size of the largest partition in terms of nodes. In a connected network the largest partition comprises all nodes in the network. Together with the number of partitions, the LCC can express the connectivity characteristics of the network more precisely, since it also gives information about the distribution of nodes in the network.

Another metric for describing the connectivity of a network is the average *number of neighbors*. Two nodes are neighbors if there exists a bidirectional link between them. This metric is also often referred to as *node degree*. The average number of neighbors relates to the robustness of a network. For random networks, it can be shown that a certain minimum number of neighbors per node is needed to achieve a network that is k-connected (i.e., there exist k paths between each pair of nodes) [19]. In general, networks that offer a higher average number of neighbors are better connected, since the probability that an end-to-end path exists between two nodes is higher. However, as only one neighbor can access the wireless medium at a time, a high number of neighbors also has negative effects on the performance of a wireless network.

The connectivity of a network can also be expressed by giving the probability that an end-to-end path exists between a pair of nodes in the network. We refer to this metric as the *connectivity degree (CD)* of a network. The CD is well-suited to estimate the performance of end-to-end routing protocols, since it relates to the probability that a path exists between a pair of nodes. In particular, the CD denotes the probability that two randomly selected nodes are in the same connected component at a given point in time. A connected network has a CD of 1 and a network where all nodes are isolated has a CD of 0. The connectivity degree at a given point in time t is calculated as follows:

$$CD_t = \sum_{P_i \in \mathcal{P}_t} \frac{|P_i|}{|N|} \cdot \frac{|P_i| - 1}{|N| - 1},$$

where N denotes the set of nodes in the network and $\mathcal{P}_t$ denotes the set of partitions that comprise the network at a given time t. $|P_i|$ denotes the number of nodes in one particular partition P_i and $|N|$ the total number of nodes in the network. In other words, CD_t is the expected value for the probability to select two distinct nodes from the same partition.

As the connectivity degree changes over time, the overall average connectivity degree CD of a network is calculated as follows:

$$CD = \frac{1}{|T|} \cdot \sum_{t=1}^{|T|} CD_t,$$

where T denotes the set of samples taken, $|T|$ denotes the number of samples and CD_t the connectivity degree of one sample.

Simulation Setup

The connectivity of a network is often analytically calculated based on a graph representing the network. Two nodes are connected via an edge if the two nodes are within wireless coverage of each other, which is usually assumed to be a circular area with a radius equal to the transmission range. However, since the presented scenario includes a wireless obstacle model this assumption does not hold. In particular, obstacles attenuate signals if they obstruct the line of sight between sender and receiver. To capture these effects while assessing the network connectivity, we take a different approach to gather data about the connectivity of nodes.

To assess the connectivity of the network, simulations in the OMNeT++ simulation framework are performed which use the mobility traces generated by the BonnMotion tool (see Section 3.1). To capture which nodes are connected at a certain point in time, all nodes regularly broadcast packets and log from which nodes they receive packets. To reduce collisions due to the synchronization of broadcasts from different nodes, a jitter is applied to the broadcast interval. Following this approach, two nodes are considered as *connected* if they receive at least one packet from each other within a defined time window. The time window is set to a multiple of the packet creation interval and defines the sampling interval. For instance, if the broadcast interval is set to 0.25 s and the time window is set to 1 s, two nodes are considered to be connected for 1 s if they would receive at least one out of four packets from each other within the last time window. These broadcasts reveal all 1-hop neighbors of a node. Based on the information about direct neighbors, all n-hop paths in the network can be calculated by exploiting transitive relations (e.g., if A is a neighbor of B and B is a neighbor of C, A and C are 2-hop neighbors). All nodes that are connected directly or via an n-hop path form a *connected component* (we use the term *partition* interchangeably). If there is only one connected component, consisting of all nodes in the network, the whole network is *connected.* Otherwise the network is *partitioned.* In contrast to an analysis which presumes homogeneous transmission ranges, this approach also captures effects of the wireless obstacle model.

The simulation parameters are listed in Table 3.1. It is worth noting that the wireless range is varied to simulate different connectivity characteristics and also includes rather unrealistic settings for common wireless networks. In particular, wireless ranges of 100 m up to 200 m are rather unrealistic for an IEEE 802.11 interface in such a challenging environment like a chemical facility. However, the main purpose of the experiments is to evaluate the connectivity characteristics of the network and not to simulate a realistic Wi-Fi network.

Simulation Results

The number of partitions and the size of the largest connected component over the simulation time is shown in Figure 3.4. In general, the connectivity in the network increases for larger transmission ranges. For a transmission range of 25 m (see Figure 3.4a) there are at least two network partitions at any time. This means that the network is never connected. Hence, MANET protocols are not able to establish communication between all pairs of nodes in the network. Although the time for which the network is connected increases for larger communication ranges, the network is partitioned most of the time, even for a transmission range of 200 m (cf. Figure 3.4e). The partitioning of the network is a result of node movements and wireless attenuation that is experienced by nodes working inside the buildings. These nodes are completely isolated or form smaller connected components with other nodes that are located in or nearby the same building.

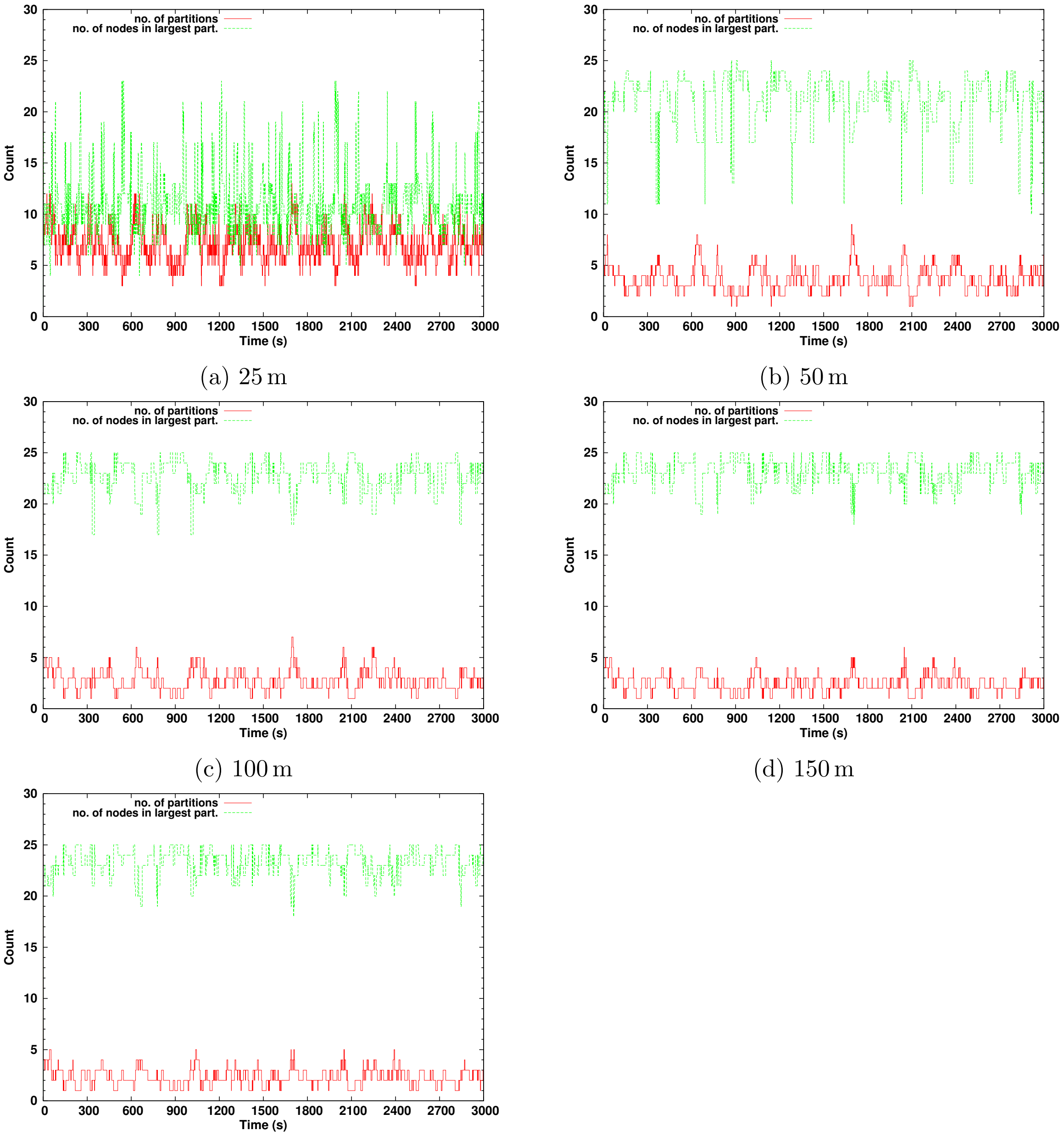
The simulation results show that the connectivity characteristics of the chemical incident

Table 3.1: Simulation parameters

Wireless model	
MAC protocol	802.11 (g)
Propagation model	Free-space path loss ($\alpha = 2$)
Transmission range	from 30 m to 200 m
Wireless obstacle model [112]	
Per-wall attenuation	18 dB
Indoor attenuation	0.5 dB/m
Mobility model [10]	
IL	8/8 (total no. / no. of transporters)
PWFTA	8/4
CCS	4/0
TOC	1/0
APP	4/4
Node speed	1 to 2 m/s
Node speed (vehicles)	5 to 12 m/s
Traffic model	
Type	IP broadcast
Packet size	100 bytes
Send rate	4 packets/s
Jitter	5 ms

scenario are very challenging and that it is very hard to provide a connected network. This shows that the assumption that end-to-end paths between all nodes exist is not always true in such a scenario. Although the network is partitioned most of the time, all nodes are also regularly connected with each other. If nodes wait to transmit packets until such an end-to-end path is available, communication would be possible between any pair of nodes. This shows that DTN routing approaches may be useful in this scenario, although waiting for transmission opportunities would introduce large delays that depend on the mobility of the nodes (i.e., how long it takes until sender and receiver are in the same connected component).

On the other hand, the size of the largest connected components shows that end-to-end routing is suited for large parts of the network. A transmission range of 50 m (see Figure 3.4b) allows the nodes to form a connected component that contains the majority of



(a) 25 m

(b) 50 m

(c) 100 m

(d) 150 m

(e) 200 m

Figure 3.4: Number of connected components and number of nodes in largest partition over time for varying transmission ranges.

nodes most of the time. For transmission ranges of 100 m and more, the largest connected component contains more than 20 nodes (i.e., more than 80% of all nodes) most of the time (cf. Figure 3.4c, Figure 3.4d and Figure 3.4e).

The average number of connected components is shown in Figure 3.7. It can be seen

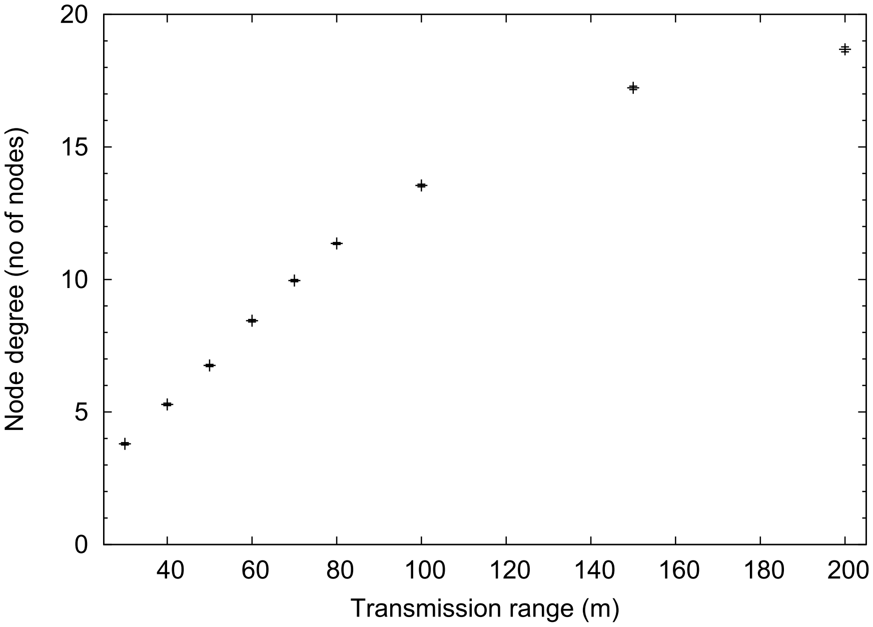


Figure 3.5: Node degree for varying transmission ranges.

that the number of connected components clearly decreases between transmission ranges from 30 m up to 70 m. Further increasing the transmission range does not affect the number of partitions significantly. The size of the largest connected component behaves similarly, as shown in Figure 3.8. The LCC only increases significantly for lower transmission ranges, until to 80 m where the nodes in the PWFTA, APP, CCSs and the TOC are within the same connected component most of the time. However, increasing the transmission range any further does not affect the LCC significantly. The CD of the chemical incident scenario is depicted in Figure 3.9. For a transmission range of 30 m the CD is less than 0.4 since several partitions exist in the network. It doubles at a transmission range of 60 m but then only slightly increases further. For a transmission range of 200 m the CD is about 0.85.

The aforementioned results concerning the number of connected components, the LCC and the CD show that the network connectivity can only be improved significantly for transmission ranges up to about 80 m in the given scenario. Using higher transmission ranges of up to 200 m does not significantly improve the connectivity of the network. In particular it is not possible to connect all nodes in the network. On the other hand, increasing the transmission range also increases the probability that transmissions collide since more nodes share the same access medium. Figure 3.5 and Figure 3.6 show the average number of neighbors for varying transmission ranges and how the number of neighbors

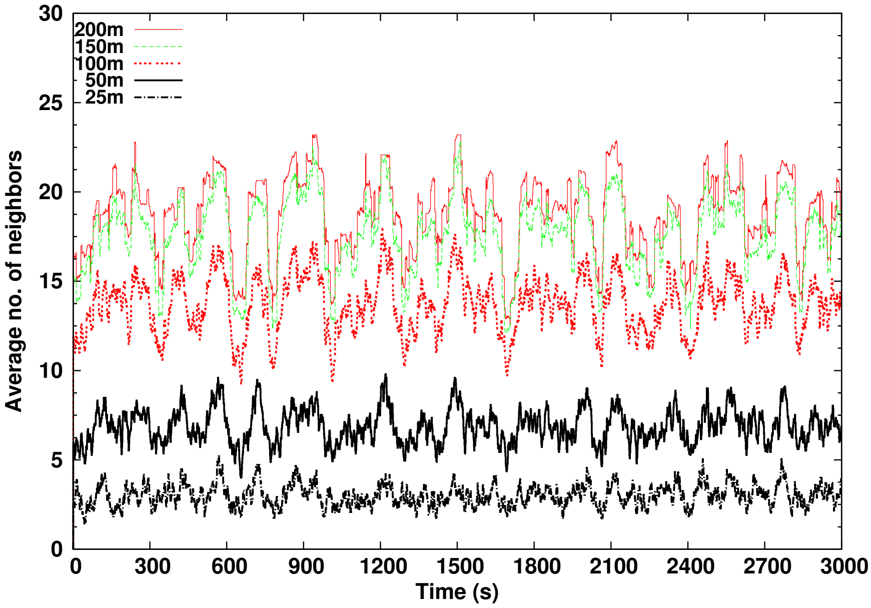


Figure 3.6: Node degree over time for varying transmission ranges.

varies over time. It can be seen that the average node degree changes significantly, even for transmission ranges greater than 80 m. For instance, for a transmission range greater than or equal to 150 m the average number of neighbors is about 18. Hence, 18 nodes compete in order to access the wireless medium and these nodes all share the available bandwidth. This means that the majority of nodes cannot transmit data concurrently since they are in the same collision domain, which limits the total network capacity. Hence, although larger transmission ranges have a positive effect on the connectivity of the network, it may be necessary to limit the transmission range to reduce collisions in the dense parts of the network. In this particular scenario, a transmission range of 60 m up to 100 m offers a good tradeoff between network connectivity and network resource contention.

3.2.3 Discussion

The presented simulation results show that the chemical incident scenario is challenging in terms of connectivity. Some nodes are only intermittently connected with the rest of the network. Obviously, this is partially a result of the scenario setup (i.e., IL2 is rather isolated from the other tactical areas). However, it is fair to assume that in many real world incidents similar isolated areas will exist. For instance, networks from real-world emergency drills showed similar properties [35]. Increasing the transmission range (i.e.,

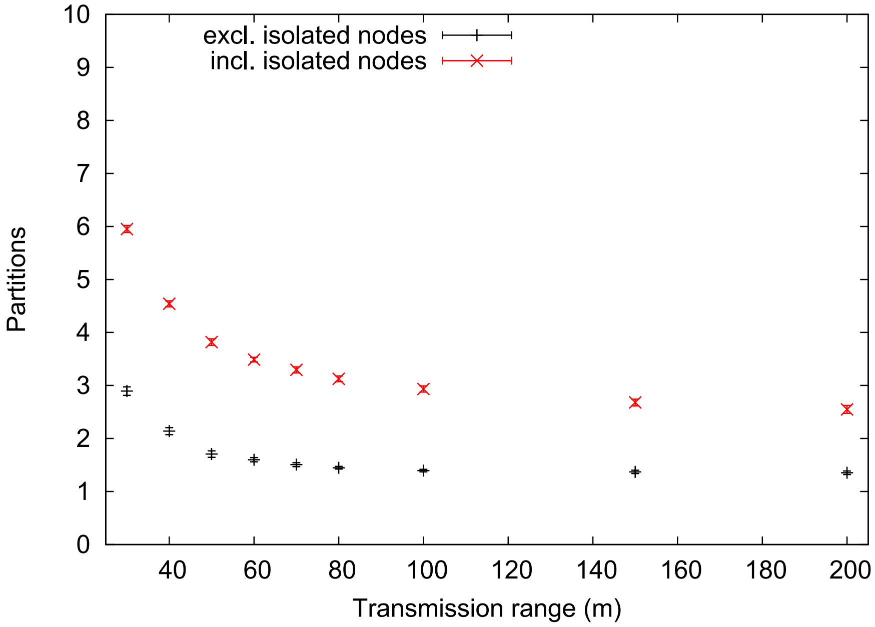


Figure 3.7: Number of connected components for varying transmission ranges.

by increasing the transmission power) is one way to decrease the number of partitions and create connected networks [19]. However, larger transmission ranges also reduce the network capacity, especially in the dense parts of the network. Hence, we argue that one cannot always assume connected networks in emergency response scenarios. Instead, other routing mechanisms such as DTN routing may be needed in such scenarios. In particular, DTN routing allows nodes to bridge network partitions by exploiting the mobility of the nodes instead of relying on large transmission ranges.

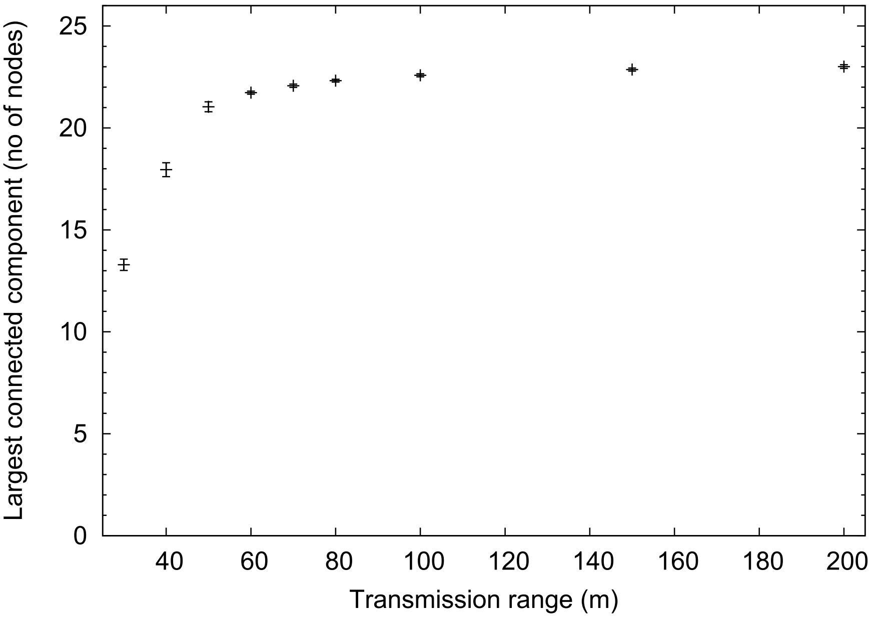


Figure 3.8: Largest connected component for varying transmission ranges.

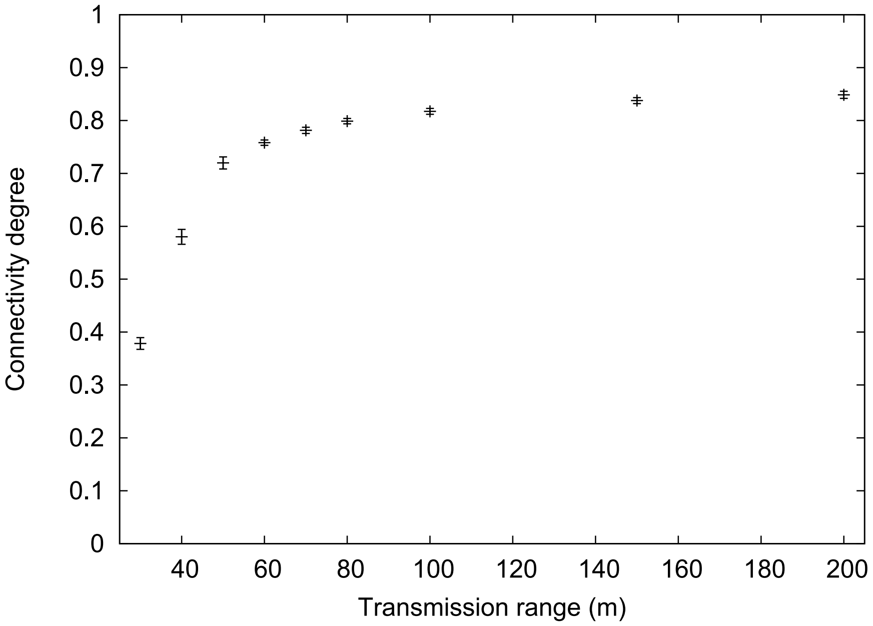


Figure 3.9: Connectivity degree for varying transmission ranges.

3.3 Full-scale Emergency Response Exercise Scenario

The BRIDGE project could participate in a full-scale exercise at the Risavika harbor near Stavanger, Norway. A full-scale exercise tries to simulate an emergency situation as realistically as possible. A full-scale exercise is performed in the field and includes the same resources and procedures that would also be used in a real emergency response.

3.3.1 Scenario Description

The Risavika exercise simulated a terror attack that caused a mass-casualty disaster at a harbor. The terror attack involved bomb explosions and shootings at different locations at the harbor, as well as a truck explosion in front of an liquefied natural gas factory that is located nearby. In particular, the exercise scenario assumed that terrorists entered the ferry terminal and a passenger ship that docked at the terminal, where they shot people and detonated a bomb. These events resulted in an assumed number of about 100 injured and dead people. The scenario comprised different locations where victims were located and needed to be evacuated or treated by first responders. In total, over 100 police officers, firefighters and paramedics participated in the exercise.

The exercise can be separated into three basic phases. In a first phase, four terrorists enter the harbor area and cause harm at three different locations within the area. According to the exercise description, it is assumed that no terrorist remains at the scene. In a second phase, the police secures the area around the harbor and makes sure that there are no threats for other first responder organizations. Afterwards, in a third phase, firefighters and paramedics are allowed to enter the scene. The first two phases are out of scope and are not modeled in the scenario that is described in this section. Instead, the modeled scenario begins after paramedics and firefighters have arrived at the scene and includes the process of evacuating people and the initial treatment of patients.

We used the disaster area mobility model to model the movement of first responders on the scene. This involves to define tactical areas including their location, shape and the node assignment to these areas. The exact sizes and shapes of tactical areas could not be assessed during the exercise. Thus, the presented values are estimations based on our observations on the scene and the scenario description of the full-scale exercise. To define the size and location of the tactical areas, we pursued the following approach: First, we used an online map service to get an areal image of the Risavika harbor and the latitude (lat) and

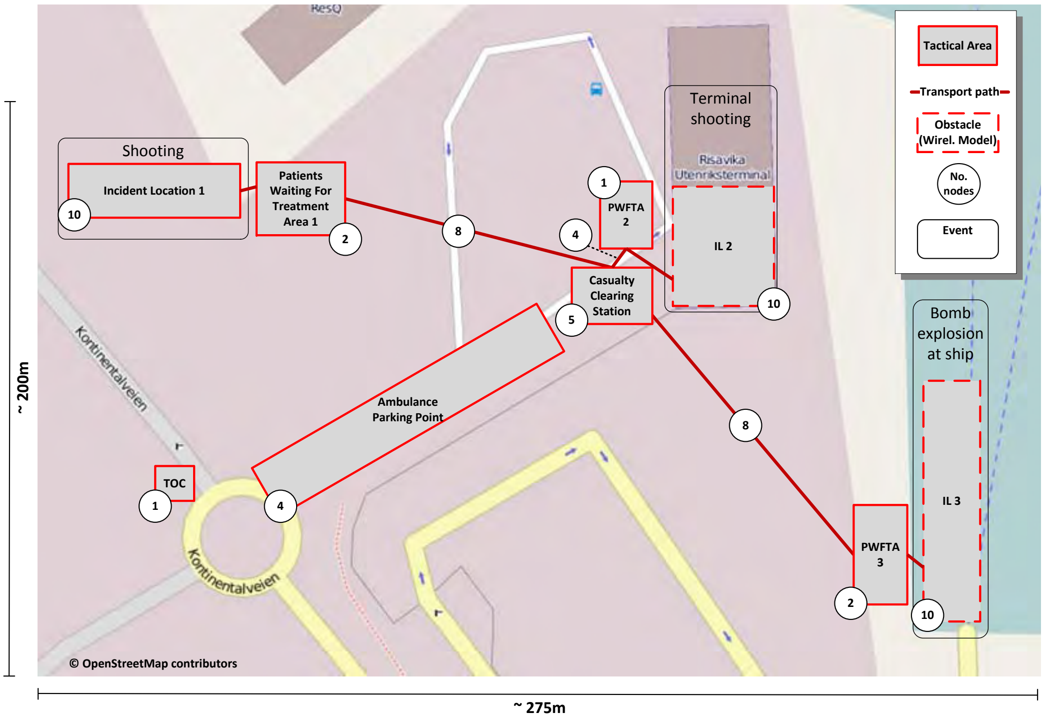


Figure 3.10: Overview of the Risavika exercise scenario.

longitude (lon) coordinates of important locations in the exercise. This includes the terminal building or the location where the ship was located during the exercise. We then arranged all tactical areas of the disaster area model according to the exercise descriptions and our on-scene observations of the full-scale exercise. The lat/lon coordinates received from the map service were then converted to XY coordinates that could be used to model the scenario based on the disaster area mobility model. Additionally, the number of first responders per tactical area was estimated based on our observations and the exercise scenario descriptions. The terminal building and the ship were modeled as wireless obstacles.

The resulting scenario is depicted in Figure 3.10 and shows the locations of all tactical areas and the number of nodes within each area. It consists of three Incident Locations that represent the aforementioned incidents. One Incident Location (IL 3) represents the ship where a simulated bomb explosion takes place. In the course of the exercise a training ship has been used, instead of the ferry that usually docks at the terminal. Thus, first responders had to enter the ship via a gangway next to the terminal, instead of using the gangway that directly leads into the terminal building. IL 3 reflects this and is placed where the training ship was located during the exercise. Another Incident Location (IL 2) is the entrance hall of the terminal building where a shooting was simulated. The third Incident Location (IL 1) is an area at a parking lot in front of the terminal building where another simulated shooting takes place. Near to each IL, a PWFTA is placed. Additionally, we modeled one CCS that is located in front of the terminal building, since many designated victims were picked up by ambulances from this location. The APP is modeled along the driveway to the terminal building. Finally, the TOC is located next to a roundabout at the entrance of the harbor area. A difference to the full-scale exercise is that ambulances are not part of the modeled scenario. The main reason for excluding ambulance is that we are mainly interested in the movement of first responders on the scene and their communication with the local incident command post. Hence, the traces do not include ambulances that leave the scene and come back later or even do not return to the incident scene.

It is important to note that we needed to change one aspect of the disaster area mobility model in order to model the exercise more realistically. According to the original definition of the disaster area mobility model [12], transport nodes choose their target area randomly. In the example of the exercise scenario, a transport node that is assigned to the IL 3 in front of the ship could select and move to any PWFTA that is on the scene, before coming back to IL 3. We changed the behavior of transport nodes so that instead of randomly choosing a target area, transport nodes always use the closest target area as their destination. For example, a transport node that is assigned to IL 3 on the ship transports all patients to PWFTA 3 in front of the ship but will not use any other PWFTA further away. This change has been performed since that behavior could also be observed during the exercise. We believe that this behavior is more realistic in situations with several hotspots, since first responders usually avoid using unnecessary long transport paths.

The node distribution is shown in Figure 3.11 (see Section 3.2.1 for a description of how the node distribution is calculated). It can be seen that the areas near the three disaster events provide the highest density of nodes. These are the locations of the ILs and the PWFTAs where many nodes are located. The locations in front of the terminal building are most populated. The area where the TOC is located also provides a relatively high dwell time, since the node in the TOC remains there throughout the entire simulation. The histogram also reveals the paths which are used by the transport nodes to move patients between the different tactical areas.

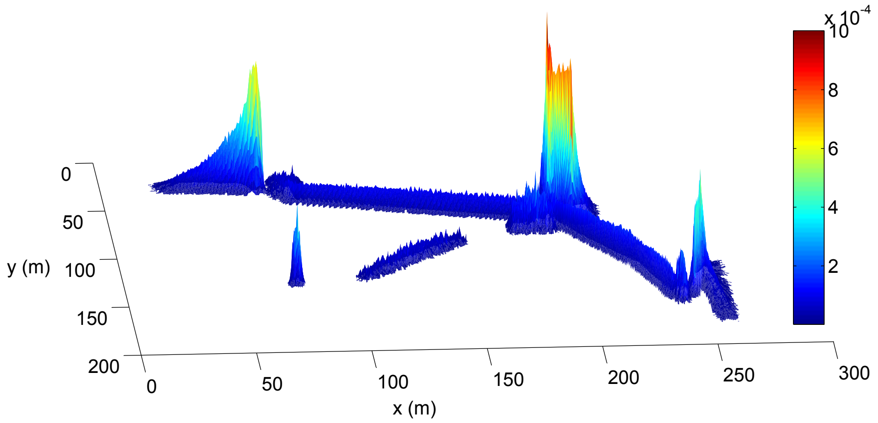


Figure 3.11: Normalized node distribution of the Risavika exercise scenario.

3.3.2 Connectivity Characteristics

This section describes a simulation based study that has the goal to evaluate the connectivity characteristics of the full-scale exercise scenario.

Metrics

The connectivity is assessed using the same metrics as in the previous evaluation (see Section 3.2.2), namely: number of partitions, largest connected component (LCC), node degree and connectivity degree (CD).

Simulation Setup

The setup of the evaluation is following the same approach as the previous evaluation of the connectivity characteristics of the chemical incident scenario. The mobility is modeled with the BonnMotion tool and the resulting scenario is imported into the OMNeT++ simulator to create connectivity traces. A more detailed description can be found in Section 3.2.2. Important simulation parameters are listed in Table 3.2.

We evaluated the connectivity characteristics for transmission ranges from 30 m to 80 m. One may argue that for outdoor envronments Wi-Fi networks usually provide higher transmission ranges than 80 m. However, these values have been chosen since observations during

Table 3.2: Simulation parameters

Wireless model	
MAC protocol	802.11 (g)
Propagation model	Free-space path loss ($\alpha = 2$)
Transmission range	from 30 m to 80 m
Wireless obstacle model	
Per-wall attenuation (terminal)	18 dB
Indoor attenuation (terminal)	0.5 dB/m
Per-wall attenuation (ship)	50 dB
Indoor attenuation (ship)	1 dB/m
Mobility model	
IL1	10/10 (total no. / no. of transport nodes)
PWFTA1	10/8
IL2	10/10
PWFTA2	5/4
IL3	10/10
PWFTA3	10/8
CCS	5/0
TOC	1/0
APP	4/0
Node speed	1 to 2 m/s
Traffic model	
Type	IP broadcast
Packet size	100 bytes
Send rate	4 packets/s
Jitter	5 ms

the Risavika exercise have shown that these values are reasonable. In particular, these values are based on experiences with the BRIDGE Mesh that has been deployed during the exercise and did not provide stable links for higher transmission ranges. Similar values have also been observed for smartphones that used the Help Beacons application to transfer distress signals to the local command post.

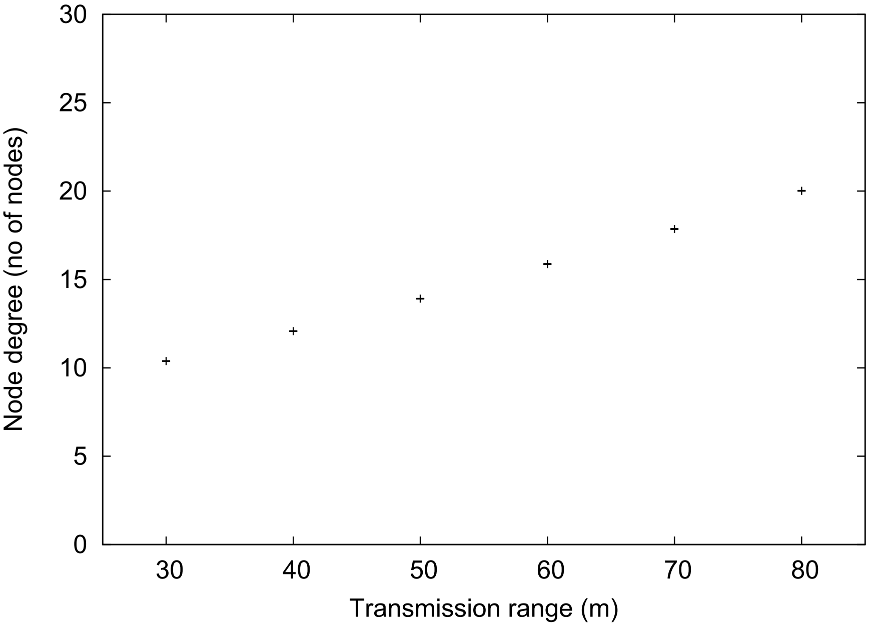


Figure 3.12: Node degree for varying transmission ranges.

Simulation Results

The average node degree (cf. Figure 3.12) shows that the network is relatively well-connected in terms of neighboring nodes. Depending on the transmission range, each node has 10 to 20 neighbors on average. However, since nodes are not equally distributed and some nodes also work indoors, the network is usually not connected. For larger transmission ranges, the size of the largest connected component converges to around 60 (see Figure 3.13). Similarly, the number of partitions is always greater than two, as depicted in Figure 3.14.

The CD for varying transmission ranges is depicted in Figure 3.15. The CD is about 0.45 for a transmission range of 30 m. It increases notably up to a transmission range of 60 m, where the CD is about 0.85. For larger ranges (i.e., 70 m and 80 m), the CD only slightly increases to about 0.88.

The size of the largest partition in the network and the number of partitions over time are shown in Figure 3.16. For a transmission range of 30 m the network is never connected and the size of the LCC varies greatly over time (cf. Figure 3.16a). Similar variations in the connectivity of the network can be seen for transmission ranges of 40 m and 50 m (cf. Figure 3.16b and Figure 3.16c). For larger transmission ranges the size of the LCC is more

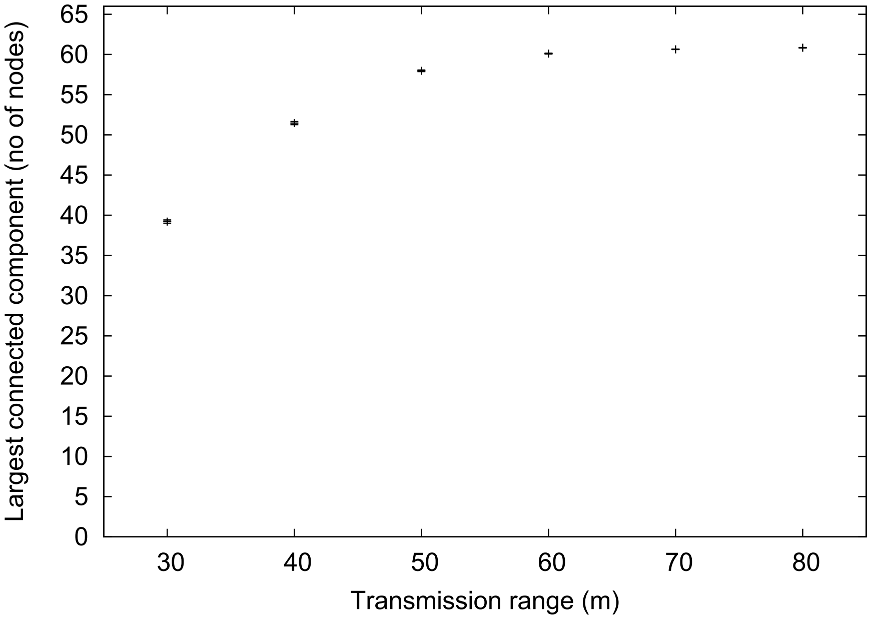


Figure 3.13: Largest connected component for varying transmission ranges.

stable, although the network still gets disconnected regularly (see Figures 3.16d, 3.16e and 3.16f).

3.3.3 Discussion

This section described modeling a full-scale emergency response exercise that has been carried out in a harbor in Norway. In total more than 100 first responders from different organizations participated in the exercise. We modeled the rescue phase of the exercise where people from three different incident areas are treated. The scenario that has been modeled uses the disaster area mobility model that has also been used to model the chemical incident scenario described earlier in this chapter. This mobility model proved to reproduce the movements of the first responders in a realistic way since the separation-of-room concept could also be observed during the exercise. However, we had to change the model in one aspect to better reflect the behavior of transport nodes. Based on this scenario, a connectivity evaluation has been performed. Results showed that the connectivity of the network is diverse and challenging, in particular, the fact that some parts of the network are rather dense and well-connected, whereas other parts are only intermittently connected.

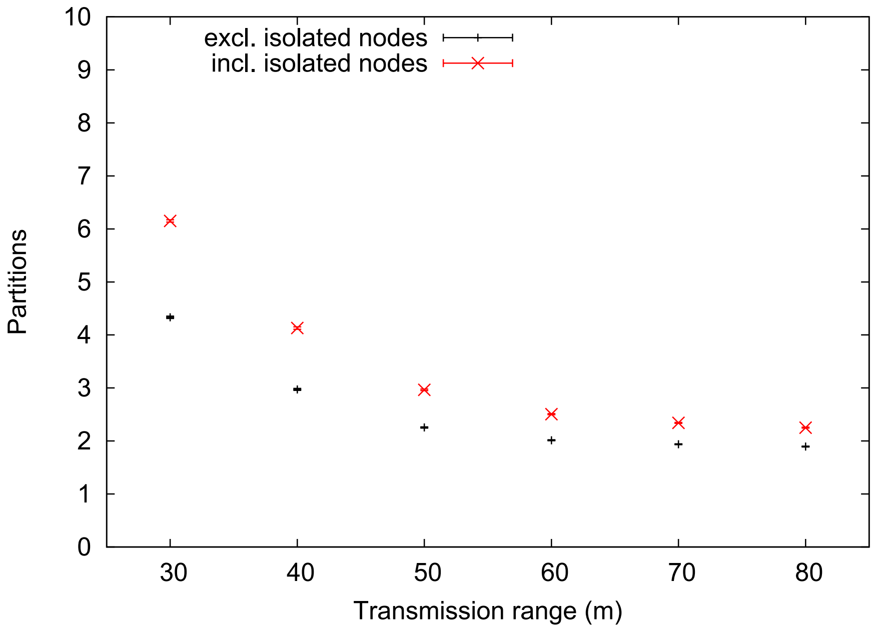


Figure 3.14: Number of partitions for varying transmission ranges.

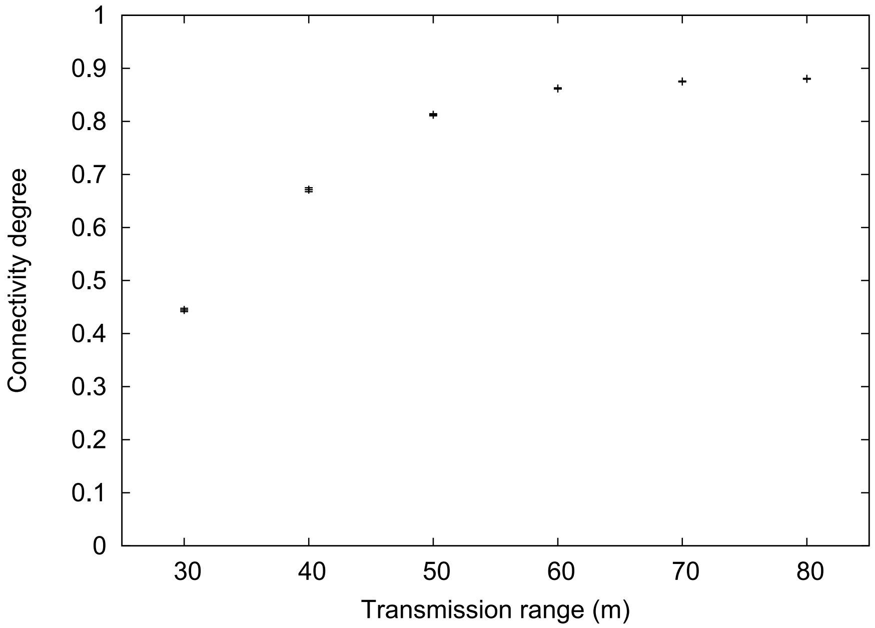
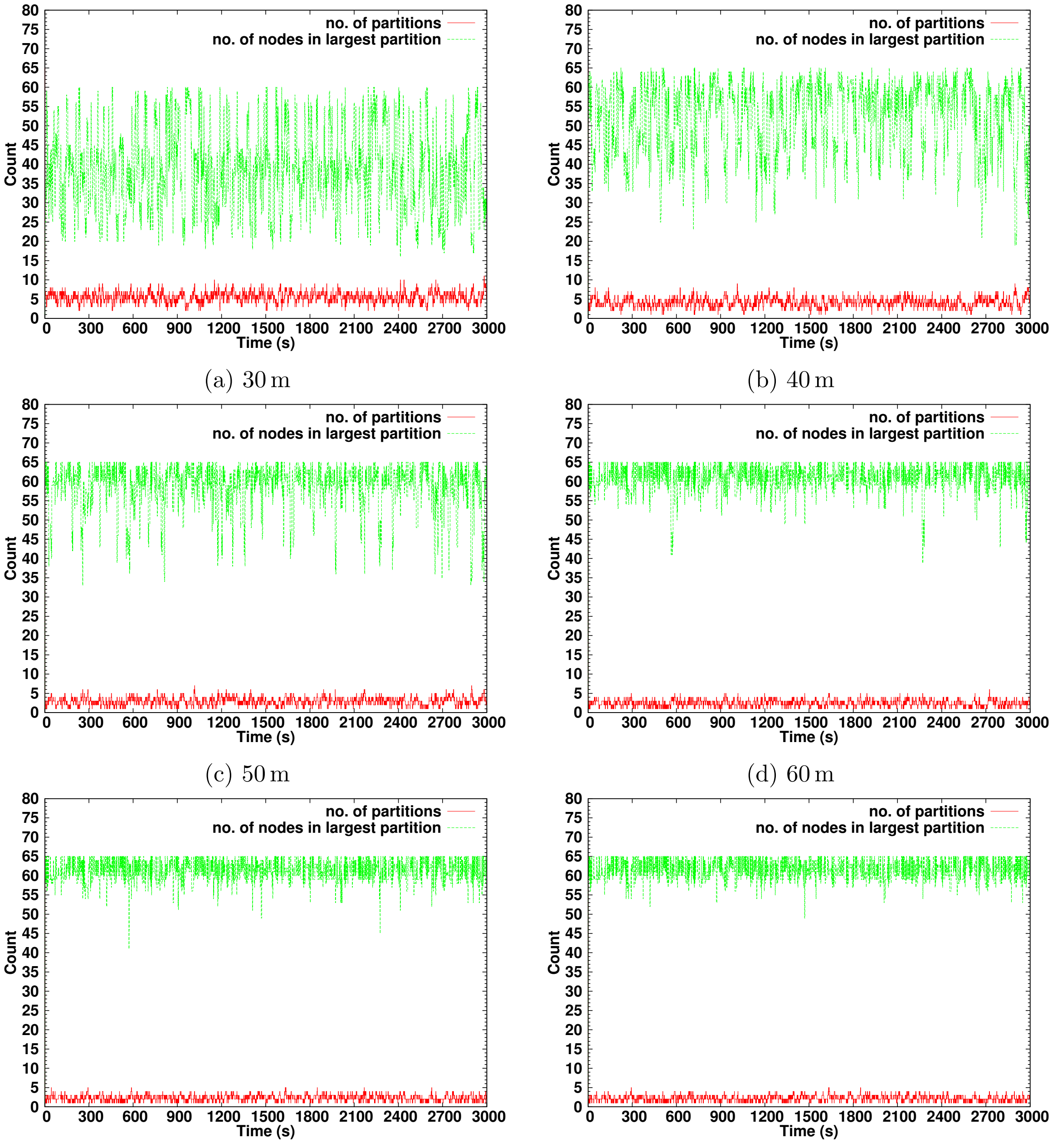


Figure 3.15: Connectivity degree for varying transmission ranges.



(a) 30 m

(b) 40 m

(c) 50 m

(d) 60 m

(e) 70 m

(f) 80 m

Figure 3.16: Connectivity characteristics of the Risavika scenario in terms of connected components for varying transmission ranges.

3.4 Evaluation of MANET Routing Protocols in the Chemical Incident Scenario

In the previous sections we have presented two emergency response scenarios and evaluated their connectivity characteristics. This section presents an evaluation of several state-of-the-art MANET routing protocols in the chemical incident scenario. The evaluation includes the two proactive protocols OLSR and BATMAN and the two reactive protocols AODV and DYMO, which have been described in Section 2.2. The purpose of this evaluation is to show how the different MANET routing protocols perform in a disaster scenario. This is different to evaluations that use generic scenarios and evaluate how the protocols perform using different parameter sets for the routing protocols, or under different mobility or traffic models [25, 79].

3.4.1 Scenario Description and Simulation Setup

The evaluation uses the chemical incident scenario that has been described in Section 3.2. The simulations were performed using the INETMANET framework [8] for the OMNeT++ network simulator. The INETMANET framework provides implementations for several MANET routing protocols, including AODV, DYMO, BATMAN and OLSR. For the OLSR protocol the expected transmission count (ETX) metric was used instead of hop count. INETMANET includes two implementations of the DYMO protocol and we used the more recent DYMO-FAU implementation. The DYMO specification suggests to limit the buffer size to 50 packets and delete packets that are older than five seconds. We added the same constraints to the AODV packet buffer. Apart from these modifications, all experiments were performed using the default parameters of the respective MANET routing protocol. All wireless nodes were modeled as IEEE 802.11g nodes with a maximum transmission rate of 54 Mbit/s and a transmission range of 100 m. Every experiment lasted 3000 seconds and was repeated 10 times.

In order to assess the performance of the routing protocols a traffic model is needed that describes the characteristics of the data traffic that is introduced by the nodes. To simulate this network workload, every node sends UDP packets following an on/off traffic pattern to the node that is located in the technical operational command center (i.e., node 0 in the scenario depicted in Figure 3.17). The on time is chosen from a random interval

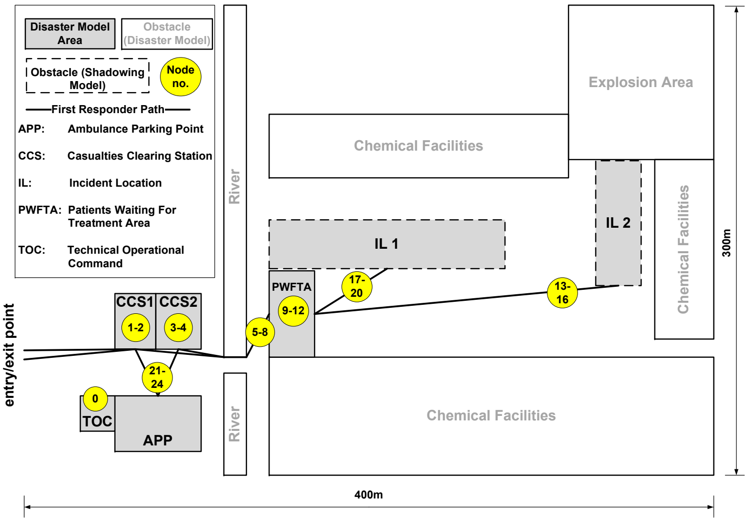

Disaster Model Area
Obstacle (Disaster Model)
Obstacle (Shadowing Model)
Node no.
First Responder Path
APP: Ambulance Parking Point
CCS: Casualties Clearing Station
IL: Incident Location
PWFTA: Patients Waiting For Treatment Area
TOC: Technical Operational Command
River
Explosion Area
Chemical Facilities
IL 1
IL 2
PWFTA
17-20
13-16
9-12
5-8
CCS1
CCS2
1-2
3-4
21-24
0
TOC
APP
entry/exit point
300m
400m

Figure 3.17: Chemical incident scenario

between 3 seconds and 7 seconds. The off time is chosen from an interval between 5 seconds and 10 seconds. During on time 10 packets/second with a packet size of 1024 bytes are sent. This simple traffic pattern simulates updates from the first responders that are sent to the incident commander located in the TOC. Such updates could include data from vital or other sensors or short text messages that describe the current situation of a first responder.

Three well-known metrics are used to evaluate the performance of the protocols: packet delivery ratio (PDR), hop count and end-to-end delay. The PDR describes the fraction of packets that are retrieved by the destination. The hop count is a measure for the length of the path (i.e., the number of nodes that forward a packet). The end-to-end-delay expresses the time a packet needs to travel from source to destination.

3.4.2 Evaluation Results

One of the most important metrics of a routing protocol is the packet delivery ratio. Figure 3.18 shows the average PDR of the evaluated routing protocols. AODV achieves an average PDR of 89%, followed by OLSR with 83%, BATMAN with 81% and DYMO with 72%. Although the overall packet delivery ratio is above 70% for all protocols, some nodes experience significantly higher packet loss rates. Evaluating the PDR for every node (i.e., how many packets of a certain node arrive at the operational command center) shows the differences between the nodes outside the chemical facility and the nodes working inside the facility. Some of the latter nodes also temporarily operate indoors. Basically, all nodes that

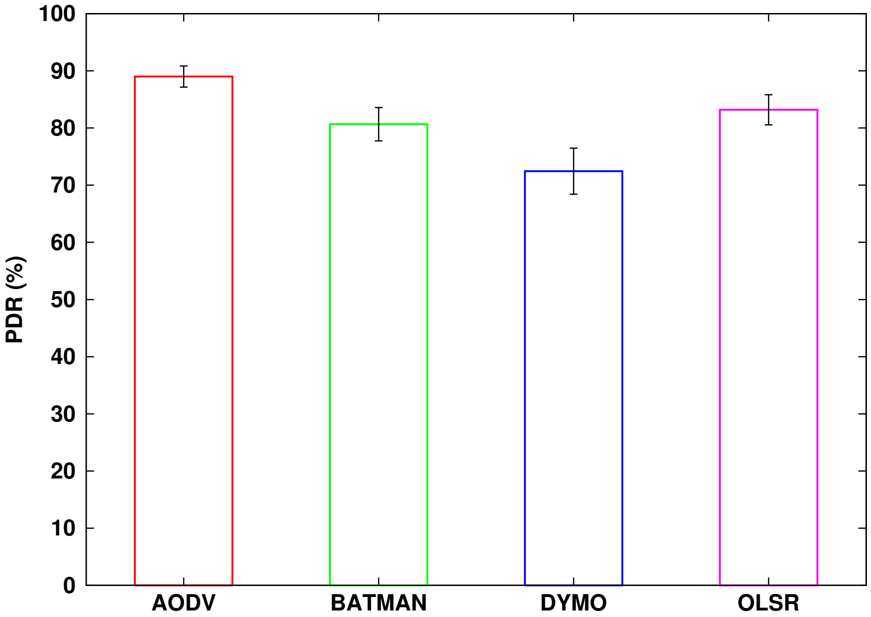


Figure 3.18: Average packet delivery ratio of the evaluated routing protocols.

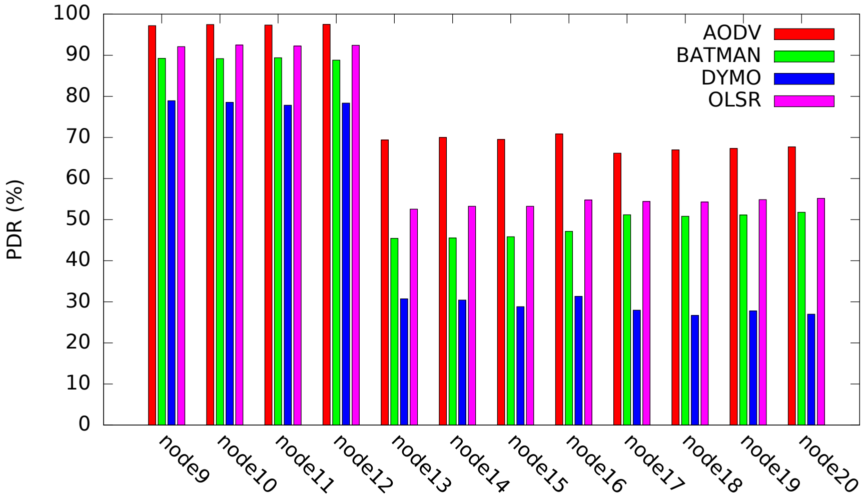


Figure 3.19: Average packet delivery ratio of the mobile nodes operating inside the facility.

operate in front of the facility (i.e., nodes 1-4 and 21-24) achieve a PDR of nearly 100%, whereas the PDR of the nodes within the facility is much lower. Figure 3.19 shows the PDR of the nodes that are located within the chemical facility. These nodes experience a packet loss rate of up to 70% (in the case of DYMO). This high packet loss is caused by higher mobility and by temporary work indoors (i.e., nodes 13-20 enter buildings). The performance of the routing protocols also differs more for these intermittently connected nodes. AODV

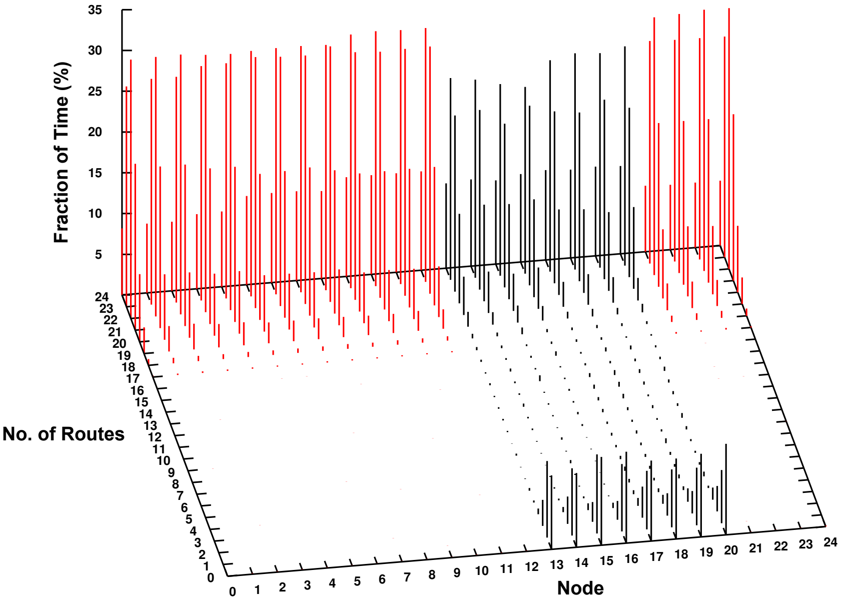


Figure 3.20: Connectivity established by OLSR (i.e., number of routes reported by OLSR).

accomplishes to deliver twice as many packets as DYMO, the worst performing protocol for these nodes and about 50% more than OLSR, the second best protocol. In [9] similar differences between the PDR of AODV and DYMO are reported. One reason for the loss of packets when using DYMO is that the protocol may not find a path within 5 s which causes the packet to be dropped from the packet buffer before it can be forwarded. However, as AODV and DYMO are both reactive and have similar path finding and repair mechanisms, the difference in the packet delivery ratio should not be that significant and may also be caused by flaws in the implementation of DYMO in the OMNeT++ simulator.

The realistic first responder movements and the hybrid indoor/outdoor environment results in a network that is diverse in terms of connectivity. The evaluated proactive protocols BATMAN and OLSR calculate routes to all nodes in the network. The generated routing tables can be used to show the connectivity in the network, as perceived at the network layer. Figure 3.20 depicts how many routes are reported by OLSR for which fraction of simulation time. The figure shows that some nodes in the network (i.e., nodes 13 to 20) are not connected to any other node for about 10% of the simulation time (i.e., about 300 seconds). Moreover, these nodes are connected to less than three other nodes for about 25% of the simulation time. These results clearly show that the network is inhomogeneous in terms of connectivity. The network regularly becomes partitioned and is rarely connected

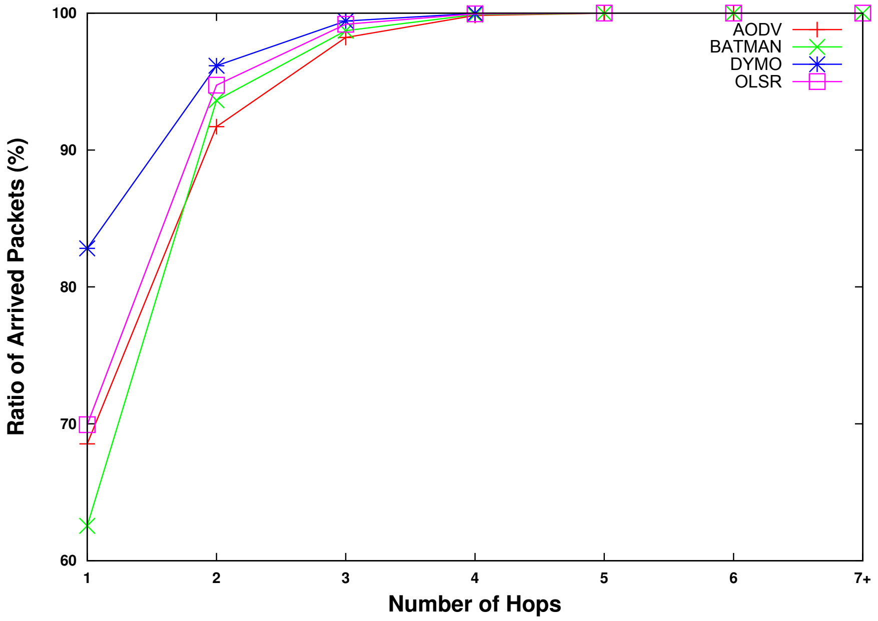


Figure 3.21: Cumulative distribution function of the hop count.

(i.e., OLSR reports routes to all other nodes in the network for less than 15% of the time).

Figure 3.21 shows the cumulative distribution function (CDF) of the hop count. In general, the paths in the network are very short. All protocols delivered over 90% of the packets within two hops. The reactive protocols AODV and DYMO delivered all packets within six hops. In OLSR and BATMAN some successfully delivered packets experienced a hop count of up to 28 for OLSR and up to 32 (i.e., the maximum TTL set at the IP layer) for BATMAN. This is an indication that OLSR and BATMAN produce temporary rooting loops. Such routing loops occur if the routing tables are not consistent and packets traverse repeatedly the same nodes, until the routing tables converge or the packets are dropped at the IP layer (i.e., the time-to-live expires). Consequently, routing loops decrease the packet delivery ratio. DYMO delivers most of the packets within one hop. However, this may result from DYMO's low PDR for the nodes that are farther away (i.e., more than one hop) from the command center.

Moreover, the packet delivery delay has been evaluated. In general, all routing protocols achieve similar results and deliver packets with very low delays. As AODV and DYMO buffer packets until a route is found, some packets experience higher delays. However, as all packets have the same destination, only the first few packets within an on-period are delayed, unless mobility causes route failures.

3.4.3 Related Work

Although disaster response operations are often used in research papers to motivate the need for mobile ad-hoc networks, it has been little researched how standard MANET routing protocols perform in emergency scenarios.

Johansson et al. [59] studied three MANET routing protocols (DSDV, AODV and DSR) under different scenarios, including a disaster area scenario. The disaster scenario consists of three groups of nodes, representing three rescue teams and two fast moving nodes that represent vehicles. Additionally, it contains obstacles that block the movement of nodes and constrain which nodes can communicate. However, compared to our work, no disaster-specific mobility model was used but members of the rescue teams move randomly and vehicles follow a predetermined path. The obstacle model is also less precise. An obstacle just completely blocks communication if it intersects the line-of-sight between two nodes. On the contrary, the obstacle model used in our work calculates the signal attenuation of an obstacle based on real world measurements.

Reina et al. [103, 104] used the same disaster area mobility model that we used, to evaluate the performance of three reactive routing protocols, namely AODV, DSR and a modified version of AODV that supports multi-path routing, called AOMDV. The results show that AODV performs best among the evaluated protocols in terms of packet delivery ratio. However, the evaluation also shows that the different tactical areas have diverse connectivity and mobility characteristics and that the low connectivity of disaster scenarios provides a challenge for all evaluated end-to-end-protocols. These results are in line with the evaluation results that have been presented in this section.

Wister et al. [127] evaluated if AODV and DYMO are appropriate routing protocols for rescue task applications. However, the evaluations were performed in a generic scenario. Nodes are randomly placed in the simulation area and move according to the random way point mobility model. The authors evaluated the protocols based on packet delivery ratio, throughput, routing overhead and energy consumption. Although the authors concluded that DYMO is more appropriate than AODV for rescue tasks in disaster situations, the evaluated scenario is too generic for a reliable conclusion. Our work shows that a more realistic emergency response scenario exhibits some distinct features that are not covered by a generic scenario.

3.5 Conclusion

This chapter contributes to the research goals of this thesis by providing a modeling framework to realistically model emergency response scenarios. In particular, we use a realistic mobility model that mimics the movements of first responders on a disaster scene. Additionally, we also captured the effects of obstacles that attenuate wireless signals. Based on this framework, two emergency response scenarios have been presented. The characteristics of these scenarios have been shown, which is another contribution towards the research goals.

Emergency response scenarios are a promising application domain for ad-hoc networking since this type of networking is independent of fixed communication infrastructure. However, results showed that opportunistic networks created by first responders are challenging, since they are diverse in terms of connectivity. A performance evaluation of several state-of-the-art MANET routing protocols in a realistic emergency response scenario showed that some nodes are severely affected by the fact that MANET routing cannot cope with a partitioning of the network. Although increasing the transmission range is a means to reduce the number of partitions in the network, it would also introduce more collisions in the dense parts of the network. One possible solution to improve the routing performance in emergency response scenarios is to adopt ideas from delay-/disruption-tolerant networking (DTN). The next chapter introduces approaches that combine routing approaches from the MANET and the DTN domains.

CHAPTER 4 Combined Mobile Ad-hoc and Delay-/Disruption-Tolerant Routing

In the previous chapter we have shown the connectivity characteristics of wireless networks in two emergency response scenarios. Results showed that the networks are diverse in terms of connectivity. On the one hand, the networks get partitioned regularly. On the other hand, some parts of the networks are well-connected. Hence, we argue that neither end-to-end routing (MANET routing) nor routing for delay-/disruption networking (DTN routing) may suffice in such scenarios but a combination of these approaches is needed. This chapter presents state-of-the-art routing approaches that integrate ideas from MANET and DTN routing in order to provide data delivery in diverse networks. We contribute to this area of research by presenting two routing protocols that have been developed based on the findings of the previous chapter and current state-of-the-art protocols from this domain. The first routing protocol integrates packet buffering into a MANET routing protocol in order to bridge disruptions in the network. The main idea behind this approach is to rely on information that is gathered by a proactive MANET protocol to detect such disruptions in the network. In case a sender detects that the network is partitioned and the destination cannot be reached instantly, packet buffering is used in order to prevent packet loss. This hybrid approach works with any proactive MANET routing protocol without requiring any changes of the MANET protocol (e.g., no new control messages or changes to existing control messages are needed). However, the downside of this hybrid approach is that it can only bridge temporal disruptions and fails if the sender and the receiver are never in the same connected component. Hence, we present an extended version of the protocol that is able to determine custodian nodes based on the information collected by the proactive MANET protocol. In particular, custodians are selected based on information from the routing table that is periodically calculated by the MANET routing protocol. Based on this information, nodes can decide to either buffer messages and wait for better transmission opportunities or transfer the message to a custodian node.

This chapter is structured as follows: Section 4.1 gives an introduction and describes why hybrid MANET/DTN approaches are beneficial for some scenarios. Section 4.3 gives an overview of state-of-the-art approaches for hybrid MANET/DTN routing, before Section 4.2 presents a classification of these approaches. Afterwards, we present two routing protocols that combine MANET and DTN routing. The first protocol integrates packet buffering into MANET routing in order to bridge temporary partitioning of the network (see Section 4.4). The second approach (see Section 4.5) also provides means to bridge permanent disruptions by opportunistically selecting custodian nodes in cases where end-to-end paths are not available. Finally, Section 4.6 concludes the chapter.

Please note that this chapter is based on previously published work. In particular, the state-of-the-art and classification of combined MANET/DTN routing schemes that are presented in Section 4.3 and Section 4.2 have been published in [98]. The routing approach that is described in Section 4.4 has been published in [97]. Finally, the extended version of this approach described in Section 4.5 has been published in [99].

4.1 Introduction

MANET and DTN routing protocols have been designed with different network connectivity characteristics in mind. On the one hand, MANET routing protocols assume end-to-end paths and hence rather dense networks where such end-to-end connections can usually be established. On the other hand, DTN routing protocols usually assume that the network is very sparse and contacts between nodes are rare. This also implies that the existence of multi-hop paths and connected components that include several nodes are seen as rather uncommon.

Since MANET and DTN routing protocols address networks with different connectivity characteristics, neither MANET nor DTN routing protocols are suited for networks that are very inhomogeneous. In this context inhomogeneous means that networks are partitioned but also provide well-connected regions or that the connectivity characteristics of the network change significantly over time. While MANET routing is unable to provide an inter-partition communication, DTN routing is not efficient in the well-connected regions of such networks.

There are networks that are challenging for both MANET and DTN routing approaches. A formal framework by Manfredi et al. [75] confirms this assumption. The framework uses the connectivity of the network, the uncertainty of links and network contention to organize

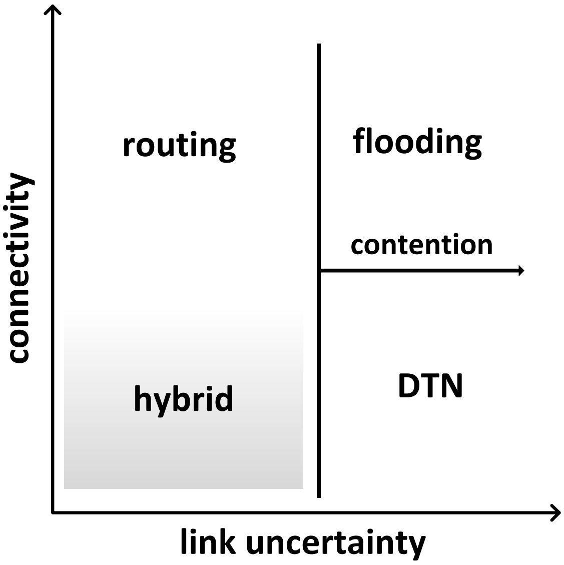


Figure 4.1: Framework for deciding the optimal routing scheme (adapted from [75]).

the decision space for choosing the best suited routing approach into regions where path-oriented routing (i.e., MANET routing), DTN routing or flooding (i.e., sending messages to all nodes in the network) is most appropriate. Figure 4.1 depicts the framework. According to this framework, MANET routing is best suited when there is a high probability that a route exists and the route is stable (i.e., the link uncertainty is low). DTN is best suited when paths are not available or are likely to fail. Hence, DTN routing may even be beneficial in well-connected networks which are very dynamic and prone to link disruptions. Flooding can only be used in unreliable networks with low network load since flooding introduces a lot of overhead. The validity of this general decision framework has also been underpinned by simulations and network traces [75]. Interestingly, most of the networks that were analyzed spent most of their time in the low connectivity and low uncertainty region (i.e., only a few but relatively stable paths exist). As path-based routing is best suited for stable networks and DTN routing (or flooding, depending on the network load) is best suited for networks with low connectivity, this hybrid region is a field of application for protocols that combine both routing paradigms.

4.2 A Classification of Hybrid MANET/DTN Approaches

Hybrid MANET/DTN approaches can be divided into three basic classes. The first class of approaches includes DTN mechanisms (e.g., store-and-forward routing, probabilistic custodian selection, message replication) into a MANET routing protocol. Another possibility to design hybrid MANET-DTN routing schemes is to combine the DTN bundle protocol with a MANET routing protocol. Finally, there are approaches that do not rely on existing protocols but are designed in a way that they can work in a broad range of networks, for instance, by using routing metrics that perform well under diverse connectivity characteristics.

4.2.1 Integration of DTN Mechanisms into MANET Routing Protocols

This type of hybrid approaches integrates DTN mechanisms into a traditional MANET protocol. Particularly, these approaches change an existing end-to-end MANET protocol in order to provide communication between network partitions. To achieve inter-partition communication, at least a store-and-forward mechanism needs to be integrated. Optionally, routing performance may be improved by selecting message custodians based on predicted future communication opportunities and replicating messages in the network. The advantage of this kind of approaches is that they can be implemented at the network layer without adapting the upper layers. However, certain applications such as real-time multimedia communication cannot tolerate higher delays and jitter which are introduced by packet buffering. Thus, also changes in the applications itself may be needed.

4.2.2 Support for the DTN Bundle Protocol

This kind of approaches combines the DTN bundle protocol [110] with a traditional MANET routing scheme. The bundle protocol is an application layer protocol that forms a store-and-forward overlay network. The basic protocol units are called bundles and are typically larger than data units of the underlying transport and network protocols. The bundle protocol itself does not define how bundles are routed but requires an additional DTN routing algorithm. The DTN routing protocol that is used determines if packets are replicated and how custodians are selected. Hence, the performance of this kind of hybrid approaches is mainly influenced by the DTN routing protocol that is used. As the bundle protocol is an application layer protocol, the decision between MANET and DTN routing has to be made at the application layer as well.

Since the decision between MANET and DTN routing is performed at the application layer, applications may choose between MANET and DTN routing based on application-specific context. For instance, a voice communication application could switch from live-streaming to an asynchronous "walkie-talkie"-like communication, which is more appropriate in the presence of network partitions. In such cases, the application could make the user aware of the current state of the network and the current mode of operation (e.g., that only asynchronous communication is possible). On the other hand, this kind of hybrid approaches requires the modification of existing applications. Another disadvantage is that the bundle protocol introduces some additional overhead, especially when all data has to be encapsulated in bundles, even if end-to-end paths are available. This increases the overhead of the protocol and may decrease the performance of the network.

4.2.3 Design of New Routing Protocols for Diverse Networks

There are also approaches that do not combine or integrate existing MANET or DTN protocols but are especially developed to support a broad range of networks with diverse connectivity characteristics. One key to successfully developing such hybrid protocols is to find routing metrics that perform well under diverse connectivity settings. The main advantage is that these protocols have been designed particularly for hybrid networks and use mechanisms and metrics that are suited for well-connected as well as for sparse networks. On the other hand, deployment of such clean-slate approaches may be difficult since no existing MANET protocols nor the DTN bundle protocol can be re-used.

4.3 State-of-the-art in Combined MANET/DTN Routing

Many routing schemes have been introduced, both in the MANET as well as in the DTN domain. Compared to that, hybrid schemes that combine these two approaches are not as well researched. However, the interest in such approaches is increasing, since there are many scenarios where combined approaches are beneficial. In this section an overview of state-of-the-art approaches in this context is given. We cluster the approaches based on the three basic classes that we have introduced in the previous section.

4.3.1 Protocols that Integrate DTN Mechanisms into MANET Routing

The Context-aware Adaptive Routing (CAR) protocol [82] is one of the first approaches that combines MANET with DTN routing. In particular, CAR integrates custodian selection and message buffering, two well-known mechanisms from DTN, into a proactive distance vector MANET routing protocol. The proactive routing protocol is utilized to exchange network-related context information such as the change rate of connectivity or the probability that two nodes are connected. Based on this information, CAR uses a context framework to calculate and predict the delivery probability between nodes. The information about the best candidate node to deliver a message is added to the routing table. In connected parts of the network, CAR uses a proactive MANET routing protocol to exchange data. In partitioned networks, CAR uses the delivery probability to determine the best custodian for the message. As messages are not replicated, CAR introduces only little overhead for the exchange of context information, piggybacked on routing control messages.

The Hybrid MANET DTN (HYMAD) protocol [126] combines techniques from traditional MANET routing protocols and DTN routing. HYMAD partitions the network into several disjoint groups of nodes. All nodes within a group are connected by an end-to-end path and a conventional MANET routing protocol can be used for intra-group communication. For inter-group communication a DTN routing protocol (e.g., Spray and Wait, Epidemic Routing) is used. Hence, a HYMAD group can be seen as one node in a DTN network. The maximum size of a group is a means to control the communication paradigm. For instance, if small groups are used (e.g., all members must be within two hops), more DTN-style inter-group communication is needed because the network is partitioned into many groups. If the groups are very large (e.g., the entire connected portion of the network), HYMAD acts like a MANET protocol with a store-and-forward capability.

The Delay-Tolerant DYMO (DT-DYMO) protocol [67] integrates a probability model into the reactive DYMO routing protocol. The probability model is based on the history of encounters between nodes. DYMO's routing control messages and the route request process are modified in order to find potential custodian nodes, that can deliver data messages in the presence of network disruptions. The route finding process is modified compared to the original DYMO protocol (cf. Section 2.2). In particular, all DT-DYMO route requests contain a delivery probability threshold and nodes reply with a route response if their delivery probability is greater than this threshold. If an end-to-end path is available, DT-DYMO works similar to the unmodified DYMO protocol. However, in the presence of disruptions, a DT-DYMO source node forwards a message to the node which offers the highest probability of meeting the destination. This node stores the message until it can be delivered to the destination. In order to perform an accurate delivery likelihood estimation, nodes periodically exchange their delivery probabilities with custom beacon messages.

BATMAN Store-and-Forward (SF-BATMAN) [39] adds a store-and-forward capability to the proactive MANET routing protocol BATMAN. It is designed to be compatible with the standard BATMAN routing protocol. Hence, it does not change routing control messages nor forward multiple copies of a message. An SF-BATMAN node stores a message if currently no path to the destination can be found. Similarly, packets are buffered if the designated next hop was not recently active (i.e., a control packet was received recently via this node). This reduces packet loss due to stale links. Apart from these modifications, SF-BATMAN acts like the basic BATMAN protocol. Whenever a node receives a routing control packet which may update or validate a routing table entry, the node tries to send all buffered packets.

AODV-OPP [92] integrates store-and-forward functionality into the AODV protocol. AODV-OPP does not change AODV's route discovery process but only intervenes when no end-to-end paths can be found, or an existing path breaks. In such cases, a node will forward a packet to its neighbors instead of dropping it. Buffered packets are also forwarded if a new neighbor is detected, or a route to the packet's destination becomes available. In the latter case, the packet is removed from the buffer and sent via the end-to-end path. To reduce the overhead that is introduced by replication, AODV-OPP limits the number of message copies. Since AODV is a reactive protocol, new routes are only discovered when a node has to send data to a destination for which currently no route is known. However, in the case of AODV-OPP route discovery needs also be triggered for buffered packets. Thus, whenever a node detects a new neighbor, it triggers a route finding process for the destination of the first packet in its packet buffer. However, this may cause the creation of many RREQ messages which are broadcast in the network and hence increase the routing control overhead. Therefore, each AODV-OPP node limits the number of path requests that are issued within a certain period.

The Storage Aware Routing (STAR) protocol [56] uses a two-dimensional routing metric that is based on short-term and long-term route costs to decide whether to store or forward packets. STAR utilizes OLSR to discover paths in the network and modified routing control messages in order to monitor short term and long term link costs (e.g., the link delay) as well as the available storage of other nodes. Similar to traditional MANET routing protocols, STAR utilizes the path that provides the minimum cost to deliver packets. However, if the short term costs of a link are significantly higher than its long term costs, a node would store the packet instead of forwarding it. The rationale behind this approach is that increased short term delays are an indication that the link is already saturated. Likewise, packets are stored if there is no path to the destination available or if the nodes on the end-to-end path do not provide enough storage space to buffer the packet. Compared to the basic OLSR protocol, STAR tries to increase the overall delivery ratio in the network by storing packets to prevent network congestion and buffer overflows.

4.3.2 Hybrid Protocols Using the Bundle Protocol

AODV-DTN [88] combines AODV with the DTN bundle protocol (BP) [110]. To be more precise, AODV messages are extended and the route request/reply process is modified to exchange information about which nodes in the network support the BP. These nodes are in the following referred to as DTN routers. Since the control messages contain information about DTN routers, the source is aware of the shortest end-to-end path and also knows available DTN routers after the route finding process has succeeded. If the source node supports the BP, applications can dynamically switch to bundle transport when no end-to-end path is available. As nodes must also support the BP to use DTN routing, this approach basically enhances the DTN bundle routing by an AODV-based discovery process for DTN routers. Hence, this approach is best suited for networks where (most of) the nodes support the BP.

Lakkakorpi et al. [68] introduced an adaptive routing scheme that allows a message source to choose between a reactive MANET protocol (e.g., AODV) and the bundle protocol using DTN routing. The decision between MANET and DTN routing is based on information that is locally available or can be gathered by means of probing packets. Such information could include the node density or the available bandwidth. Based on this context information, a decision framework selects between a MANET and a DTN routing scheme. The basic operation of the MANET routing protocol is not changed (e.g., AODV control messages and the route finding process are not modified). The decision is only made at the message source and intermediate nodes do not change the routing paradigm. Thus, if the sender decides to send data via an end-to-end path and the path is disrupted while the data is transferred towards the destination, the data would not be buffered but dropped by the node that is affected by the path break. Thus, the decision framework may also select to use the bundle protocol in the presence of an end-to-end path, if this path is unstable. In particular, the source node estimates the transfer time of a packet and the lifetime of the path to the destination. If the estimated packet transfer time is larger than the estimated path lifetime, the bundle protocol would be chosen to prevent the aforementioned problem.

Delay Tolerant Structured Overlay Link State Routing (DTS-OLSR) [90] builds a DTN-based overlay network on top of the OLSR routing protocol. The periodic link state updates of OLSR are used to form and maintain an overlay network. This overlay network provides methods to register and find overlay nodes that support the DTN bundle protocol (these nodes are called DTS-OLSR nodes). If a node does not support the BP, it may use the nearest DTS-OLSR node to send and receive bundles. All communication between the DTS-OLSR and the non DTS-OLSR node is performed via so called lite bundles. Hence, each messages has to be encapsulated into a bundle or a lite bundle before it can be sent, even if an end-to-end path exists. As a result, DTS-OLSR introduces some communication overhead which decreases its performance compared to standard OLSR, especially when the network is well-connected [90].

Delay Tolerant Link State Routing (DTLSR) [40] combines the ideas of link-state routing with the DTN bundle protocol. DTLSR is mainly designed for networks in developing regions and assumes that nodes are rather static and topology changes are not too frequent. Like traditional link-state protocols, DTLSR uses link state announcements (LSAs) to convey data about the network topology. However, there are some differences to traditional link state routing. First, DTLSR uses the BP for transmitting LSAs. Second, the announcements have a large lifetime (on the order of hours). Hence, LSAs need not be broadcast regularly but only if link information changes. Third, the path calculation also utilizes paths that are currently not available but may get available before the message expires. Similarly to LSAs, all payload data is transmitted by means of bundles. Thus, in contrast to other combined MANET/DTN approaches, DTLSR does not integrate DTN mechanisms into a MANET protocol but rather uses the concept of link state announcements within a DTN architecture. Although the approach borrows ideas from traditional link state routing, it is mainly intended for applications that can cope with delays on the order of hours or days (e.g., email communication in rural areas).

4.3.3 Routing Protocols Designed for Diverse Networks

The Robust Replication Routing (R3) protocol [120] does not extend or switch between existing routing protocols but is designed in a way that it performs well under different connectivity characteristics. R3 achieves this by adapting the number of message replications based on the distribution of path delays. In order to monitor path delays, all nodes periodically exchange probing packets. The distribution of path delays has a direct effect on the benefit of replicating a packet and sending it via multiple paths. This benefit is also called replication gain and is higher if the predictability of the delay is low (i.e., the path delays are highly variable). If the expected delay is well predictable, R3 uses the path with the minimum expected delay (MANET-style routing). If the expected delay is unpredictable, R3 uses multiple paths to convey the message via those paths that minimize the expected delay (DTN-style routing). R3 uses source routing (i.e., the addresses of all nodes along the path are stored in the packet header) in order to allow the source node to control which paths are used.

FansyRoute [37] adds packet replication to link-state routing in order to tackle the challenges of intermittently connected networks. The main idea of the protocol is that each node may forward a packet to multiple neighbors, based on local connectivity characteristics and a desired delivery probability. In other words, each node adaptively adjusts its number of outputs. The number of outputs is also called the fan-out of a node. Based on periodic hello messages for neighbor detection and topology control messages for link advertisements, FansyRoute uses a modified Dijkstra's shortest path algorithm to calculate the minimum paths in the network using the average availability of a path as a metric. When a node has to forward a packet, it decides, based on the average path availability, to how many neighbors to forward a message in order to satisfy the desired delivery probability. It has to be noted that FansyRoute targets delay-intolerant applications and hence does not use packet buffering. The main contribution of FansyRoute is the adaptive selection of the fan-out of nodes in the network based on delivery requirements and the current state of the network. No replication is used if a single path is available which offers an average availability that is greater than the target delivery probability. In that case, FansyRoute works similar to traditional MANET link-state protocols such as OLSR. In other cases it works like other MANET multi-path routing protocols [119] which try to increase the reliability of routing in the presence of link failures by utilizing several paths in the network.

The Hybrid Opportunistic Routing (HOR) [16] protocol integrates replication-based forwarding with an opportunistic forwarding approach that exploits the broadcast nature of the wireless medium. It is important to note that in the context of HOR, opportunistic routing denotes a routing approach for MANETs that has initially been introduced by Biswas and Morris [24] and may not be mistaken with the idea of opportunistic routing in the context of DTNs (i.e., making routing decisions without a priori knowledge about mobility or connectivity). HOR uses unicast and broadcast transmissions to forward packets and differentiates between three types of forwarding approaches. It uses broadcasts to transfer packets to direct neighbors (direct forwarding) and two-hop neighbors (two-hop forwarding). For longer paths, packets are replicated and forwarded to custodian nodes using unicast transmissions (replication-based forwarding). Since other nodes overhear broadcasts, nodes can obtain information about packet transfers in their vicinity. This allows nodes to coordinate each other in deciding which nodes have to forward a packet in the case of two-hop forwarding. Additionally, overhearing can reduce duplicate transmissions and also improves buffer management since nodes can avoid transmitting or storing packets which have been previously transmitted or have already been delivered. This is especially beneficial in dense networks in order to save resources. In cases where neither a direct nor a two-hop path is available, replication is used, which especially improves the delivery ratio in sparse networks.

4.3.4 Comparison of State-of-the-Art Hybrid MANET/DTN Approaches

A summary of the hybrid MANET/DTN approaches can be found in Table 4.1. The approaches are compared on different aspects. First, which type of MANET routing principle or protocol is used. Some approaches are dependent on a certain MANET protocol as they include additional information in control messages or modify the route finding process. Other approaches are more generic in the sense that they can be used with any MANET protocol that follows a certain routing approach such as link state routing or distance vector routing. The second aspect that is considered is whether the approaches use the bundle protocol for data delivery. The last two aspects that are considered are whether message replication and custodian selection are supported. For protocols that use the bundle protocol, these two aspects are usually dependent on the DTN routing protocol that is used.

Table 4.1: Comparison of combined MANET/DTN routing approaches

Protocol	**MANET prot.** **(routing approach)**	**Bundle** **protocol**	**Message** **replication**	**Custodian** **selection**
AODV-DTN [88]	AODV	optional[1]	optional[2]	optional[2]
AODV-OPP [92]	AODV	no	yes	yes
BATMAN-SF [39]	BATMAN	no	no	no
CAR [82]	DSDV	no	no	yes
DT-DYMO [67]	DYMO	no	no	yes
DTSLR [40]	link-state	yes	optional[2]	optional[2]
DTS-OLSR [90]	OLSR	yes	optional[2]	optional[2]
FansyRoute [37]	link-state	no	yes	no
HOR [16]	opportunistic routing	no	yes	yes
HYMAD [126]	distance vector	no	yes	yes
Lakkakorpi et al. [68]	AODV	optional[3]	optional[2]	optional[2]
R3 [120]	link-state	no	yes	no
STAR [56]	OLSR	no	no	no

[1] The bundle protocol is used if AODV does not report a route to the destination.

[2] Depending on the DTN routing protocol that is used to route the bundles.

[3] Decision framework at sender decides about the usage of bundles.

4.4 Integrating Packet Buffering on Top of MANET Routing

This section describes a routing approach that is based on the integration of packet buffering into a MANET routing protocol. The main idea behind this approach is to use information that is already collected by a MANET routing protocol in order to detect partitions in the network. The approach centers around two decisions which can be made at the network layer: first, when to store a packet instead of forwarding it to a neighbor instantly; second, when to send a previously stored packet.

The decision to buffer a packet is made whenever a data packet is received by a node. This can either be if the node is the source of the data packet and hence the data packet is retrieved from an upper layer, or if the node has been selected as next hop by another node and receives a data packet from a lower layer. In both cases a traditional MANET routing protocol would drop the data packet if the routing table does not contain an entry for the packet's destination (i.e., the node cannot determine to which of its neighbors the packet should be forwarded). This causes packet loss and hence reduces the packet delivery ratio. However, the packet may be sent later when a next hop is available for the packet's destination. Thus, packets need to be buffered in such cases in order to provide a store-and-forward mechanism. Additionally, it is beneficial to check the state of an existing routing table entry since the entry may be invalid. In such a case the routing table contains an entry for the packet destination which contains an unreachable next hop node. Such stale route entries are another cause for packet loss. This check for stale routing information is needed since routing protocols need some time to detect and handle stale route entries (e.g., to recalculate the routing table to update the next hop information, or to remove the entry from the routing table). Hence, packets may also be stored if a node detects that a neighbor cannot be reached currently.

It is important to note that these modifications do not change the routing decisions of the underlying MANET routing protocol. Thus, packets are always sent to the node that has been selected by the MANET routing algorithm to be the best next hop for a packet's destination. Algorithm 4.1 shows the pseudo code of the decision logic for storing packets.

The second check that is performed detects when buffered packets can be forwarded or delivered (see Algorithm 4.2). This check can also make use of the characteristics of proactive MANET routing protocols. In particular, in proactive routing protocols such a decision can be made whenever a routing control packet has been received, since that may

Algorithm 4.1: Decision logic for storing data packets.

```
Data: packet
begin
    $nextHopAddr \longleftarrow getNextHop(packet)$;
    if $nextHopAddr = null$ then
        $bufferPacket(packet)$
    end
    else if $hasValidLink(nextHopAddr) = false$ then
        $bufferPacket(packet)$
    end
    else
        $sendTo(nextHopAddr, packet)$
    end
end
```

update the routing table or the state of links. In particular, there are three cases when a buffered packet can be sent: First, a new route has been found which is entered into the routing table. Second, a route entry has been updated and contains a different next hop than before. Third, a stale route becomes available again (i.e., the link to the next best next hop is available again).

The first two cases are a result of receiving a routing control packet that includes new information about the topology of the network. The third case may either also be caused by receiving a routing control packet over a link that has previously been inactive, or by some link layer detection mechanism. In this work we do not rely on information from the data link layer but only use network layer information to assess the state of a link. This is possible since proactive routing protocols periodically broadcast information which can be used to determine the state of a link.

When the decision logic for sending buffered packets decides that previously buffered packets can be sent, the order in which to send the packets need to be defined as well. In this work we follow the first in, first out (FIFO) queuing policy, which means that the oldest packets are sent first. Similarly, if a buffer is full the oldest packet is dropped first. Whenever a packet has been forwarded to a neighboring node, it is removed from the buffer. Thus, at any time only a single copy of a packet exists in the network.

To handle possible obsolete routes, our approach defines a *MaxLinkTimeout* parameter and stores packets if the link has not been not active in the last *MaxLinkTimeout* seconds. This parameter is used in the *hasValidLink* method. Since proactive routing protocols periodically exchange control information, such a link validity check can use information that is already provided by the routing protocol. For instance, BATMAN provides information about when the last router originator message (OGM) has been received. If the most recent OGM was received less than *MaxLinkTimeout* seconds ago, the route is considered to be active. Similarly, OLSR nodes regularly exchange HELLO messages that can be used to detect obsolete routes. Although our hybrid MANET/DTN approach could also use a custom probing mechanism to determine which links are active, it is beneficial to rely on information that is already provided by the routing protocol. In this way no additional control overhead needs to be introduced to perform the link validity check.

Algorithm 4.2: Processing buffered packets upon control packet reception.

```
Data: bufferedPkts
begin
    foreach $packet \in bufferedPkts$ do
        $nextHopAddr \longleftarrow getNextHop(packet)$;
        if $hasValidLink(nextHopAddr) = true$ then
            $sendTo(nextHopAddr, packet)$;
            $bufferedPkts \longleftarrow bufferedPkts \setminus \{packet\}$
        end
    end
end
```

The main idea of the presented approach is to rely on information gathered by a proactive MANET routing protocol in order to detect the lack of end-to-end paths and invalid route entries and buffer packets in such cases. This practically combines traditional MANET routing with store-and-forward routing. The main advantage is that no additional overhead needs to be introduced to perform the aforementioned detection and that existing MANET routing protocols are not changed.

The approach has also some drawbacks. Packet buffering on top of a MANET routing protocol allows nodes to only bridge temporal partitions in the network. However, the sender and receiver have to be in the same connected component in order to establish an end-to-end path and exchange data. If sender and receiver are never in the same connected component, the approach fails to deliver data. Additionally, the approach relies on periodic updates of the routing table. Hence, it is does not work well in combination with reactive protocols that establish paths only when needed.

The following section describes an improvement of the approach where packet buffering is enhanced by forwarding data to custodian nodes that may be able to deliver the data to the destination. This mechanism allows nodes to bridge permanent disruptions, i.e., packets can be delivered even if the source node and the destination node are never in the same partition.

4.5 Combined MANET/DTN Routing with Packet Buffering and Utility-based Forwarding

In this section we introduce a hybrid routing approach that integrates packet buffering and opportunistic forwarding into traditional MANET routing. We refer to this approach as Combined MANET/DTN Routing (CoMANDR). Similar to MANET routing protocols, CoMANDR uses a routing table that includes information about end-to-end paths to route packets in the connected parts of the network. Thus, it works similarly to traditional end-to-end routing protocols if end-to-end paths are available. Additionally, two mechanisms from DTN routing are utilized. First, packets are buffered in case there is no end-to-end path available. Packet buffering allows nodes to bridge temporal partitioning of the network. Second, nodes also opportunistically forward packets to nodes that are likely to improve the chance of delivery. The decision to forward a packet is based on the utility of the other node to deliver the message to the destination. This mechanism is also able to bridge permanent partitions of the network.

The pseudo code in Algorithm 4.3 describes the algorithm that decides between end-to-end and DTN routing. In general, CoMANDR prefers end-to-end paths and only falls back to store-and-forward routing if no continuous path exists. If no end-to-end path exists, CoMANDR determines if there is a neighbor that has a higher utility for the packet's destination. If such a neighbor exists, the packet is forwarded to this node. While this procedure is repeated at every node, the packet is sent towards the destination.

One idea that influenced the design of CoMANDR is the fact that traditional end-to-end routing is widely used in ad-hoc networks and that the information that is provided by a MANET routing protocol may also be beneficial for DTN routing. For instance, the

MANET routing protocol may provide some information that can be used to estimate the chance that two nodes will meet. Thus, CoMANDR can re-use information that is collected by a MANET protocol and is already locally available at a node, to improve the forwarding decisions of a DTN routing protocol. Such useful information items include the MANET routing table or other information about the network topology that is provided by the underlying end-to-end protocol (e.g., link state announcements). However, it would also be possible to collect and integrate additional information if needed. By combining MANET and DTN routing, CoMANDR can cope with disruptions when the network is partitioned and provide efficient routing when the network is well-connected.

4.5.1 Packet Buffering

Packets are buffered if there is no end-to-end path available, i.e., the routing table does not contain a routing entry for the next hop of a packet. Additionally, it is also checked if an existing routing table entry is still valid. An entry is considered to be invalid if its next hop entry is currently not available (i.e., there is no wireless link available). Such stale route entries may be an effect of link outages caused by the mobility of nodes or obstacles and MANET routing protocols need some time to detect and handle such events. Thus, packets may be lost because they are sent to an unavailable neighbor, which may decrease the overall packet delivery ratio. To identify if a next hop is available, MANET routing control traffic can be monitored. Additionally, information from other layers may be used (e.g., information about the status of links provided by the underlying link layer protocol).

Apart from deciding when to buffer a packet, it is also important to decide when a buffered packet can be sent. In case of temporary link outages, packets may be sent as soon as the link is available again, or a proactive MANET routing protocol provides an alternative path. Thus, the decision to send packets can be performed whenever the routing table is updated or whenever nodes meet.

4.5.2 Utility-based Forwarding

The utility of a node describes the node's fitness to deliver a packet towards its destination. In general a node will hand over a packet to another node if the other node has a higher utility value. The utility may be dependent or independent of the destination [115]. A

Algorithm 4.3: Packet routing in CoMANDR.

```
Data: packet
begin
    $nextHopAddr \longleftarrow getNextHop(packet)$;
    if $nextHopAddr \neq null$ and $hasValidLink(nextHopAddr) = true$ then
        $sendTo(nextHopAddr, packet)$;
    end
    else
        $neighbors \longleftarrow getConnectedNodes()$;
        $U_{id} \longleftarrow getUtility(this, dest)$;
        $U_{target} \longleftarrow U_{id} + (U_{id} - (U_{id} \cdot \gamma^2))$;
        foreach $j \in neighbors$ do
            $U_{jd} \longleftarrow getUtility(j, dest)$;
            if $U_{jd} > U_{target}$ then
                $U_{target} \longleftarrow U_{jd}$;
                $nextHopAddr \longleftarrow j$;
            end
        end
        if $nextHopAddr \neq null$ then
            $sendTo(nextHopAddr, packet)$;
        end
        else
            $bufferPacket(packet)$;
        end
    end
end
```

destination-independent utility function is based on characteristics of the potential custodian node, such as its resources or mobility. On the other hand, destination-dependent utility functions are based on the relationship between a node and the destination, such as how often a node has met the destination, or if a node and the destination belong to the same social group.

The combined use of a utility table and a MANET routing table allows nodes to route packets in connected as well as disrupted networks. The MANET routing table represents some sort of spatial information (i.e., which nodes are currently in the vicinity of a node). Combining current routing table information with utility functions that take historic data into account (e.g., information about previous states of the routing table), effectively calculates spatio-temporal clusters of nodes. This information allows a node to determine to which other node a packet should be sent, when there is currently no end-to-end path to the destination available.

The performance of a utility function is influenced by the characteristics of the scenario. Hence, it is important to choose a utility function or a combination of functions that fits the specifics of the intended application scenario. We have chosen a utility function that uses routing table entries to calculate meeting probabilities based on the well-known PROPHET routing algorithm [73]. However, in contrast to PROPHET, CoMANDR does not assume that the network is sparse. Hence, nodes periodically exchange their meeting probabilities with other nodes, instead of exchanging them only when two nodes meet. It is important to note that only direct neighbors need to exchange their meeting probabilities and this information may also be piggy-backed with periodic control messages of the underlying MANET routing protocol. Hence, the introduced overhead is rather small. In contrast to the PROPHET protocol that only considers when two nodes directly meet (i.e., there is a direct link between the nodes), CoMANDR also considers multi-hop information from the routing table. This means that a node i considers to be connected to another node j if it has a routing table entry for node j with a distance less than infinite. This allows nodes to exploit multi-hop paths to determine contacts with other nodes. Another difference is that the meeting probability is updated periodically and not only when two nodes meet. This results in some further changes compared to the PROPHET protocol. In particular, in CoMANDR each node manages *clusters* of nodes. A cluster is a set containing nodes which are potential custodian nodes for a certain destination (i.e., they offer a certain utility to deliver data to the destination). Since it is assumed that nodes run a proactive MANET routing protocol, it is possible to add the information about utilities to existing control messages. Alternatively, nodes may use a custom beaconing mechanism to periodically broadcast their utility values to their neighbors. Before we describe the calculation and management of these clusters, we will first describe the calculation of the utility values.

As the MANET routing protocol regularly updates the routing table entries, the meeting probabilities and thus the utility values for other nodes are regularly updated as well following Equation 4.1. Every node i manages a utility value for every node j that it has met. The set of known nodes includes all destinations for which a routing entry currently exists or has existed previously (i.e., disconnected nodes that are kept in the utility table until their utility value drops below a certain threshold). So if a route to node j is known, node i will update the utility value for node j (denoted by U_{ij}) using the following utility update function:

$$U_{ij} = U_{ij} + (1 - U_{ij}) \cdot \alpha, \tag{4.1}$$

where $\alpha \in]0, 1[$. The parameter α determines how fast the utility converges towards 1 if there is a contact between two nodes.

On the other hand, for a node k that is currently not in the routing table but has a utility value, the utility value U_{ik} is updated as follows:

$$U_{ik} = U_{ik} \cdot \gamma, \tag{4.2}$$

where $\gamma \in]0, 1[$. It determines how fast the utility value decreases if there is no contact between node i and node k.

Every node regularly broadcasts all calculated utilities (i.e., the utility table) to its direct neighbors. When a node receives the utility table of another node, it can use this information to update its own utility table following Equation 4.3. In particular. if a node i is in contact with node j and receives $j's$ utility table containing a utility value for node k, node i can transitively update its utility value for node k. We use the following transitive update function [49]:

$$U_{ik} = max(U_{ik\ old}, U_{ij} \cdot U_{jk} \cdot \beta) \tag{4.3}$$

The parameter β is used to control the impact of transitivity. $\beta \in [0, 1]$, where a value of 0 disables transitivity.

We performed experiments to empirically find parameters for the utility calculation that

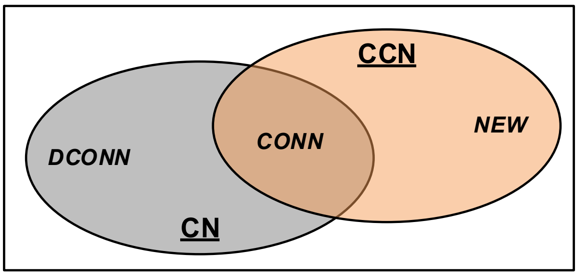


Figure 4.2: Relation between the managed sets of nodes.

suit the scenarios. In particular, we carried out simulations using different values for the parameters α, β and γ and measured the delivery ratio. We omit details about the results here but refer the interested reader to Appendix B. Summing up the results, it can be said that γ has the highest impact on the performance and that higher values, close to 1 achieve better results. The main reason is that γ determines how long entries are kept in the cluster and hence determine the list of potential custodian nodes. The other two parameters have less impact on the delivery ratio and many different value combinations yield similar results.

The pseudo code for updating the utility table of a node is given in Algorithm 4.4. Each node manages information about which nodes are currently connected (CCN). This information can be gathered from the routing table (i.e., $n \in CCN$ if there exists a routing table entry for node n). Additionally, each node manages a set of cluster nodes (CN) that offer a utility that is greater than a certain threshold (i.e., $n \in CN$ if $U_n > U_{exit}$). Based on these two sets, a node can determine if new nodes are available or existing nodes became unavailable. In particular, the set $CONN$ contains all nodes that are currently connected and also have been previously known (i.e., $CONN = CCN \cap CN$). The set NEW contains all nodes which are currently connected but are not known already (i.e., $NEW = CCN \backslash CN$). The set $DCONN$ contains all nodes that have been previously known but are not connected anymore (i.e., $DCONN = CN \setminus CCN$). The relation between the sets is depicted in Figure 4.2.

If the utility of another node drops below a certain threshold U_{exit}, the node is removed from the cluster. The reasons are to limit the calculation efforts and to reduce the amount of data to be exchanged by reducing the size of the utility table. Another option would be to limit the size by only keeping the n highest entries in the cluster. However, removing nodes with a low utility value has another advantage. Since such nodes only offer a low chance of delivering the packet, selecting one of these nodes as custodian would actually not

Algorithm 4.4: Utility and cluster calculation at a node i.

```
Data: set of currently connected nodes $CCN$
set of known nodes in cluster $CN$
table containing utility values $UT$;                    /* indexed by node ids */
Result: updated utility table $UT$
begin
    $CONN \longleftarrow CN \cap CCN$;
    $NEW \longleftarrow CCN \setminus CN$;
    $DCONN \longleftarrow CN \setminus CCN$;
    /* update utility value for every node that is already known and
       connected                                                           */
    foreach $j \in CONN$ do
        $U_{ij} \longleftarrow UT[j] + (1 - UT[j]) \cdot \alpha$;
        $UT[j] \longleftarrow U_{ij}$
    end
    /* init utility value for newly connected nodes                        */
    foreach $n \in NEW$ do
        $CN \longleftarrow CN \cup \{n\}$;
        $UT[n] \longleftarrow U_{init}$
    end
    /* update utility value for known nodes that are disconnected          */
    foreach $k \in DCONN$ do
        $U_{ik} \longleftarrow UT[k] \cdot \gamma$;
        /* remove node if its utility drops below threshold value          */
        if $U_{jk} < U_{exit}$ then
            $CN \longleftarrow CN \setminus \{k\}$;
        end
        $UT[k] \longleftarrow U_{jk}$
    end
end
```

improve the delivery probability significantly. Thus, removing such nodes from the set of possible custodians is a means to reduce the amount of transmissions that do not contribute to the delivery of a message.

A node only forwards packets to nodes that offer a utility that is significantly better than the node's own utility. This reduces the number of transmissions that do not significantly improve the delivery probability. Additionally, this prevents nodes with similar utility values to repeatedly exchange the same packets which would create routing loops. For example, imagine a situation where two nodes i and j have very similar utility values concerning a destination node d. Both nodes are currently not in contact with node d. Node i has a packet for d which it forwards to node j because $U_{id} < U_{jd}$. However, shortly after node j has received the message, it updates its utility table and hence the utility value U_{jd} decreases following Equation 4.2. This results in $U_{jd} < U_{id}$ to become true which in turn causes j to send the packet back to node i. However, when node i also ages its utility value, $U_{jd} < U_{id}$ will be true again which causes i to send the packet back to node j, and so forth. To prevent this kind of routing loops, a node only forward packets to another node if the other node has a utility value that is at least ΔU greater than the node's own utility. As the utility value does not increase linearly, ΔU has to be calculated dynamically based on the current utility value. To prevent routing loops due to asynchronous aging of very similar utility values between nodes, ΔU has to be at least $U_{id} - U_{id} \cdot \gamma$, where i is the current node and d the destination of a packet. This means i would only forward packets destined for a node d to a node j if $U_{jd} > U_{id} + \Delta U$.

In general, ΔU can be calculated as $\Delta U = U_{id} - U_{id} \cdot \gamma^x$, where x has to be at least 1 to prevent the aforementioned routing loop problem. However, x may also be set to a higher value, which means that the difference between a node's own utility value and the utility value of a neighbor has to be larger before packets are forwarded to a neighbor. However, if this minimum required difference is set too high, packets may not be forwarded despite the fact that this would increase the delivery ratio. Based on evaluations with different values for x, we found that $x = 2$ offers a good tradeoff between preventing unnecessary transmissions (i.e., transmissions that do not increase the delivery ratio) without negatively affecting the delivery ratio by missing opportunities to forward packets. Thus, as described in Algorithm 4.3, nodes use $\Delta U = U_{id} - U_{id} \cdot \gamma^2$ when calculating the so called target utility U_{target}, denoting the minimum utility that another node has to offer to be chosen as custodian node.

4.6 Conclusion

This chapter presented routing approaches that combine techniques from traditional end-to-end routing (MANET routing) and routing for delay-/disruption tolerant networking (DTN routing). It reviewed and classified several state-of-the-art approaches from this domain. We identified three particular classes. First, the integration of DTN mechanisms into MANET routing protocols. Second, approaches that complement the DTN bundle protocol with MANET routing. Third, approaches that are not based on existing MANET routing protocols or the bundle protocol but use metrics that allow them to support a broad range of networks with diverse connectivity characteristics. There is no superior design approach since all of them provide different advantages and disadvantages. Instead, it can be noted that the decision for a certain design approach depends on the target application scenario and the expected connectivity characteristics of the networks.

Furthermore, this chapter contributed to the research goals of this thesis by introding two combined MANET/DTN approaches that we believe are useful in emergency response scenarios. The first approach that is described in Section 4.4 extends MANET routing with packet buffering. The main design goals of this protocol are to not interfere with the basic behavior of the underlying MANET routing protocol (e.g., not changing routing control messages or the route finding process) and allow for an easy integration with existing IP networks. The main idea of the protocol is to utilize information that is already provided by the MANET routing protocol in order to decide when to buffer packets. The downside of this approach is that it does not bridge permanent disruptions but requires that the source and the destination are in the same connected component at some point in time. The second approach that is presented in Section 4.5 improves the first approach by providing a mechanism to bridge permanent partitions. It uses information from the underlying MANET routing protocol in order to determine which nodes are potential message custodians. Both approaches fall into the first class of design approaches, namely they complement MANET routing with mechanisms from DTN routing. The reason for this is that the evaluations in Chapter 3 have shown that the networks are basically well-connected and hence MANET routing works well in parts of the network. We designed the DTN extensions to bridge partitions in the network in a way that allows for easy integration with existing protocols. For instance, the protocol that has been described in Section 4.4 can actually be used in existing networks which use OLSR or BATMAN. Similarly, only little changes are needed to integrate the protocol that has been described in Section 4.5.

In the next chapter we evaluate both approaches with a focus on the emergency response scenarios that have been presented in Chapter 3 in order to determine whether a combination of MANET and DTN approaches outperforms routing from the MANET and the DTN routing domains.

CHAPTER

5 Evaluation of Routing Protocols in Emergency Response Scenarios

This chapter presents several simulation-based studies that evaluate routing protocols from different domains (i.e., MANET routing, DTN routing, and a combination of the two approaches) in emergency response scenarios. In particular, the evaluations are performed in the chemical incident scenario and the Risavika exercise scenario which have been presented in Chapter 3.

This chapter is structured as follows: First, Section 5.1 describes the framework that is used for the evaluation. Section 5.2 presents related work concerning the evaluation of routing protocols in emergency response scenarios. The evaluation presented in Section 5.3 shows how the hybrid MANET/DTN approach that integrates packet buffering with MANET routing performs in the chemical incident scenario. The second evaluation, presented in Section 5.4, evaluates our combined MANET/DTN approach CoMANDR and other approaches in the Risavika exercise scenario. Section 5.5 includes an evaluation of CoMANDR in a more generic scenario. Finally, Section 5.6 concludes this chapter.

Please note that this chapter is partially based on previously published work. In particular, the evaluation presented in Section 5.3 is based on [97] and the evaluation described in Section 5.5 has been originally presented in [99].

5.1 Evaluation Framework

All evaluations are performed using the evaluation framework that has been described in Section 3.1. We use a combination of OMNeT++ and the ONE simulator to benefit from the different advantages of these two simulation frameworks. In particular, OMNeT++ is used to evaluate our hybrid MANET/DTN routing approach (cf. Section 4.4). For the evaluations that focus on DTN protocols the ONE simulator is used, since it provides implementations of different DTN routing algorithms and is widely used in the DTN research domain. However, OMNeT++ is still used to generate connectivity traces that consider effects of wireless propagation and obstacles that attenuate wireless signals (cf. Section 2.5). These connectivity traces are used as input for the ONE simulator which does not include models concerning the propagation of wireless signals.

5.2 Related Work

To the best of our knowledge, there are no existing works that evaluate hybrid MANET/DTN routing protocols in disaster response scenarios. Instead, existing work concerning routing in emergency response scenarios either focuses on MANET routing or DTN routing. Related work in the context of MANET routing protocols has been presented in Section 3.4.3. In the domain of DTN routing, Martín-Campillo et al. [76] use the disaster area mobility model to evaluate routing protocols such as MaxProp, Epidemic Routing and PROPHET. The evaluation results show that MaxProp provides the best delivery ratio and that Epidemic Routing and PROPHET do not perform well in scenarios with high message loads because of network congestion. However, the evaluation scenario only includes communication between two zones (i.e., Incident Location and one treatment zone, such as a PWFTA or a CCS). We believe that this simplification has an effect on the results of the evaluation and that it is important to include more elements of a disaster response scenario.

5.3 An Evaluation of Hybrid MANET/DTN Routing in the Chemcial Incident Scenario

This section presents a simulation-based evaluation of our hybrid MANET/DTN protocol that we presented in Section 4.4. The protocol is evaluated in the chemical incident scenario. The evaluation includes implementations of the protocol on top of the well-known OLSR and BATMAN routing protocols (cf. Section 2.2).

5.3.1 Scenario Description and Simulation Setup

The evaluation uses the chemical incident scenario that is described in Section 3.2. The chemical incident scenario includes 25 nodes that represent first responders that move at the scene. The scenario consists of two Incident Locations (IL 1 and IL 2) representing buildings that contain trapped persons. These locations also represent wireless obstacles which negatively affect connectivity of first responders entering these buildings. Additionally, there is PWFTA inside the facility. The most important area in front of the facility is the TOC where the incident commander is located.

Another important aspect beside the movement pattern of the nodes is the generated network traffic. In this evaluation, every first responder node regularly sends packets to the node that is located in the TOC in front of the chemical plant. This traffic model has been chosen since status updates and other information about a first responder and his/her surroundings (e.g., photos taken by first responders, data from body sensors) are important to increase the situation awareness of the incident commander.

The hybrid MANET-DTN approach is implemented on top of existing implementations of the BATMAN and OLSR protocols that are part of the INETMANET framework [7] for OMNeT++. To simulate the aforementioned traffic model, all nodes send UDP packets to the node located in the TOC, after an initial waiting time of 60 s. The simulation time of every experiment is 3000 s and every experiment is repeated 20 times. The most important simulation parameters are listed in Table 5.1.

5.3.2 Experiments

We use *packet delivery ratio* (PDR) and *delay* as metrics, since they are widely used routing protocol performance metrics. In a first series of experiments, several parameters for the link validity check that is performed in the `hasValidLink()` method (cf. Algorithm 4.1), are evaluated. This method checks if a link is available and packets sent via this link are likely to be delivered. If `hasValidLink()` returns false for the next hop of a packet, the packet is buffered, otherwise, it is sent instantly. In OLSR and BATMAN, nodes regularly send control messages to announce themselves (i.e., OGMs in BATMAN and HELLO messages in OLSR). If such a message from a neighboring node has been received recently, the link to this neighbor is likely to be available. To be more precise, `hasValidLink()` checks if the link has been updated in the last $MaxLinkTimeout$ seconds. We evaluate $MaxLinkTimeout$ values of 1 s, 3 s and 5 s. It is important to note that OLSR and BATMAN use different control message intervals. Hence, the same $MaxLinkTimeout$ value is actually differently strict for BATMAN and OLSR. For instance, setting $MaxLinkTimeout$ to 3 s means that the loss of one OLSR HELLO message causes the link to be seen as inactive, whereas at least one OGM loss is tolerated in the case of BATMAN (assuming the use of the intervals given

Table 5.1: Simulation parameters

Wireless model	
MAC protocol	802.11 (g)
Propagation model	Free-space path loss ($\alpha = 2$)
Transmission range	100 m
Transmission rate	54 Mbit/s
Traffic model	
Pattern	on/off
On-time	3-7 s
Off-time	5-10 s
Packet rate	10 packets/s
Packet size	1024 byte
Sent packets per node (mean)	11897
OLSR routing parameters	
Hello interval	2 s
TC interval	5 s
MID interval	5 s
Metric	Expected transmission count
BATMAN routing parameters	
OGM interval	1 s
OGM window size	64
Route purge timeout	640 s

in Table 5.1). If the timeout is set too high, more packets are lost because of outdated link information. On the other hand, setting this parameter too low causes many data packets to be buffered unnecessarily, which increases the processing overhead and may even cause packet losses if the buffer is full.

In a second set of experiments the buffer capacity is varied between 50 and 1000 packets. For the given traffic pattern, a buffer size of 1000 resulted in no buffer overflows. Additionally, packet buffering is disabled (i.e., the buffer size is set to 0) to show routing performance without the store-and-forward mechanism. This case represents the original OLSR and BATMAN protocols. It is expected that larger buffer capacities increase the packet delivery ratio as more packets can be buffered in the case of route failures. However, the increase comes at the expense of a higher packet delay.

5.3.3 Simulation Results

The packet delivery ratio (PDR) is an important metric to evaluate the performance of routing protocols. The unmodified versions of OLSR and BATMAN achieve an average PDR of about 83.2% and 80.7%, respectively. Figure 5.1 shows the average PDR (including the 95% confidence intervals) of OLSR and BATMAN for different buffer sizes and *MaxLinkTimeout* values. In general, a higher buffer capacity results in an increase of the PDR as longer disruptions can be covered by the store-and-forward mechanism. However, for a *MaxLinkTimeout* of 5 s and 3 s the PDR cannot be increased any further, since the buffers never get filled completely.

Figure 5.1 also shows how the *MaxLinkTimeout* parameter influences the PDR. Reducing the allowed link timeout causes the store-and-forward mechanism to react earlier to link breaks. Thus, fewer packets are lost on stale routes but are only sent if a link update has been received recently. However, it is important to take the default route update interval of the routing protocol into account when adjusting the *MaxLinkTimeout* parameter. If the *MaxLinkTimeout* is set too strict (i.e., much smaller than the default update interval), the PDR would decline if the buffer capacity is not sufficient. This is due to the fact that many packets are buffered unnecessarily (i.e., `hasValidLink()` returns a false positive because the timeout is set too strict) and may be dropped if the buffer is full. Thus, the smallest *MaxLinkTimeout* value that we evaluated is 1 s (i.e., the OGM update interval of BATMAN).

For *MaxLinkTimeout* values of 3 s and 5 s and small buffer sizes (i.e., buffer capacity $\leq$ 200) OLSR achieves a higher average delivery ratio than BATMAN for the same parameter set. This is an indication that OLSR repairs routes more quickly than BATMAN. For bigger buffer capacities (i.e., $\geq$ 500) the advantage disappears as a further increase of the PDR is limited by other factors (e.g., transmission errors, packets buffered at the end of the simulation, routing loops). For a *MaxLinkTimeout* of 1 s, OLSR outperforms BATMAN for all buffer capacities and achieves a PDR of nearly 98% for a buffer capacity of 1000, whereas BATMAN achieves a PDR of about 96%. On average, the hybrid MANET/DTN protocol can deliver about 19% more packets than the original BATMAN protocol and 18% more than the original OLSR protocol.

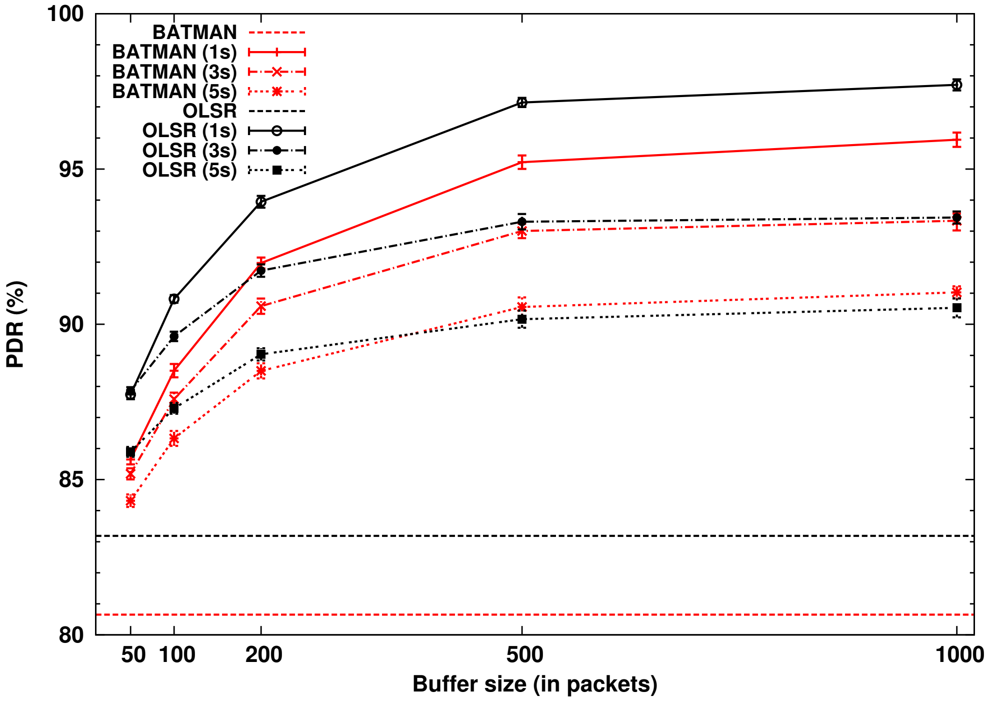


Figure 5.1: Packet delivery ratio for different buffer capacities and *MaxLinkTimeout* values.

Since the network is diverse in terms of connectivity, it is interesting to investigate the packet delivery ratio of certain hosts. The nodes that move between the two buildings (i.e., IL1 and IL2) and the PWFTA have the lowest connectivity with the incident commander at the TOC. Thus, these hosts should benefit most from the hybrid MANET-DTN routing scheme. Figure 5.2 shows the PDR of the two first responder teams that enter the two Incident Locations. Each bar in the diagram shows the average PDR of the nodes that belong to the same team for a certain buffer capacity. Without the store-and-forward mechanism (denoted by bs-0) about the half of all packets do not reach the command center. The store-and-forward mechanism increases the PDR of OLSR to over 93% for both teams (in the case of unlimited buffers, i.e., bs-1000). BATMAN achieves a slightly lower PDR of 86% for the team moving into IL1 and 91% for the team moving into IL2.

The packet delivery ratio of the nodes that are not prone to disruptions (i.e., the nodes in front of the facility) cannot be significantly improved by the store-and-forward mechanism. However, the PDR of these nodes is also not negatively affected by buffering packets. Hence, it can be stated that the network benefits from the hybrid MANET-DTN approach.

The end-to-end packet delays are short if the store-and-forward extension is disabled.

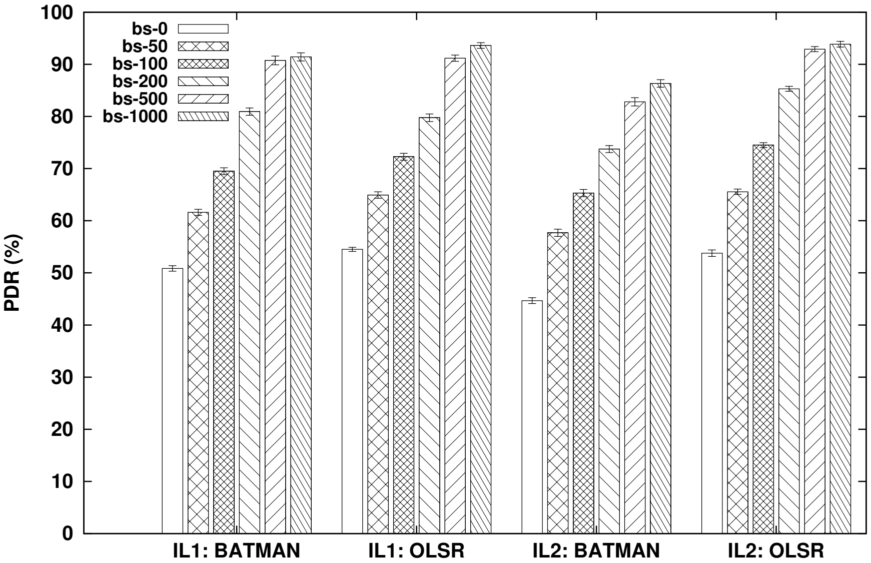


Figure 5.2: Average packet delivery ratio for varying buffer sizes (bs) and a *MaxLinkTimeout* of 1 s, for the two groups of nodes that move between the PWFTA and the Incident Locations IL1 and IL2.

All packets are delivered within 38 ms if only instantly available paths are used. If the store-and-forward extension is enabled, the average delay increases, mainly as a result of packet buffering. Table 5.2 presents the packet queuing times for varying buffer sizes and a *MaxLinkTimeout* of 1 s, since the queuing times contribute most to the end-to-end delay. As the queuing times are asymmetrically distributed, the table contains the quartiles (denoted by Q1, Q2 and Q3) instead of the mean values. The queuing times show that network disruptions are rather short and the majority of stored packets can be sent within a few seconds. This is an indication that most packets are stored because of short-lived link disruptions (i.e., the link validity check method returns false) and not as a result of long term disruptions, caused by the mobility of nodes. It can also be seen that OLSR has significantly smaller queuing times than BATMAN. This may be a result of shorter route repair times that allows OLSR nodes to send buffered packets earlier. Furthermore, this difference could also be an indication that in the case of OLSR more packets are buffered because the `hasValidLink()` method returns false. In this case the packets are sent as soon as a HELLO message is received (i.e., the link is considered to be valid again) which will happen much more frequently than topology changes due to the mobility of nodes.

As the basic route calculation algorithms of BATMAN and OLSR are not changed, the hybrid MANET-DTN scheme does neither directly impact the hop count of a packet, nor

Table 5.2: Quartiles of the queuing time T_Q for varying buffer sizes and a $MaxLinkTimeout$ of 1 s.

Buffer	OLSR: T_Q (s)			BATMAN: T_Q (s)		
size	Q1	Q2	Q3	Q1	Q2	Q3
50	0.23	0.48	0.84	0.16	0.91	3.00
100	0.25	0.51	0.97	0.36	1.45	5.21
200	0.26	0.56	1.20	0.68	2.20	7.87
500	0.29	0.61	1.69	0.81	3.06	10.07
1000	0.29	0.63	1.81	0.81	3.17	10.64

the overall routing control traffic. However, it is important to note that the store-and-forward mechanism has some implications on these two measures. Particularly, it decreases the relative routing overhead (i.e., the ratio between control traffic and data traffic) as more data packets can be delivered without introducing any additional control messages. Similarly, the average hop count is slightly increased as the store-and-forward mechanism mainly increases the PDR of the nodes that are farther away from the destination and utilize longer multi-hop paths.

5.3.4 Discussion

In this section, we evaluated how a hybrid MANET/DTN approach, based on the integration of a store-and-forward mechanism into a proactive MANET routing protocol, performs in the chemical incident scenario. The simulation scenario includes a realistic first responder mobility model and a wireless obstacle model that allowed us to model a realistic emergency response. The simulation results show that a store-and-forward mechanism is beneficial for the packet delivery ratio of both MANET routing protocols. Thus, it can be stated that a hybrid MANET-DTN routing scheme increases the robustness of the network as disruptions can be compensated. Another advantage of this approach is that it can be integrated on top of existing MANET routing protocols without changing the original protocols.

5.4 Evaluating CoMANDR in the Risavika Scenario

The main goal of the evaluation is to show how the Combined MANET/DTN Routing (CoMANDR) routing protocol performs in the Risavika full-scale exercise scenario and to compare it with other protocols from the MANET and the DTN domains as well as with combined approaches. The evaluation includes several experiments with different transmission ranges and message characteristics to show the impacts of these parameters on the performance of the routing protocols.

5.4.1 Scenario Description and Simulation Setup

The evaluation uses the Risavika exercise scenario that is described in Section 3.3.1. The number of first responders changed in the course of the exercise, as units arrived or left the scene. For the simulation, we fixed the total number of first responders and their assignment to tactical areas. All simulation scenarios include 65 nodes which is the estimated average number of first responders that were on the scene during the exercise.

As described in Section 5.1, we used OMNeT++ to prepare connectivity traces that are provided as input for simulations performed with the ONE simulator. The connectivity traces were created for 4500 s of simulation time with a resolution of one second (i.e, there are 4500 samples for the set of neighbors per node). We prepared traces for different transmission ranges that show different connectivity characteristics. This approach combines the advantages of OMNeT++ in terms of more realistic physical and MAC layer models with the availability of well-tested implementations of several DTN routing protocols.

Voice communication is the most prominent type of traffic in emergency response operations including the Risavika exercise. Nowadays, most of the coordination and information exchange between first responders is based on voice communication. However, we did not model voice communication for two reasons. First, voice communication in emergency response operations is usually not delay-tolerant. For instance, if a firefighter who operates in a dangerous environment cannot instantly communicate with his/her team leader, he/she has to leave the danger zone and get into safety. Hence, delays in voice communication are not tolerable in these operations, which makes store-and-forward routing approaches impractical. Second, first responders use special wireless communication systems for voice communication (e.g., TETRA) that provide long communication ranges but very limited bandwidth, compared to other wireless technologies such as Wi-Fi. Thus, we believe that different wireless technologies are suitable to transmit real-time and non real-time traffic. In this work we focus on additional services that tolerate delays and may use common wireless technology such as Wi-Fi. Examples for such additional services is the Help Beacons application [5], electronic triage systems [57] or video delivery (see Chapter 6).

Where not denoted otherwise, every node regularly sends messages to the node that is located in the local command post (i.e., the TOC according to the disaster area mobility model). During the full-scale exercise several applications followed this traffic pattern and sent information to the local incident command post where the incident commander was located and the received data was visualized. For instance, the location and further information about distress signals that were collected by the Help Beacons application were shown on a map of the Risavika harbor. Similarly, the position and status of victims wearing the electronic triage tags were visualized.

To simulate end-to-end routing, we implemented a link state protocol for the ONE simulator that uses Dijkstra's algorithm to calculate the shortest paths in the network. We call this protocol E2E as it denotes a generic end-to-end-routing protocol. Hop count is used the as metric since the ONE does not provide link quality information. All nodes have the same view on the network. Thus, the implemented MANET routing is optimal. In reality, routing protocols have to cope with imperfect information about the network (e.g., information about links or routes is missing or wrong). Hence, routing protocols have problems to find end-to-end paths in mobile scenarios. Additionally, the throughput of end-to-end paths drastically decreases with the path length [60]. To compensate this, we added a feature to the link state routing algorithm to restrict the maximum length of routes that are reported. Thus, it is possible to show, on a generic level, how end-to-end routing behaves if it fails to find longer multi-hop paths in the network (e.g., because of the mobility of nodes). The maximum hop count is set to 5 in all experiments.

We also implemented a version of E2E, called E2E-SaF, that uses packet buffering to cope with temporal disruptions. In particular, E2E-SaF uses end-to-end paths when available and stores packets if no such path is available. The E2E-SaF protocol represents hybrid MANET/DTN protocols that offer packet buffering on top of MANET routing. One example is the protocol that has been described in Section 4.4 or a similar work by Delosieres and Nadjm-Tehrani [39].

The total simulation time is 4500 s which covers the part of the exercise where most

Table 5.3: Parameters for the generation of connectivity traces.

Mobility model	
No. nodes	65
Model	Disaster Area Mobility [12]
Speed	1 to 2 m/s
Wireless model	
Propagation model	Free-space path loss ($\alpha = 2$)
Transmission range	30 m to 80 m
Wireless obstacle model[112]	
Wall attenuation (terminal)	18 dB
Indoor attenuation (terminal)	0.5 dB/m
Wall attenuation (ship)	50 dB
Indoor attenuation (ship)	1 dB/m

victims were evacuated and treated during the full-scale exercise. All experiments are repeated 23 times[1] using different seeds for the traffic generator and the mobility model. Important simulation parameters are listed in Table 5.3 and Table 5.4. Please note that message generation is started after 500 s of simulation time to give the routing protocols some time to set up (e.g, calculate routing tables, or meeting probabilities). Similarly, message generation is stopped after 3500 s to give the routing protocols some time to deliver messages before the simulation ends.

5.4.2 Metrics

The first metric that is used to evaluate the routing approaches is the *packet delivery ratio* (PDR), showing the ratio between delivered packets and created packets. The *hop count* shows how many nodes a packet has traversed until it reached the destination. The *transmission cost* metric denotes the ratio between transmitted packets and successfully received packets. For single-copy schemes such as MANET routing, the transmission cost is proportional to the average hop count of all successfully received messages. For the multi-copy schemes the transmission cost is mainly influenced by the number of message replicas.

[1] Please note that a prime number has been chosen for the number of repetitions due to a restriction concerning simulation settings in the ONE simulator (cf. Question 5 of the ONE simulator FAQ: `http://www.netlab.tkk.fi/tutkimus/dtn/theone/qa.html#reports`, accessed Jun 15)

Table 5.4: Routing protocol parameters for the ONE simulator.

Parameters for PROPHET/CoMANDR	
$P_{init}(=\alpha)$	0.9
β	0.7
γ	0.995
Parameters for Spray and Wait	
No. of copies	6
Spraying scheme	binary (cf. Section 2.3.4)
Parameters for MaxProp	
Meeting prob. set size	65

The *delay* represents the time that is needed to transfer a packet from the source to the destination. Delay includes the buffering time and the transmission time for all nodes along the path.

One metric that is often used for evaluating mobile ad-hoc routing protocols is the routing control overhead. However, different MANET routing protocols greatly vary in the amount of control overhead they introduce [124]. As this study only includes a generic MANET protocol (i.e., E2E), it is not feasible to directly measure control overhead. Since CoMANDR and E2E-SaF are extensions of the E2E protocol, the overhead for these three protocols is comparable. It is also fair to assume that the routing control overhead of the underlying E2E routing protocol is significantly lower than the data overhead (i.e., the transmission cost) introduced by the multi-copy schemes that are evaluated in this paper. Additionally, the existing implementations of Epidemic Routing, PROPHET or MaxProp in the ONE simulator also do not take the control overhead of these protocols into account. Hence, we argue that not taking MANET control overhead into account should not hinder a fair comparison between the evaluated protocols.

5.4.3 Evaluation Results

This section includes the evaluation results. Where not denoted otherwise, figures show mean values of the 23 simulation runs and error-bars denote the 95% confidence interval. Please note that we omitted very small confidence intervals to improve the clarity of some of the presented figures.

Table 5.5: Network connectivity characteristics of the scenario.

Transmission range (in m)	Connectivity degree CD (avg)	Largest connected component (avg)	Avg. no of partitions
30	0.445	39.12	6.15
40	0.671	51.46	4.13

Table 5.5 shows the connectivity characteristics of the scenario for the two different transmission ranges that were also used in the simulations. It is worth noting that we also performed experiments with larger transmission ranges. However, the results for larger ranges are quite similar to the 40 m case and hence have been omitted.

Impact of the Buffer Size

This set of simulations assesses how the buffer size affects the performance of the different routing approaches. In particular, the buffer size is varied from 32 MB to 512 MB per node. One message is generated every 10 s (from 500 s to 3500 s) which results in a total number of 300 messages per simulation run. Each message has a size of 1 MB. Please note that the message size has been selected to show how limited buffers impact the performance of the routing protocols. For instance, with the given message size of 1 MB, a buffer size of 32 MB allows a node to only store roughly 10 % of all generated messages, whereas a buffer size of 512 MB represents the unlimited buffer case, since each node can store all the generated messages.

The flooding-based schemes Epidemic Routing and PROPHET do not perform well if the buffers are limited. Full buffers cause many packets to be dropped which results in a low PDR (cf. Figure 5.3). The packet delivery ratio of Epidemic Routing and PROPHET increases when the buffer size is increased. A dropped packet may be re-transmitted which increases the transmission cost (cf. Figure 5.4). Although MaxProp performs extensive packet replication as well, it offers the best delivery ratio among all routing schemes for all scenarios. This shows that MaxProp's congestion control and buffer management strategies can mitigate the effects of limited buffers. CoMANDR provides the second best PDR for scenarios with a buffer size of up to 128 MB. For larger buffers it is outperformed by Epidemic Routing. However, its transmission cost is up to two orders of magnitude smaller than the costs of MaxProp and Epidemic. Thus, CoMANDR offers the best trade-off between resource usage and packet delivery ratio. Since the connectivity to the node in the incident command post is very low, end-to-end routing could not deliver any packets in some simulation runs. Thus, the results for E2E routing are omitted.

The hop count of Epidemic Routing and PROPHET is higher when the buffer size is small (see Figure 5.6). The reason is that packets that are dropped because of full buffers may be re-transmitted. This may cause a packet to traverse the same node multiple times which increases the hop count. For the other protocols, the hop count is not affected significantly by the buffer size. E2E-SaF has the lowest hop count as it fails to deliver packets if the sender and receiver are far from each other. The average delay of delivered packets increases when the buffer size is increased, since it is possible to deliver more of the buffered packets which would have otherwise been dropped (cf. Figure 5.5). Figures 5.7, 5.8, 5.9 and 5.10 show how the protocols perform for a transmission range of 40 m which increases the connectivity of the network.

Figures 5.11, 5.12 and 5.13 show how the PDR improves over time for different transmission ranges. If the connectivity is low, MaxProp and Epidemic Routing benefit from the replication and can deliver more packets in a shorter amount of time, compared to the other schemes (cf. Figure 5.11). This advantage is reduced if the connectivity increases (cf. Figure 5.12 and Figure 5.13).

Impact of the Time-to-Live Attribute

This set of simulations assesses how the time-to-live (TTL) attribute affects the performance of the different routing approaches. The TTL is varied from 120 s to 960 s. One message is generated every 10 s (from 500 s to 3500 s) which results in a total number of 300 generated messages per simulation run. Each message has a size of 1 MB. The buffer size per node is large enough to store all generated messages. Thus, messages are only dropped if their TTL expires.

If the transmission range is 30 m, which results in a low connectivity, the TTL of messages has a large impact on the packet delivery ratio (cf. Figure 5.14). This is due to the fact that the destination node in the TOC is only intermittently connected. In particular, only the nodes in the APP meet this node. Thus, for small TTL values, the chance is quite high that a message times out before there is even an opportunity to deliver the message

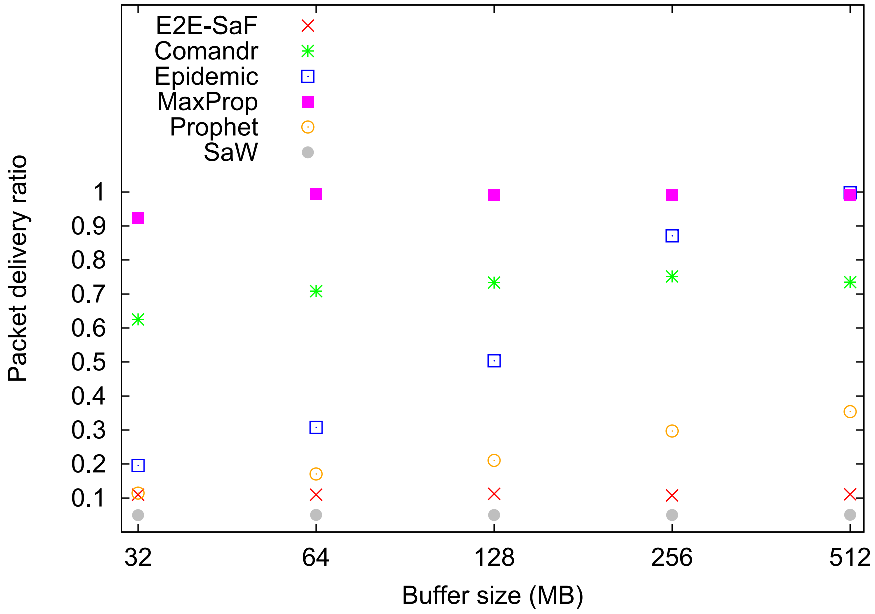


Figure 5.3: Impact of buffer size on the packet delivery ratio (transmission range 30 m).

to the node in the TOC. For a transmission range of 40 m, also other nodes meet the TOC which increases the chance to deliver a message before it times out. Thus, the PDR is not as dependent on the TTL as with a transmission range of 30 m (cf. Figure 5.16). The transmission cost decreases for most protocols if the TTL is increased (cf. Figure 5.15 and Figure 5.17). The main reason is that most protocols are able to deliver more packets when the TTL is higher.

Impact of the Transmission Bandwidth

In this set of experiments the impact of the transmission bandwidth on the performance of the routing approaches is assessed. The bandwidth is varied from 2 Mbit/s to 16 Mbit/s. To saturate the links, 6000 messages are created with a size of 1 MB each. In contrast to the other experiments where all messages are sent to the TOC, source and destination of each message are chosen randomly. The message TTL is set to 300 s but nodes can buffer all messages (i.e., unlimited buffer case). Thus, packets are only dropped if they cannot be forwarded due to congested links before they time out.

Although the hybrid single-copy schemes provide the highest hop count (cf. Figure 5.21), this routing approach clearly outperforms the other schemes if the transmission bandwidth is limited. In particular, E2E-SaF and CoMANDR outperform the other protocols in terms

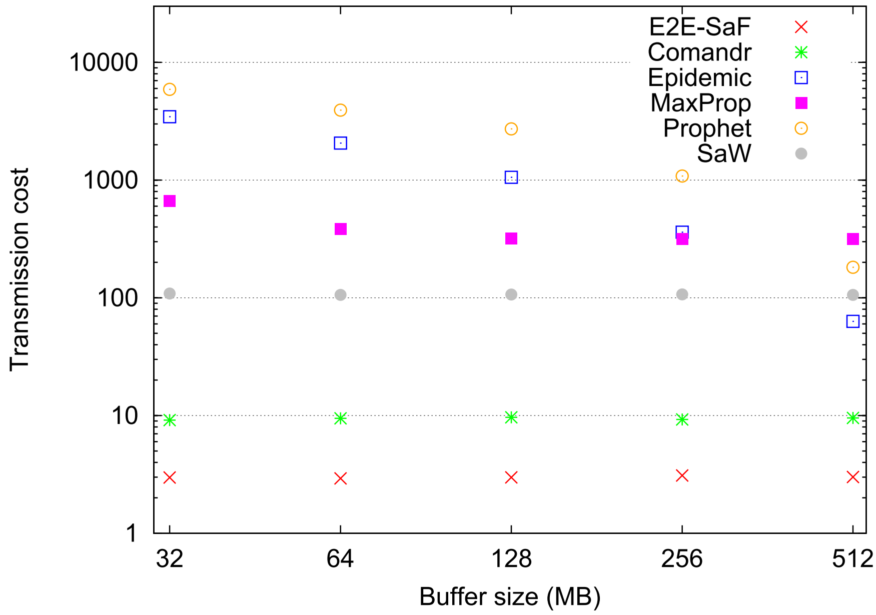


Figure 5.4: Impact of buffer size on the transmission cost (transmission range 30 m).

of PDR for a bandwidth up to 8 Mbit/s (cf. Figure 5.18) as they perform fewer transmissions and hence reduce network congestion. These two protocols also introduce a lower transmission cost than the other protocols (see Figure 5.19). As the flooding-based schemes also suffer from longer queuing times due to congested links, the single copy schemes also provide a lower delay (cf. Figure 5.20).

5.4.4 Conclusion

This section presented a comparison of different routing approaches in an emergency response scenario that is based on a full-scale emergency response exercise. The resulting network is diverse in terms of connectivity which imposes a challenge for routing protocols. Results show that DTN routing approaches are needed as network disruptions severely affect the performance of end-to-end routing approaches. In particular MaxProp could outperform the other protocols in terms of packet delivery ratio, which is one important performance metric. On the other hand, the density in some parts of the network causes MaxProp and other flooding-based schemes to produce high transmission and storage overheads. Thus, hybrid MANET/DTN schemes that offer a good trade-off between packet delivery ratio and resource usage may be preferred in emergency response scenarios. Especially if the emergency response operation takes a longer time, routing approaches that perform fewer

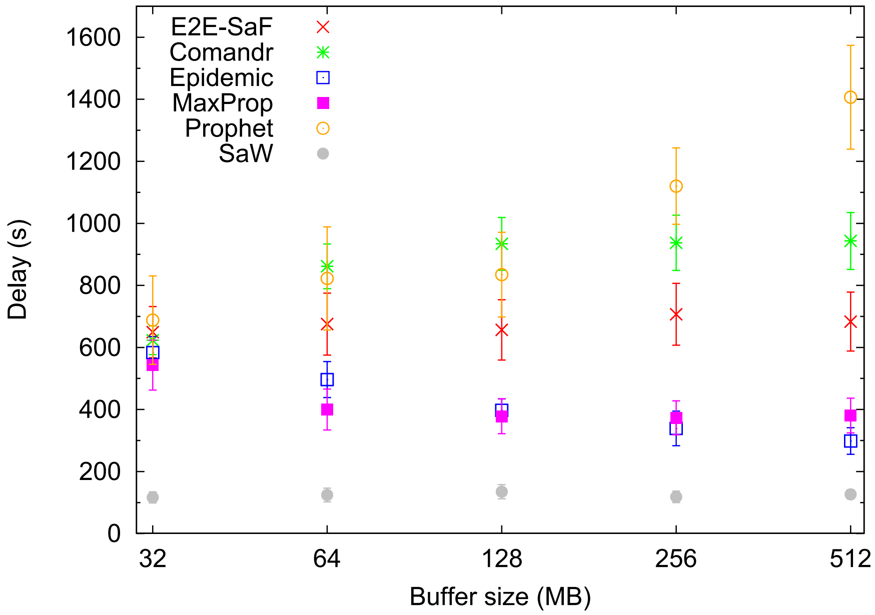


Figure 5.5: Impact of buffer size on the delay (transmission range 30 m).

transmissions and hence consume less energy are needed to save the battery of mobile devices. Thus, energy efficiency may be even more important than the packet delivery ratio in certain emergency response scenarios.

In the given scenarios, the packet delivery ratio of CoMANDR is always better than or equal to the delivery ratio of E2E and E2E-SaF routing. This shows that the mechanisms applied by CoMANDR on top of end-to-end routing, namely packet buffering and utility-based forwarding, are beneficial. In contrast to E2E routing, CoMANDR achieves packet delivery ratios that are comparable to state-of-the-art DTN routing algorithms in networks that offer low connectivity. CoMANDR can also compete with the evaluated DTN routing algorithms in terms of hop count and delay. This shows that CoMANDR is well suited for a broad range of networks.

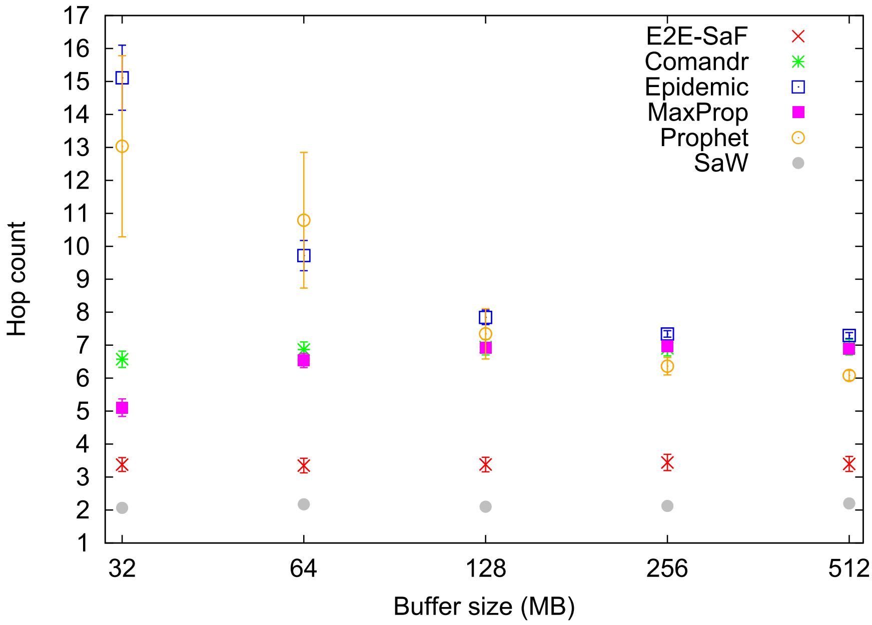


Figure 5.6: Impact of buffer size on the hop count (transmission range 30 m).

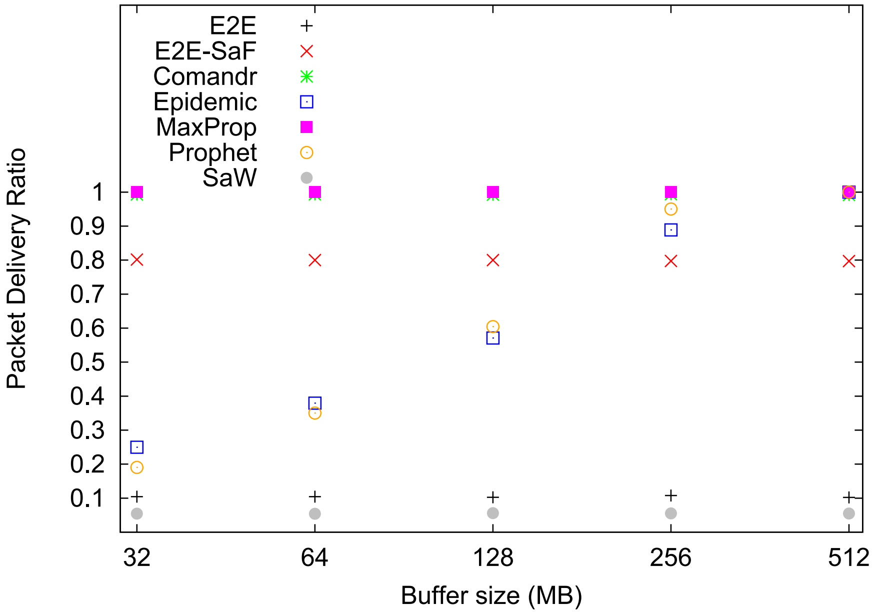


Figure 5.7: Impact of buffer size on the packet delivery ratio (transmission range 40 m).

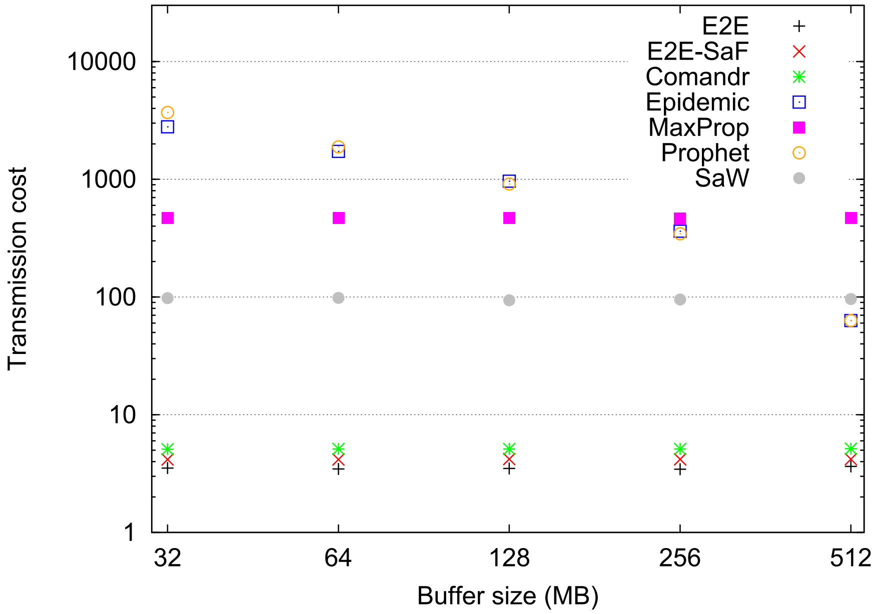


Figure 5.8: Impact of buffer size on the transmission cost (transmission range 40 m).

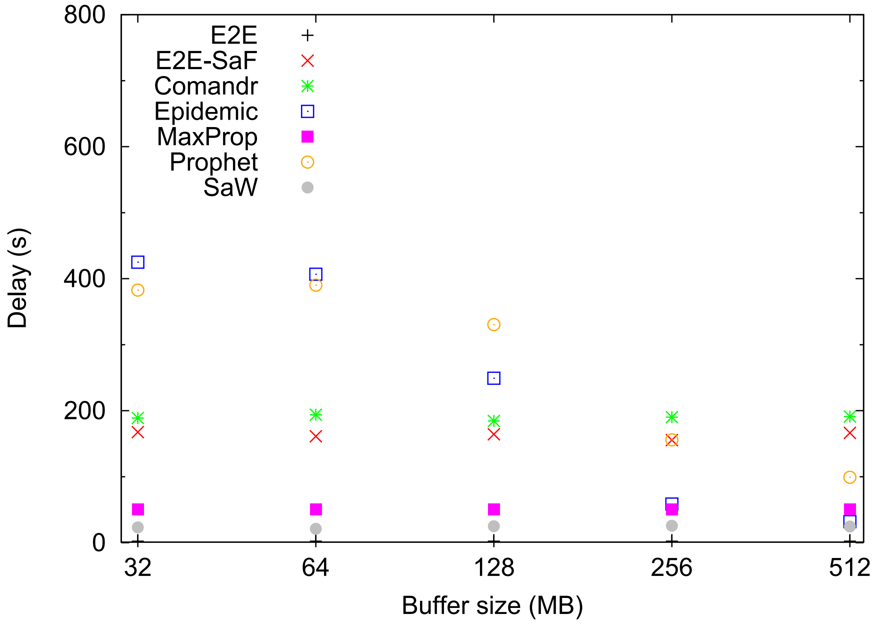


Figure 5.9: Impact of buffer size on the delay (transmission range 40 m).

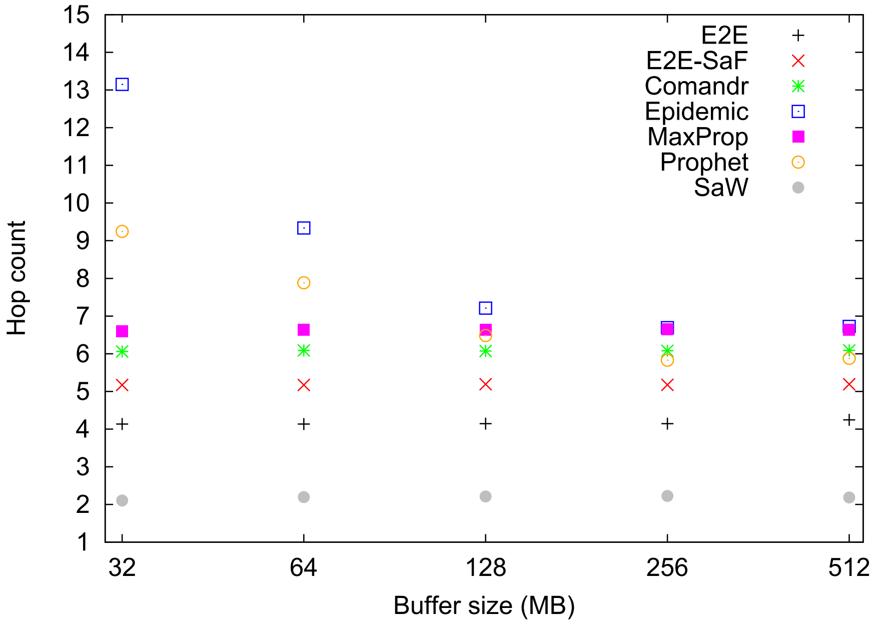


Figure 5.10: Impact of buffer size on the hop count (transmission range 40 m).

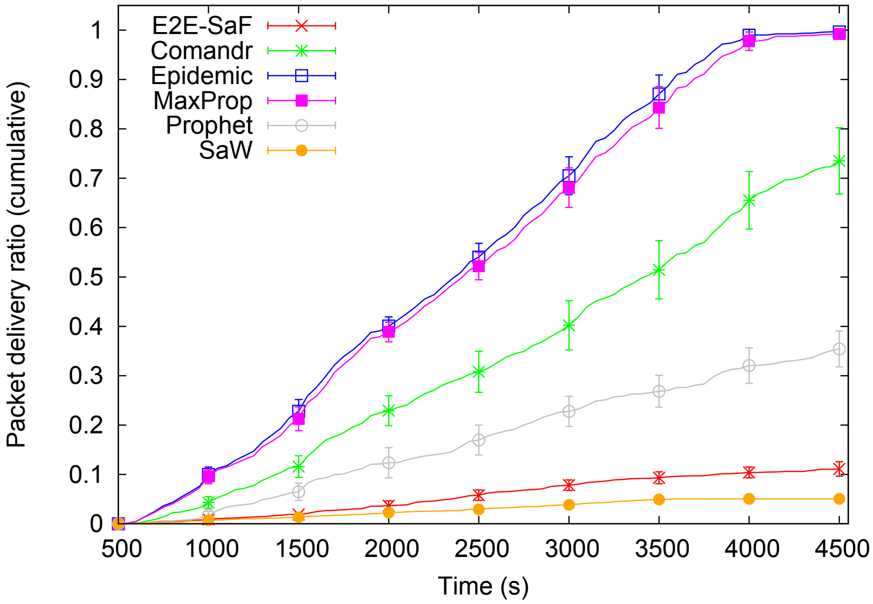


Figure 5.11: Cumulative packet delivery ratio (transmission range 30 m).

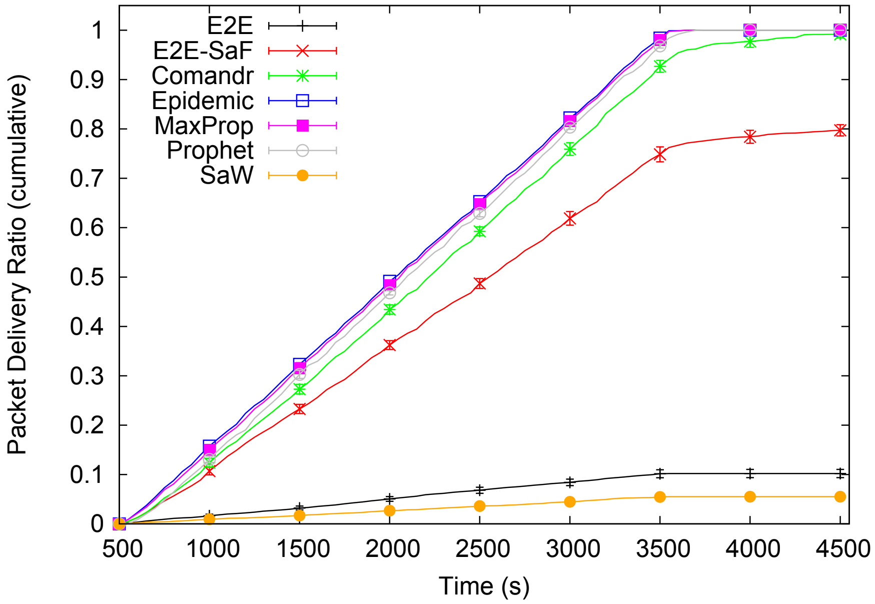


Figure 5.12: Cumulative packet delivery ratio (transmission range 40 m).

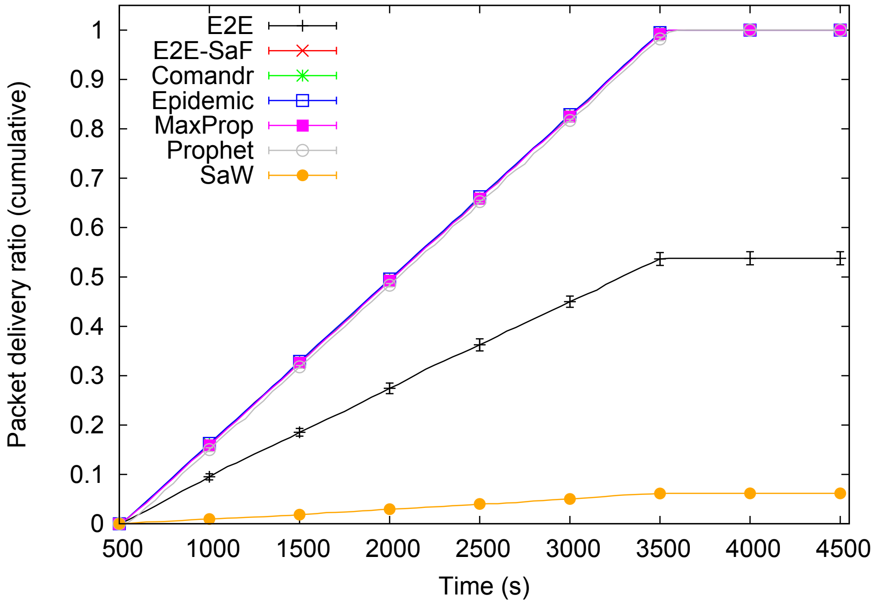


Figure 5.13: Cumulative packet delivery ratio (transmission range 50 m).

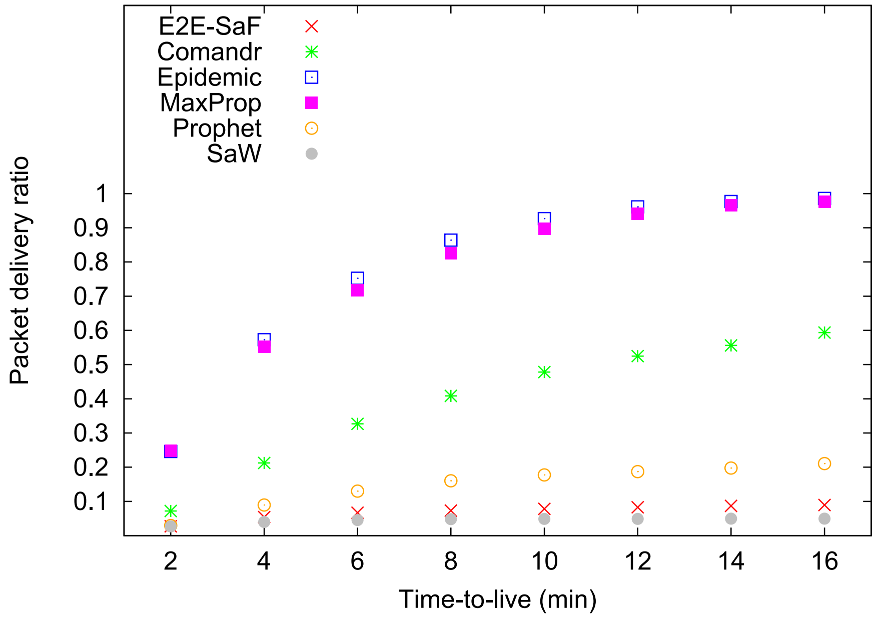


Figure 5.14: Impact of the message time-to-live on the packet delivery ratio (transmission range 30 m).

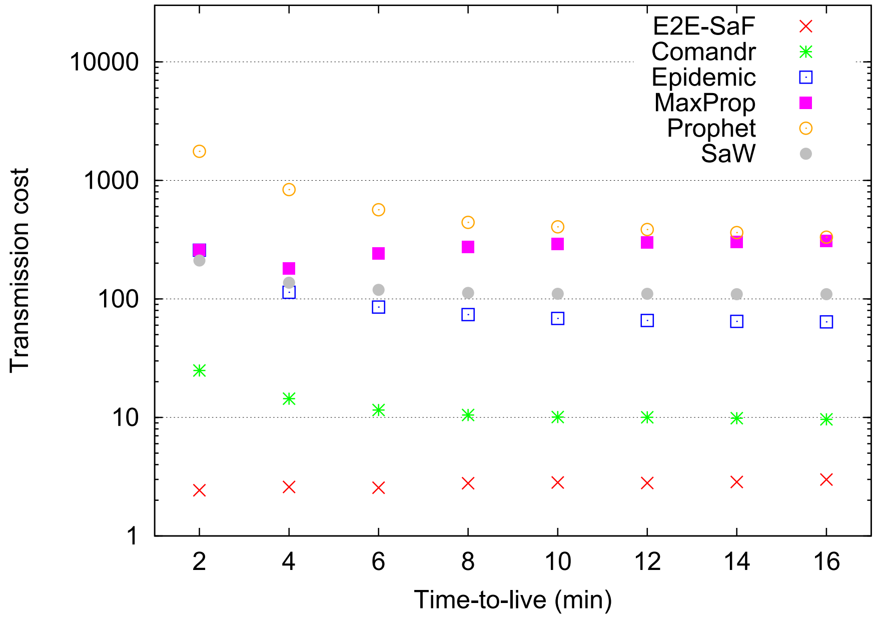


Figure 5.15: Impact of the message time-to-live on the transmission cost (transmission range 30 m).

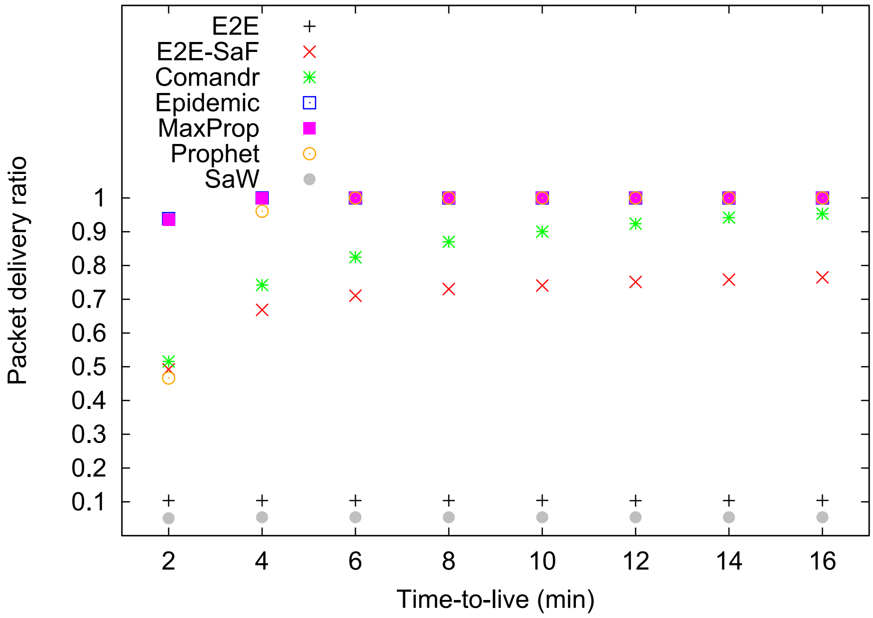


Figure 5.16: Impact of the message time-to-live on the packet delivery ratio (transmission range 40 m).

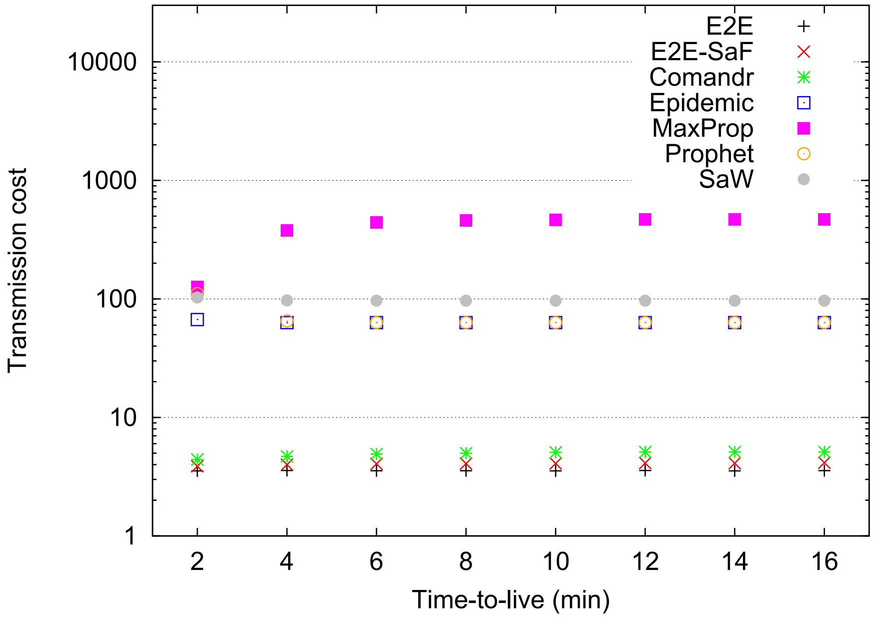


Figure 5.17: Impact of the message time-to-live on the transmission cost (transmission range 40 m).

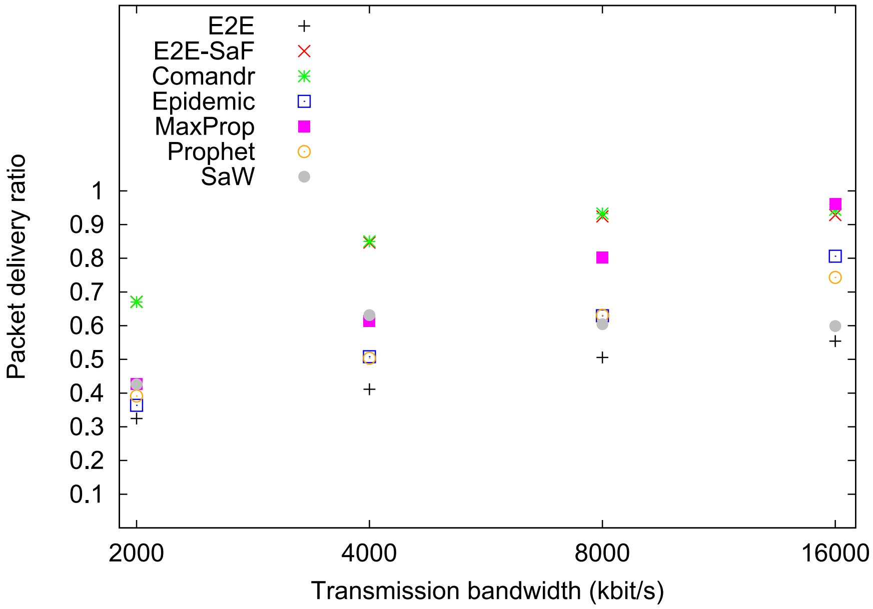


Figure 5.18: Impact of transmission bandwidth on the packet delivery ratio (transmission range 40 m).

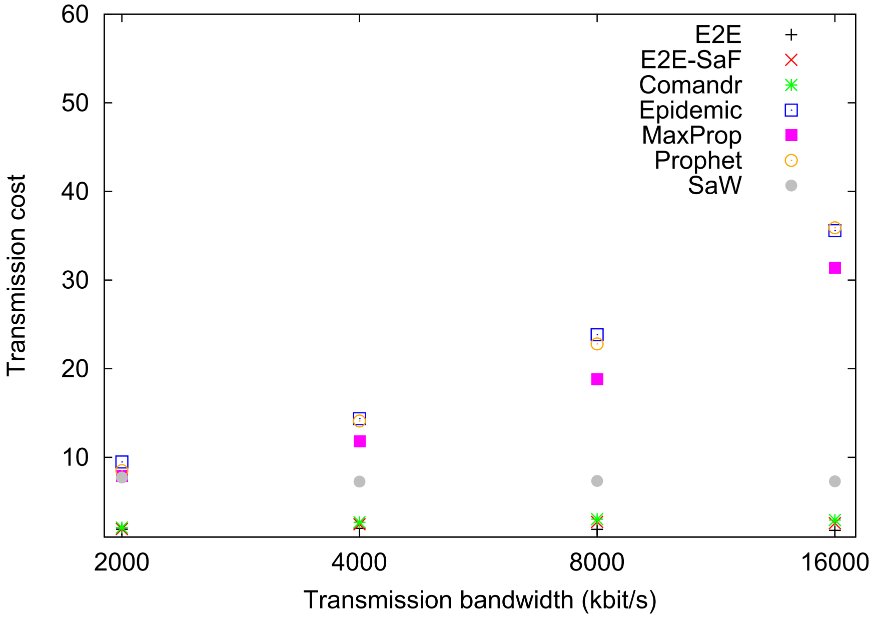


Figure 5.19: Impact of transmission bandwidth on the transmission cost (transmission range 40 m).

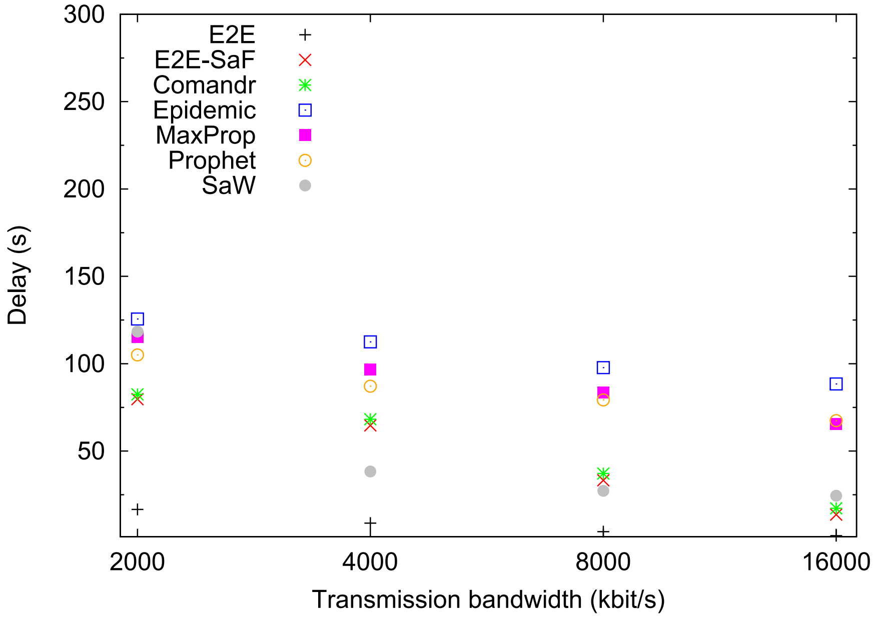


Figure 5.20: Impact of transmission bandwidth on the delay (transmission range 40 m).

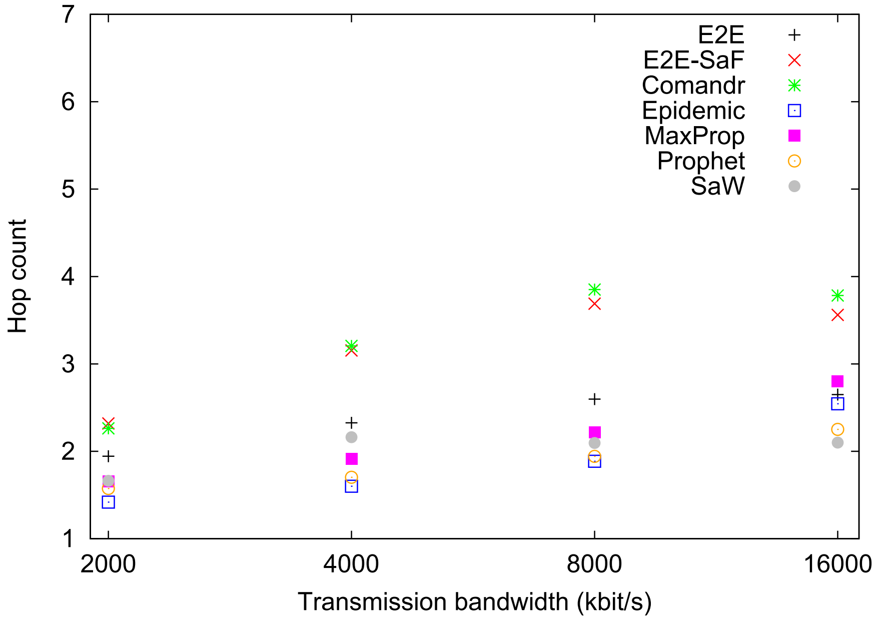


Figure 5.21: Impact of transmission bandwidth on the hop count (transmission range 40 m).

5.5 Evaluating CoMANDR in a Generic Scenario

The target application scenario for the hybrid MANET/DTN routing schemes that have been presented in the previous chapter (cf. Section 4.4 and Section 4.5) are emergency response scenarios. In the previous sections we have shown that these protocols offer good performance in such scenarios. The purpose if this section is to evaluate these schemes in a more generic scenario. In particular, this section presents an evaluation of CoMANDR in a generic scenario using random mobility where the size of the simulation area is varied in order to generate networks with different connectivity characteristics. Additionally, the evaluation includes the E2E-SaF implementation (see previous section) and several DTN routing protocols as well as general end-to-end MANET routing.

5.5.1 Scenario Description and Simulation Setup

We evaluate CoMANDR and compare it with several protocols, namely: E2E, which denotes our generic MANET routing protocol implementation for the ONE simulator (cf. Section 5.4.1), E2E-SaF, which enhances E2E with packet buffering, PROPHET and Epidemic Routing. All protocols are evaluated in several scenarios that offer different connectivity characteristics. In a first set of experiments we varied the transmission range and simulation area size to get a diverse set of networking scenarios, ranging from well-connected to sparse networks. We calculated the connectivity degree for all scenarios (see Chapter 3 for details about the metrics) and selected three scenarios offering different levels of connectivity. In particular, we selected three scenarios that use the same transmission range of 100 m but have a different simulation area size. The selected scenarios include a well-connected scenario, a sparse scenario and an intermittently connected scenario that lies between the other two.

The mobility model that is used in all scenarios is the random walk model (see Section 2.5.1). Each node selects its next destination by randomly selecting a direction, speed and distance, after waiting for a random pause time. Since the maximum distance between two consecutive waypoints is limited, nodes moving according to this model tend to stay close to each other for a longer time, compared to the random waypoint model. It is important to note that random mobility rather puts protocols which estimate the meeting probability (e.g., PROPHET and CoMANDR) at a disadvantage because these protocols assume that the future encounter of nodes is predictable. However, we argue that the low movement speed of nodes (i.e., the max speed is 2 m/s) and the fact that consecutive waypoints are close to each other, mitigate the effects of random mobility to some extent. In particular, it can be assumed that two nodes that have met recently are also more likely to meet again in the near future, compared to two nodes that are far away from each other. Moreover, it has been shown that PROPHET is still able to perform reasonably well in scenarios with random mobility [73].

Every simulation is run for 4500 s and all experiments are repeated 23 times using different seeds for the mobility model and the traffic generator. All scenarios include 100 nodes. Traffic is generated by creating a new packet with random source and destination every 0.3 s. Hence, a node generates a new packet every 30 s on average. Traffic generation is started after 500 s to allow the routing protocols to set up. No traffic is generated after 2500 s to allow the routing protocols to deliver buffered packets before the simulation ends. All packets have an infinite time to live and the buffer size has been set to a value that allows each node to buffer all generated messages. Thus, the simulation results do not include effects of dropped packets due to timeouts or full buffers. Important simulation parameters are listed in Table 5.6.

5.5.2 Metrics

Similarly to the previous evaluation of CoMANDR (cf. Section 5.4), this evaluation uses the following metrics: *packet delivery ratio* (PDR), *hop count*, *transmission cost* and *delay*.

The connectivity of the network is expressed in terms of the *connectivity degree* (CD), the *largest connected component* (LCC) and the *number of partitions* comprising at least two nodes (cf. Chapter 3).

5.5.3 Results

The connectivity characteristics of the scenarios are presented in Table 5.7. It can be seen that the three scenarios cover a broad range of connectivity. The scenario with the smallest simulation area dimensions is well connected (i.e., the mean CD is about 0.88 and on average nearly 93% of the nodes are connected in one large partition). On the other hand, the scenario with a simulation area of 1000 m x 1000 m only offers a CD of about 0.16 and less than a third of all nodes are part of the largest partition. The connectivity characteristics of the third scenario are between the other two.

Table 5.6: Simulation parameters

Mobility model	
No. nodes	100
Model	Random Walk
Movement speed	1 to 2 m/s
Pause time	0 to 60 s
Distance (min,max)	0 to 50 m
Wireless settings	
Transmission range	100 m
Transmission rate	4 Mbit/s
Traffic model	
Packet creation interval	500 to 2500 s
Packet creation rate	1 msg every 30 s (per node)
Packet size	100 kB
Packet buffer size	700 MB (per node)
Parameters for PROPHET routing/CoMANDR	
$P_{init}(=\alpha)$	0.9
β	0.7
γ	0.995

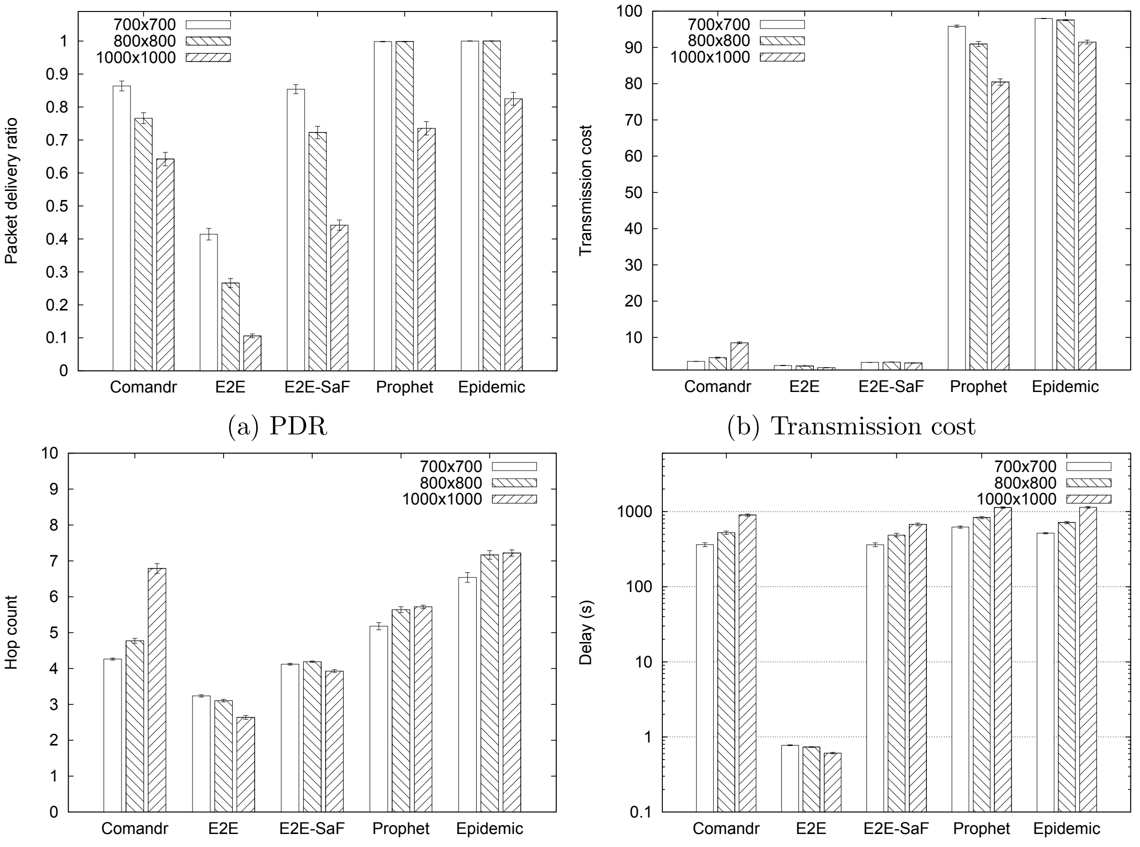
Table 5.7: Scenario characteristics in terms of network connectivity.

Size of area (in m x m)	Avg. connectivity degree CD	Largest connected component (avg)	Avg. no of partitions
700x700	0.882	92.886	1.915
800x800	0.634	74.95	3.853
1000x1000	0.157	30.276	17.982

The packet delivery ratio for all evaluated protocols in the three scenarios is shown in Figure 5.22a. Unless otherwise stated, figures show mean values of all simulation runs and error bars denote the 95% confidence interval. Traditional end-to-end MANET routing (i.e., E2E) is clearly outperformed by the other protocols and achieves the lowest PDR in all scenarios. Epidemic Routing can deliver most packets in all scenarios. This is due to the fact that the link bandwidth is very high and nodes can store all packets in their buffers, which is the ideal case for Epidemic Routing. No packets are dropped because of full buffers which maximizes the performance of Epidemic Routing. PROPHET can achieve a similar PDR in well-connected and intermittently connected scenarios. The performance results of CoMANDR and E2E-SaF are comparable in the well-connected scenario. The reason for this is that source and destination are very likely to be in the same connected component at some point in time and the packets can be delivered via an end-to-end path. Hence, E2E-SaF works similarly to CoMANDR in this scenario and both protocols achieve nearly the same PDR. However, CoMANDR outperforms E2E-SaF concerning the packet delivery ratio in the other two scenarios. In the sparse scenario, CoMANDR could deliver nearly 50% more packets than E2E-SaF. This performance gain is achieved by the utility-based forwarding scheme of CoMANDR that forwards packets towards the destination. Thus, CoMANDR can deliver packets to destinations that are never in the same connected component as the source, which improves its performance compared to E2E-SaF.

The protocols are diverse in terms of transmission cost as shown in Figure 5.22b. Due to its aggressive replication scheme, Epidemic Routing nearly performs 100 packet transmissions to deliver one packet. Although PROPHET can reduce this number by not forwarding packets to neighbors that have a lower delivery predictability, it still replicates packets extensively. E2E produces the lowest transmission cost as it only delivers packets via the shortest available end-to-end path. As the path has to be available instantly, it drops packets if it fails to find such an end-to-end path. E2E-SaF has a higher transmission cost than E2E, as buffering packets allows it to deliver more packets via longer paths. CoMANDR has a higher transmission cost if the connectivity is low. However, compared to the multi-copy schemes Epidemic and PROPHET, its transmission cost is still very low. Thus, CoMANDR offers the best trade-off between packet delivery ratio and transmission cost among all protocols. We believe that this is a very important feature of CoMANDR as resources are often scarce in mobile networks. Reducing the number of transmissions and hence reducing the wireless channel utilization and battery consumption, while still providing a good packet delivery ratio, is an important issue in many scenarios.

The hop count is shown in Figure 5.22c. In general, it can be said that the hop count is correlated with the packet delivery ratio. In particular, the protocols that achieve a higher packet delivery ratio achieve this by utilizing longer paths which increases the average hop count. Since E2E routing only delivers packets via end-to-end paths, its hop count is limited by the fact that the available end-to-end paths do not comprise many hops, especially in



(a) PDR

(b) Transmission cost

(c) Hop count

(d) Delay

Figure 5.22: Performance comparison for scenarios with different connectivity characteristics.

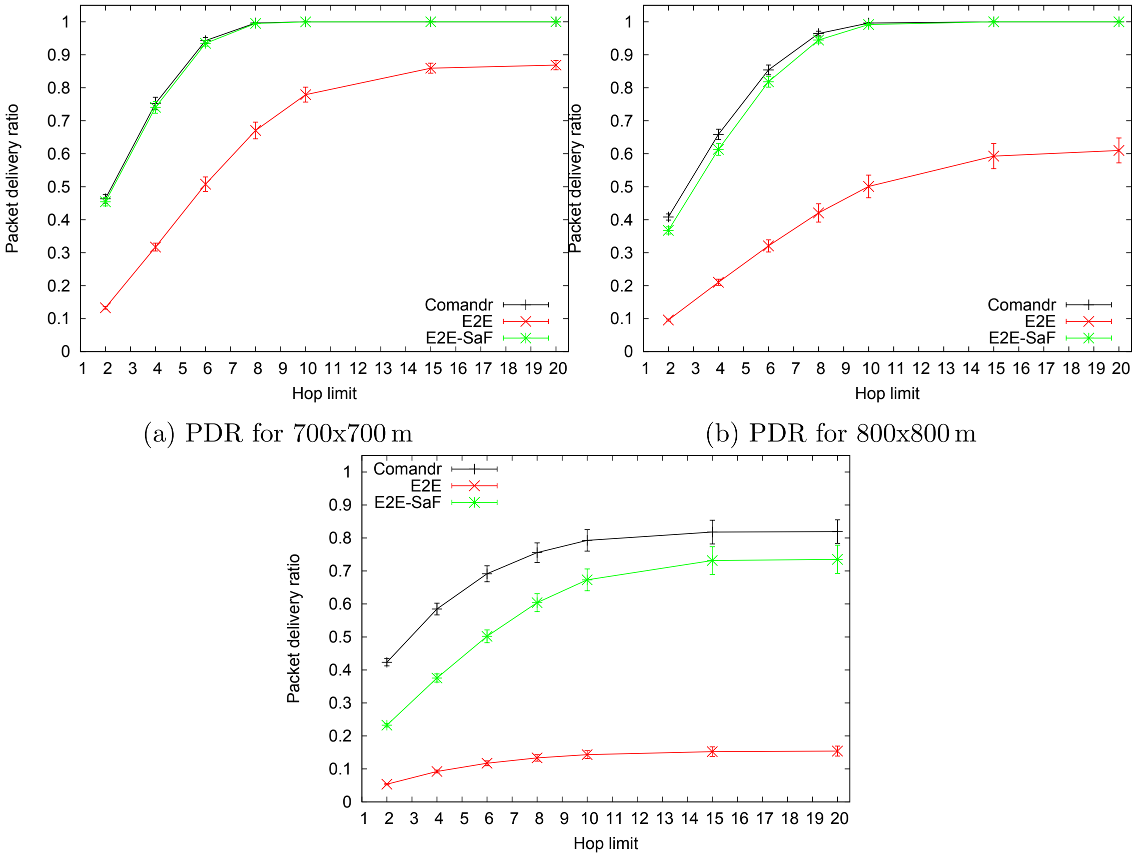
the sparse scenario. Furthermore, since we limited the maximum length of end-to-end paths that are used in order to simulate imperfections of MANET protocols in real networks (cf. Section 5.4.1), the maximum hop count is limited as well. As mentioned before, E2E-SaF can deliver more packets via longer paths as it stores packets if no end-to-end path is available, or the end-to-end path breaks while the packet is on its way to the destination. Similarly, the multi-copy schemes Epidemic Routing and PROPHET have a higher hop count as they are able to deliver more packets via long paths. The hop count of CoMANDR is similar to the one of E2E-SaF for the well-connected and intermittently connected scenarios. In the sparse scenario, CoMANDR's utility-based forwarding technique finds more paths but also needs more hops. However, as only one message copy is passed in the network, this does not cause a high transmission cost.

Evaluation results in terms of delay are shown in Figure 5.22d. Since the E2E protocol only uses instantly available end-to-end paths, it has the lowest delay, however, at the cost of a low PDR. The other protocols have a significantly higher delay due to packet buffering. Similar to the hop count, the delay is correlated with the PDR.

To evaluate the effect of the previously described hop count limitation, we also performed experiments with different values for the maximum length of utilized end-to-end paths. For the previous experiments, we limited the maximum path length to five which is a rather conservative estimation and limits the performance of E2E routing and the protocols depending on it (i.e., CoMANDR and E2E-SaF). Figure 5.23 shows how the PDR is affected by the length limitation of end-to-end paths. An interesting finding is that the store-and-forward mechanism of E2E-SaF and CoMANDR is a good means to increase the PDR, when the MANET protocol cannot find longer multi-hop paths. For instance, in the intermittently connected scenario (see Figure 5.23b), CoMANDR with a maximum end-to-end path length of four outperforms E2E routing with practically no restriction (i.e., hop limit 20). Even in the well-connected scenario, ideal MANET routing (i.e., E2E) has a lower PDR than CoMANDR and E2E-SaF for path length limitations greater than five (see Figure 5.23a). This is an indication that CoMANDR may also perform better than traditional end-to-end MANET protocols in well-connected but quickly changing networks, where traditional MANET protocols fail to find end-to-end paths because of the mobility of nodes.

We also performed experiments to assess the performance of CoMANDR using different values for α, β and γ. Similar to the results of the parameter study that is presented in Appendix B, the aging factor γ has a higher impact on routing performance than α and β. Especially in scenarios with low connectivity, γ should be set to a high value as this increases the PDR, without increasing the transmission cost significantly. Based on these results, we have chosen the values listed in Table 5.6 which offered a good performance in all scenarios.

In the given scenarios, the packet delivery ratio of CoMANDR is always better than or equal to the delivery ratio of E2E and E2E-SaF routing. This shows that the mechanisms applied by CoMANDR on top of traditional end-to-end routing, namely packet buffering and utility-based forwarding, are beneficial. In contrast to E2E routing, CoMANDR achieves packet delivery ratios that are comparable to state-of-the-art DTN routing algorithms in the intermittently and low connected scenarios. It is worth noting that sufficiently large buffers were provided in all scenarios. This is beneficial for Epidemic Routing and PROPHET since the packet delivery ratio is not negatively affected by packet drops caused by full buffers. On



(a) PDR for 700x700 m

(b) PDR for 800x800 m

(c) PDR for 1000x1000 m

Figure 5.23: Packet delivery ratio for different end-to-end path hop limits.

the other hand, CoMANDR is much more efficient. Thus, the performance of CoMANDR will obviously be less affected by limited resources. This shows that CoMANDR is well suited for a broad range of networks.

5.5.4 Discussion

This section presented results from more generic scenarios where nodes move randomly on the simulation area. Similar to the other evaluations in this chapter, the scenarios offer diverse connectivity characteristics. Evaluation results show that CoMANDR can compete with, or can outperform, other state-of-the-art routing protocols from the MANET and DTN domains. One important advantage of CoMANDR is that it offers a very good trade-off between packet delivery ratio and transmission cost. Since the intended application scenarios of CoMANDR include networks consisting of resource constrained mobile devices, saving resources such as battery is important.

5.6 Conclusion

This chapter presented several simulation-based evaluations of the two combined routing approaches that have been introduced in the previous chapter. Additionally, the evaluations included protocols from the MANET as well as the DTN domains in order to compare approaches from different domains in emergency response scenarios. To the best of our knowledge, there have been no previous evaluations of combined MANET/DTN approaches in emergency response scenarios. The presented results showed that combining MANET and DTN routing is beneficial in emergency response scenarios and that approaches from the DTN domain and the MANET domain have shortcomings. One of the main reasons for these results are the diverse connectivity characteristics of the networks. On the one hand, certain parts of the networks are well-connected which is beneficial for MANET routing protocols. On the other hand, the networks get partitioned regularly which decreases the performance of MANET routing and requires mechanisms from DTN routing such as store-carry-forward routing. Hence, we argue that it is important that the routing algorithms that are used in such scenarios can cope with diverse network characteristics and operate in well-connected as well as in disrupted networks.

One interesting topic for future work would be to also compare our hybrid MANET/DTN approaches with the state-of-the-art approaches that have been presented in Section 4.3. Based on the classification we presented in Section 4.2, we believe that approaches that integrate DTN mechanisms into MANET routing are better suited for emergency response scenarios than approaches from the other two classes. The reason for that is that the networks are in general well-connected and hence MANET routing will often be the best routing strategy. Hence, a comparison with approaches from this class would be particularly interesting.

CHAPTER 6 Disruption-tolerant Multimedia Delivery

Multimedia delivery is usually seen as a time-critical task where the multimedia content needs to be delivered within certain delay limits. This is a challenging task in best effort networks that do not provide any delay guarantees. Wireless networks provide some additional challenges such as varying links due to the mobility of nodes, packet loss and out-of-order delivery. Thus, several different techniques such as cross-layer optimizations (e.g., adapting a video based on information from routing protocols or the wireless channel), packet prioritization or MAC layer adaptations have been proposed, in order to tackle the challenges of wireless networks [72]. To provide low delays and reduce jitter is certainly an issue for interactive multimedia delivery scenarios such as video conferencing or IP-telephony. However, there may be some use cases where these constraints may be relieved, for instance, because the multimedia content is not consumed right after delivery. In other cases the topology of the network may not allow to deliver multimedia content instantly, for instance, if sender and receiver are in different network partitions. In such cases, large delivery delays cannot be avoided. As we have shown in Chapter 3, networks for emergency response operations are prone to such disruptions. The lack of end-to-end paths makes it impossible to deliver multimedia content instantly, which causes many existing multimedia delivery systems and protocols to fail. To tackle this issue, this chapter presents a multimedia delivery system that can operate in disrupted networks and hence may help improve the situational awareness in emergency response scenarios. The proposed system is based on HTTP Adaptive Streaming (HAS) but uses a modified version of HTTP which supports bridging network partitions and thus allows the system to deliver multimedia content in partitioned networks.

This chapter is structured as follows: First, Section 6.1 analyzes multimedia usage in emergency response scenarios. Afterwards, Section 6.2 introduces the basics of state-of-the art protocols for multimedia delivery and the challenges they face in DTN scenarios. In Section 6.3 we describe our disruption-tolerant multimedia delivery system. The system is evaluated in Section 6.4, before Section 6.5 describes a prototype implementation for

Android OS. Finally, Section 6.6 concludes the chapter. Please note that this chapter is partly based on previously published work [100].

6.1 Multimedia Usage in Emergency Response

Real-world studies with practitioners [69] have shown that mobile video can improve the efficiency of emergency response operations. The studies identified three typical use cases for multimedia in such scenarios. First, first responders may record videos while they drive to the incident scene. These recordings can provide information about the traffic situation and hence be used to re-route other teams to alternative routes in the case of traffic problems. Another use of mobile video is for enhancing on-scene situation reporting by improving the situational awareness and helping to create a common operational picture. For instance, an incident commander may record a video showing how the incident scene looks when responder teams arrive at the scene. Finally, videos may be used after the incident to replay key phases of the response work for documentation and training purposes. The studies that are presented in [69] focus on use cases where the incident commander records videos that are displayed in an off-site command center. Depending on the size or type of the disaster, other use cases may be imaginable. For instance, in a forest fire scenario, first responders could deploy video cameras that observe certain spots on the incident scene. Furthermore, first responders could record videos on the incident scene which are consumed at local command posts.

In addition to studying the use cases of mobile video in emergency response operations, the consumption of videos has been studied [17]. Based on the temporal dimension, one can differentiate the following uses cases. The first type of use is the *live use* where videos are consumed while they are broadcast. For this type of use it is important that the delivery delay is small (e.g., on the order of seconds). The *near live use* describes cases where a video is consumed a few minutes after it has been recorded, for instance, to check if the right amount of resources has been dispatched on the scene. The third use case is the *scheduled use* where videos are watched in scheduled meetings or conferences during the incident. Finally, the *post incident use* describes how videos are consumed for completing incident reports or providing additional material for investigators after the incident. Examples for all but the live use case could be found during a study of real-life emergency response operations [17]. The main reason for the lack of live use is that the involved persons usually have more important, time-critical tasks to perform that prevent them to immediately watch live video streams. Although the study did not find any live video use case, this finding cannot be generalized, since there may be other use cases for it (e.g., remotely observing a particular area on the incident scene that is too dangerous for first responders to stay). However, it may be argued that this type of use is rather uncommon in emergency response operations.

From these studies two important conclusions can be drawn. First, video use for emergency response operations is delay-tolerant which means that videos are usually not consumed while they are broadcast but used as a form of asynchronous communication [17]. Second, the videos usually have rather short durations. In particular, videos are usually less than a minute and only up to a few minutes in some cases [69]. This is due to the fact that first responders neither have the time to record nor to consume long video sequences. Instead, professional first responders selectively record important scenes which they think are useful for improving the situational awareness at the command center.

An example scenario where delay-/disruption-tolerant multimedia delivery is needed is shown in Figure 6.1. First responders have created local wireless networks (e.g., by deploying wireless routers and by carrying mobile devices that provide Wi-Fi interfaces). In order to improve the situational awareness, a first responder records a video which provides visual information from an event at a certain location. This video cannot be delivered instantly to a node that is located in the local incident command post. Instead, the mobility of first responders needs to be exploited in order to bridge network disruptions. Based on the findings from the aforementioned studies, we assume that this visual information from the disaster scene can improve the situation awareness, although it may be received with a delay of several minutes. Naturally, the acceptable delivery delay depends on the situation that is recorded. However, in scenarios where the network coverage or bandwidth does not suffice to deliver multimedia content instantly, such a delay-/disruption-tolerant multimedia delivery may be the only alternative.

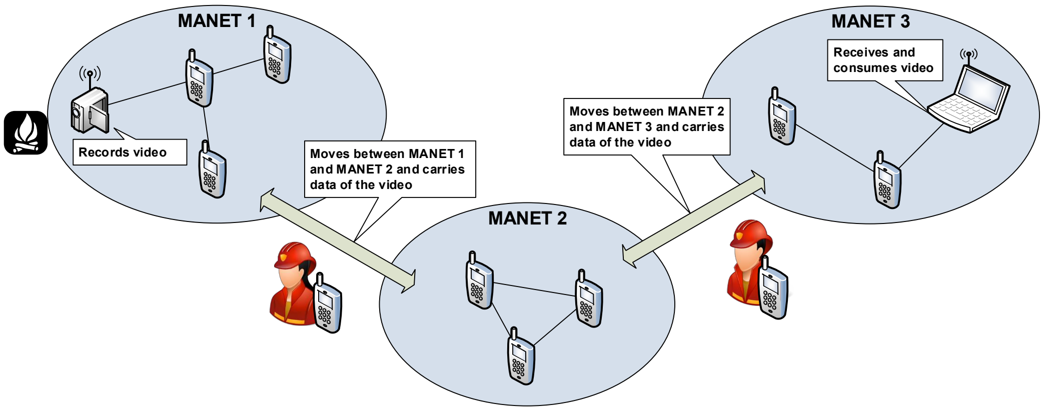

MANET 1
Records video
Moves between MANET 1 and MANET 2 and carries data of the video
MANET 2
Moves between MANET 2 and MANET 3 and carries data of the video
MANET 3
Receives and consumes video

Figure 6.1: Example scenario

6.2 Multimedia Delivery Protocols

This section aims to give an introduction of two state-of-the-art multimedia streaming approaches, namely the Real-Time Transport Protocol (RTP) and HTTP Adaptive Streaming (HAS). Neither of these approaches have been designed with intermittent connectivity in mind. Hence, this section also discusses the suitability of these two approaches for DTN scenarios.

6.2.1 Real-Time Transport Protocol

The Real-Time Transport Protocol (RTP) [109] is an application layer protocol that has been designed to deliver real-time data over IP-networks. Usually, UDP is used as transport protocol since its low delivery delay is favored over TCP's reliability for real-time applications. RTP can be used in different use cases such as IP-telephony, live streaming or for video-on-demand. RTP is usually accompanied by the Real-Time Streaming Protocol (RTSP) and the RTP Control Protocol (RTCP). RTSP [108] is used to establish and control a media session. It is a stateful protocol that offers text-based requests which allow a client to control the streaming session (e.g., starting, pausing or stopping the stream). RTCP [109] provides statistics about a media session which can be used to control the quality of service (QoS) of the multimedia session. In particular, RTCP periodically exchanges reports that include information about the quality of the streaming session between the multimedia server and the clients. The reports include information such as the number of transmitted packets, delay, jitter, error rates, etc. Based on this QoS information, the RTP server can adapt the multimedia session.

RTP does not assume that the underlying transport protocol is reliable. Thus, an RTP packet contains a sequence number to allow the receivers of a media stream to detect missing packets and restore the correct order of the packets. Additionally, the RTP packet header contains a timestamp field that includes timing information about its payload. Based on this timing information, receivers can synchronize media streams and also calculate jitter which is reported back to the RTP server using RTCP. The timestamp is dependent on the format of the payload that is carried within the RTP packet. Hence, RTP is not codec agnostic but a payload type header is needed to signal the payload that is carried within an RTP packet. The semantic of the timestamp field and other information about how payload data is packetized needs to be defined on a per-codec basis. For instance, RFC 6184 [125] defines the RTP payload format for H.264 video.

RTP has several drawbacks when used in the Internet. Since RTP is not codec agnostic, a payload specification has to be specified before a new media format can be carried via RTP. This makes RTP implementations more complex since different codecs usually require different packetization and parsing methods. Another disadvantage of RTP is that the server pushes data to the clients. This is problematic when clients are using network address translation (NAT) or are behind a firewall. As a result of these problems, nowadays, HTTP is often preferred over RTP for multimedia delivery. Although HTTP is actually less suited for multimedia delivery than RTP and provides none of its advanced features (e.g., media synchronization), its simplicity and compatibility with the existing Internet infrastructure makes it a valid alternative. Interestingly, HTTP-based multimedia delivery also offers some advantages in DTN scenarios, although it has not been designed with this application domain in mind. Before we discuss the advantages of using this transport mechanism in disrupted networks, we first give more details about HTTP-based multimedia delivery.

6.2.2 HTTP Streaming

In recent years streaming multimedia content in the Internet via the Hypertext Transport Protocol (HTTP) has gained momentum. HTTP offers some advantages compared to protocols that are dedicated to multimedia delivery, such as RTP. First, HTTP-based multimedia streaming can re-use the existing infrastructure such as content distribution networks (CDNs) or proxy servers. Additionally, HTTP is usually not blocked by firewalls and also works better in situations where clients use NAT.

In HTTP-based multimedia delivery, the URL of the multimedia content is included in a Web page. Usually, the content is made available in several encodings, container formats and quality settings with different bit rates. Based on user preferences or device capabilities, a client has to decide which representation to download. The simplest form of delivering multimedia via HTTP is to download the multimedia content in advance and start playback after the entire content has been received. However, this approach may introduce large start-up delays, depending on the length of the multimedia content and the download bandwidth. Furthermore, this type of delivery is not applicable for live-video use cases. HTTP progressive download is more useful for multimedia delivery since the playback can be started while the content is still being downloaded. In order to support HTTP progressive download, the content needs to be stored in a particular way (i.e., audio and video needs to be stored interleaved and information that is needed to set up decoding needs to be stored before the actual payload data). Progressive downloading works well if the available bandwidth is always higher than the bit rate of the multimedia content. Otherwise the playback may stall. This is especially a problem since it is not possible to switch to another representation with lower bit rate during playback, if the actual bandwidth is lower than the expected bandwidth.

As a result of the disadvantages of the aforementioned approaches, HTTP adaptive streaming (HAS) has been introduced. HAS is a technique that supports downloading multimedia via standard HTTP but also enables to react to situations where the available resources (e.g., bandwidth) do not meet the needed resources. The basic idea of HAS is to divide the multimedia content into segments which are downloaded separately. Similarly to other HTTP-based multimedia delivery solutions, the multimedia content is made available in different representations. However, it is possible to adapt to changes in the available resources by switching between different compatible representations during play back. Figure 6.2 shows an example of an HAS session where segments from three representations are chosen based on the available bandwidth. Adapting to the available bandwidth allows the client to prevent buffer underruns which would cause the playback to stall and hence reduce the viewing experience for the user. The available representations are described in a manifest file that needs to be acquired before the actual streaming can start.

The concept of HAS has been implemented in several streaming solutions, for instance,

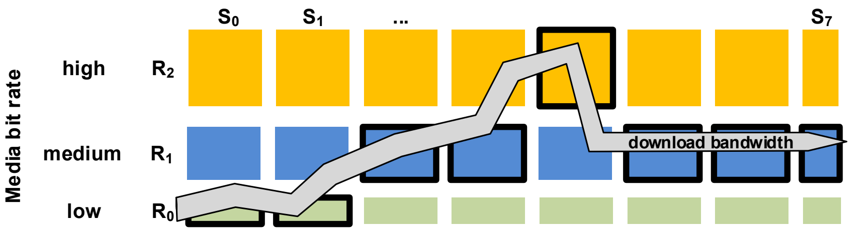


Figure 6.2: Example of HTTP Adaptive Streaming where segments (S_0 to S_7) are adaptively chosen from three representations (R_0 to R_2) based on the available download bandwidth.

Microsoft Smooth Streaming [131], Apple HTTP Live Streaming [91], Adobe's HTTP Dynamic Streaming [2] or MPEG's Dynamic Adaptive Streaming over HTTP (MPEG-DASH) [55]. While the former ones are proprietary solutions, MPEG-DASH is an open international standard. All systems have in common that the multimedia delivery is performed via HTTP but they differ in the supported content and container formats, in the way the multimedia content is described in the manifest file or how digital rights management (DRM) is performed. We have chosen MPEG-DASH as the basis for the delay-/disruption-tolerant streaming service that is described in Section 6.3.

MPEG-DASH

MPEG-DASH [55] is an international standard for delivering multimedia content via HTTP. The standard only defines how to describe the available multimedia content (i.e., the format of the manifest file) and the segment formats. Other parts of an HAS system, such as the adaptation logic for deciding which segments to download, are out of the standard's scope.

Information about the characteristics of the content and the available representations are stored in XML documents which are called Media Presentation Descriptions (MPDs). An MPD is structured as follows. Content is partitioned into one or more *periods*. Each period has a certain start point and a duration. Each period provides one or more *adaptation sets*. An adaptation set consists of *representations* that have different characteristics (e.g., frame rate, resolution, codec, media bit rate) but are compatible to each other. This means that it is possible to switch between segments from different representations within the adaptation set during playback. A representation contains information about the available segments and how to download them (e.g., a URL). In addition to the format of the MPD, MPEG-DASH also specifies the format of segments. In particular, the ISO Base Media File Format and MPEG-2 Transport Stream are supported. Further information about

MPEG-DASH can be found in the standard itself [55] or in [111, 117].

6.2.3 Multimedia Delivery Protocols in a DTN

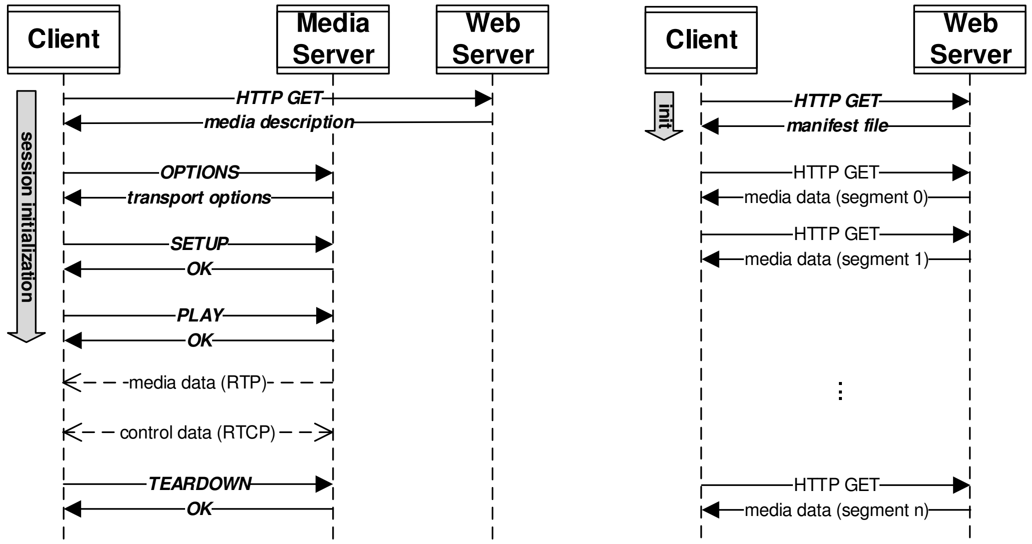
As described in Chapter 3, wireless networks for emergency response scenarios may become partitioned regularly. Thus, a multimedia communication system for emergency response operations has to take the lack of end-to-end paths into account. However, the multimedia delivery protocols that have been presented in this section assume end-to-end connections and low delivery delays between multimedia source and consumer. Neither of these two properties can be achieved in networks prone to disruptions. Thus, it is needed to re-think some of these assumptions to provide multimedia delivery in emergency response scenarios. This section reviews the multimedia delivery protocols that have been introduced in the last section in the context of disruption-tolerant networking.

HTTP-based multimedia delivery has some advantages over RTP in DTN scenarios. In HTTP-based delivery the multimedia content is separated into chunks that contain video or audio data with a certain duration (e.g., two seconds). Thus, every chunk is a semantically meaningful unit for a decoder, i.e., each chunk is independent of previous chunks and can be decoded right after delivery. Such a segmentation of application data is also suggested by the DTN reference architecture [33] because it allows the network and the receiver to treat each application data unit as independent unit of work. In the context of video delivery this means that a data packet should include enough information to be decoded after its reception which is the case for segments of a MPEG-DASH system but not for RTP packets. RTP packets may contain multimedia data that is dependent on data that is transported in one or several other RTP packets. In that case, the client has to wait for all dependent RTP packets before it can decode the multimedia data and play it.

Another advantage of HTTP compared to RTP for delivery in DTNs is that HTTP utilizes the entire available bandwidth for transmitting data, while RTP usually adjusts the sending rate to the media bit rate. For instance, assume a video file with a duration of ten seconds and a bit rate of 1 Mbit/s that is to be delivered via a link that provides 10 Mbit/s. The video file would be delivered in roughly one second using HTTP, whereas RTP would limit the sending rate to the media bit rate and deliver the video in about 10 seconds. However, in mobile ad-hoc networks it is often the case that links provide a high bandwidth but are not stable. Hence, it is beneficial to utilize the full capacity of an available link.

Another disadvantage of RTP-based delivery is that it constantly exchanges information about the multimedia session between the server and its clients in the form of RTCP sender and receiver reports. Although this provides an accurate way of controlling the QoS of the media session, it is hard to ensure that these periodic reports are delivered on time and to establish a well-working control loop in a DTN. Similarly, controlling the state of the RTP session via RTSP is difficult in a DTN since the commands may take a long time until they are received and acknowledged by the server. Compared to that, HAS has no complex control loops involved and usually the client decides which representation to download based on information that is locally available (e.g., current bandwidth or buffer fill state). However, this adaptation decision could also be performed at the server or in the network. Figure 6.3 depicts the steps needed to set up a media session in both RTP and HTTP-based delivery. It can be seen that HTTP-based delivery does include fewer steps to initialize and set up the streaming session which is beneficial in DTNs where round trip times may be long and hence the interaction between server and clients should be minimized.

We have selected HTTP-based multimedia delivery, in particular MPEG-DASH, since it is better suited for DTN scenarios than RTP because of the aforementioned reasons. An open issue of HAS in DTNs is that it is usually not possible to establish an end-to-end TCP connection between sender and receiver. However, HTTP itself does not presume such an end-to-end connection and thus it is also possible to use HTTP in DTNs. The next section describes how HTTP and in particular an HAS-based multimedia delivery system can work in delay-/disruption-tolerant networks.



(a) RTP session (b) MPEG-DASH session

Figure 6.3: Comparison of RTP and MPEG-DASH session setup and control.

6.3 A Disruption-Tolerant Multimedia Delivery System

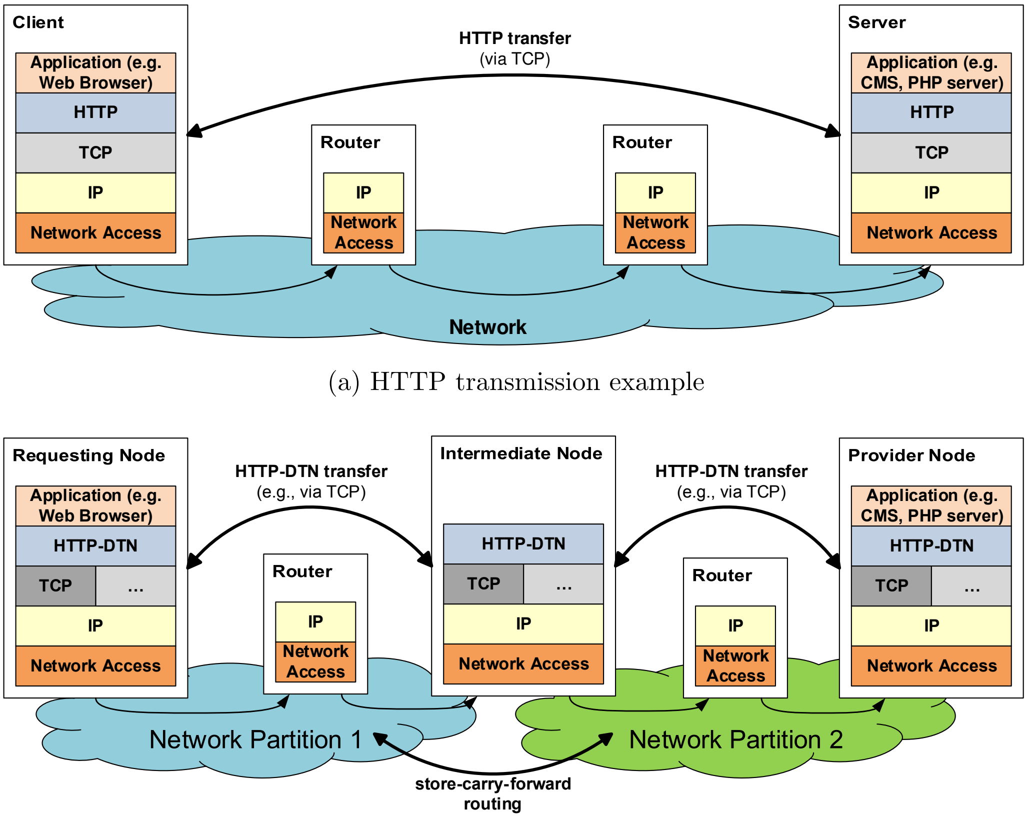
The Disruption-Tolerant Multimedia Delivery System (DT-MDS) uses adaptive bit rate streaming over HTTP, in particular MPEG-DASH. Thus, DT-DMS has the following characteristics. The multimedia content is partitioned into segments with a certain duration. The segments contain all modalities of the multimedia content such as a video stream and an audio stream. Additionally, segments are self-contained, which means that they can be decoded independently of each other. The multimedia content is made available in different qualities. These versions of the content are referred to as representations. Manifest files describe which representations are available and how they can be accessed (e.g., via a URL). The main difference between DT-MDS and other HAS systems is that DT-MDS uses a modified version of HTTP in order to work in disrupted networks.

6.3.1 Delivering Data in Disrupted Networks via HTTP

In order to use MPEG-DASH in a disrupted network, we adopt the ideas of Wood et al. [129, 130] of modifying HTTP to support data delivery in disrupted networks. The protocol is called HTTP-DTN and works similar to HTTP within networks that offer end-to-end connections between nodes, i.e., data is queried via GET and pushed via PUT or PUSH. In order to support data delivery in disrupted networks, HTTP-DTN requests are stored and forwarded in a hop-by-hop manner between nodes in different network partitions. Within one network partition, nodes may use any reliable transport protocol to transfer data between each other. This has the advantage that different transport protocols may be used in different partitions, depending on the network and device characteristics of the network partition. The differences between HTTP and HTTP-DTN concerning end-to-end semantics are depicted in Figure 6.4. To support this kind of operation, HTTP-DTN introduces additional headers. In particular, it uses the *Content-Source* and the *Content-Destination* headers to identify the original source of a request and its final destination and to route requests and files in the network using a DTN routing protocol.

Every HTTP-DTN node contains a storage for storing the received files and additional metadata which is used for routing and error detection (e.g., *Content-Source*, *Content-Destination*, MIME type, checksum). Intermediate nodes store the HTTP-DTN requests and the accompanying payload, which allows them to bridge partitions and deliver content despite the lack of end-to-end connectivity (i.e., perform story-carry-forward routing). Similar to HTTP, data can either be pulled from its origin or pushed to its destination. When two HTTP-DTN nodes come into contact, they issue PUT and GET requests for the files that have to be exchanged. The decision to exchange a file is based on the final destination of the file, which is stored in the *Content-Destination* header. Similarly, GET requests for files can be forwarded by intermediate nodes to the node that is identified in the *Content-Destination* header. In order to identify the original source of a file, the *Content-Source* header is used. Both headers may contain an IP address, DNS name or any other textual information to identify a node in the network. HTTP-DTN does not define how files or requests are routed in the network. Instead it assumes that every node provides a DTN routing protocol that is responsible for deciding how to route data in the network.

Figure 6.5 shows the architecture of an HTTP-DTN node. HTTP-DTN does not follow the client-server principle of HTTP. Instead every node may act as a server and as a client. Thus, every node has to provide an HTTP server that is used to transfer files to other nodes. The HTTP server is also used to deliver files that are created by local applications. Not every node may host applications but every node may be involved in the delivery of files on behalf of other nodes. To support the store-carry-forward routing paradigm, every node includes a storage module where received files and accompanying metadata are stored. Similarly, the storage module can be used to cache GET requests that cannot be fulfilled instantly.



(a) HTTP transmission example

(b) HTTP-DTN transmission example

Figure 6.4: Comparison of traditional HTTP and HTTP-DTN transmission.

The content and query manager is responsible for handing a received file to the application that requested it. If the file is already available in the storage module it can be served instantly, otherwise, it has to be requested from other nodes. If any of the neighbors of the node requesting the file can provide the file, the transfer is similar to traditional HTTP-based delivery. In particular, an HTTP GET request will be sent to the neighbor which will answer with an HTTP response. The response includes metadata that is stored in HTTP headers and the file that is stored in the body of the HTTP response. If the origin of the file is currently not available and the GET request cannot be fulfilled immediately, the content and query manager is responsible for caching the request locally and for forwarding it to neighbors. Thus, it also includes a DTN routing protocol.

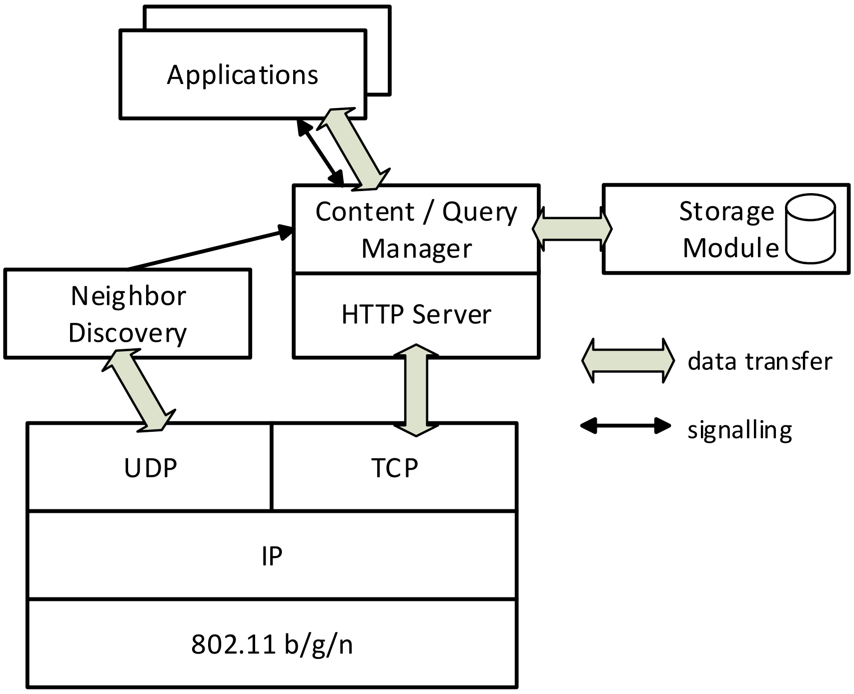
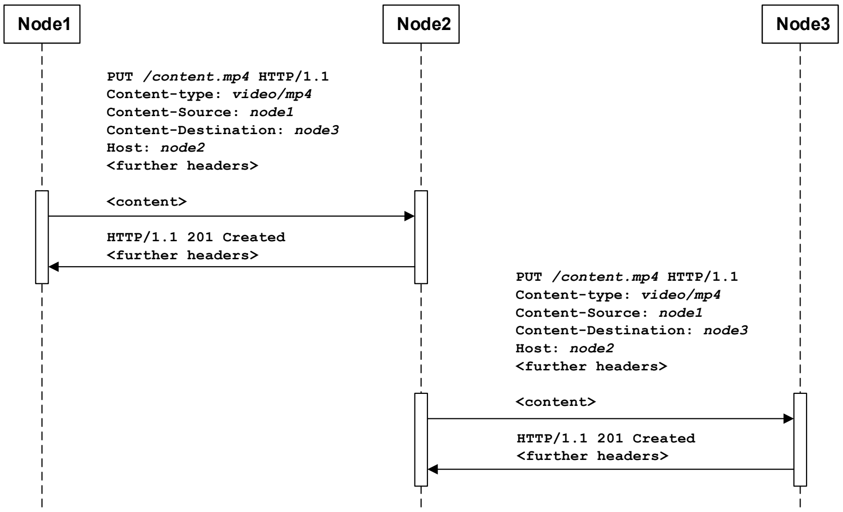


Figure 6.5: Internal architecture of an HTTP-DTN node.

6.3.2 Routing and Multimedia-Aware Forwarding

HTTP works with any reliable transport protocol [43] and is not tied to TCP, although TCP is the most widely used protocol to transport HTTP data. Similarly, HTTP-DTN does not define which transport protocol to use for transferring data between nodes. Instead, different transport protocols can be used, depending on the characteristics of the network and its devices. To route the HTTP-DTN requests in the network, any routing protocol for delay-/disruption networks may be used. The routing protocol is responsible for deciding to which HTTP-DTN node requests are forwarded in order to reach the destination. The *Content-Source* and *Content-Destination* headers are important for routing, since these headers identify the originator and the destination. To specify the destination of the next hop, the *Host* header is used. In contrast to the values that are stored in the *Content-Source* and *Content-Destination*, the value of this header may change and is only valid on a hop-by-hop basis. The example in Figure 6.6 shows how a file is delivered using HTTP-DTN. The example consists of three nodes and uses PUT to push the file from a source node (i.e., Node1) to a destination node (i.e., Node3) using two HTTP-DTN transfers. Please note that several headers are omitted to increase the clarity of the example.



```
PUT /content.mp4 HTTP/1.1
Content-type: video/mp4
Content-Source: node1
Content-Destination: node3
Host: node2
<further headers>

<content>

HTTP/1.1 201 Created
<further headers>
```

```
PUT /content.mp4 HTTP/1.1
Content-type: video/mp4
Content-Source: node1
Content-Destination: node3
Host: node2
<further headers>

<content>

HTTP/1.1 201 Created
<further headers>
```

Figure 6.6: HTTP-DTN example using PUT to deliver a file.

An HTTP-DTN node can use different forwarding strategies to decide the order in which segments are forwarded. The forwarding order is particularly important when delivering multimedia content. In order to keep the number of partially transmitted contents low, it is important to deliver many segments from the same video, instead of segments from different videos. Thus, we propose a multimedia-aware forwarding strategy that orders buffered items based on the compare function that is described in Algorithm 6.1. Manifest files have the highest priority and are exchanged before segments. Segments are prioritized based on the representation. In particular, segments from lower representations are sent before segments that offer a higher quality. The idea behind this prioritization is to increase the chance to deliver the content at least in a basic quality and only forward content in higher qualities when there are enough transmission resources available. Additionally, the recording time is used to prioritize segments from older videos. Manifest files and video files can be identified by the `getType()` method based on the MIME type that is part of the HTTP header and/or the file suffix. Additionally, we assume that the file names of segments contain all the required information (e.g., quality level, recording time, relative position within a video), which is needed to determine the forwarding order using the `getBitrate()`, `getCreationTime` and `getSegmentPos()` methods. The evaluation results that are described in Section 6.4 show that this multimedia-aware forwarding scheme increases the performance of the system compared to using first in, first out (FIFO).

Algorithm 6.1: Function to compare two messages, for ordering buffered messages based on the multimedia-aware forwarding strategy.

```
Data: msg1, msg2
Result: a negative value, if msg1 has a higher priority; a positive value, if msg2 has
        a higher priority; or 0, if both messages have the same priority
begin
    $type1 \longleftarrow getType(msg1)$;
    $type2 \longleftarrow getType(msg2)$;
    /* MPD's are prioritized over segments                                  */
    if $type1$ == 'mpd' and $type2 \neq$ 'mpd' then
        return $-1$;
    end
    else if $type1 \neq$ 'mpd' and $type2$ == 'mpd' then
        return 1;
    end
    /* older MPDs have a higher priority than newer MPDs                    */
    else if $type1$ == 'mpd' and $type2$=='mpd' then
        $timediff \longleftarrow getCreationTime(msg1) - getCreationTime(msg2)$;
        return $timediff$;
    end
    else if $type1$ == 'segment' and $type2$ == 'segment' then
        $sizediff \longleftarrow getBitrate(msg1) - getBitrate(msg2)$;
        if $sizediff \neq 0$ then
            return $sizediff$;
        end
        /* order segments with same bit rate based on their creation time
           */
        else
            $timediff \longleftarrow getCreationTime(msg1) - getCreationTime(msg2)$;
            if $timediff \neq 0$ then
                return $timediff$;
            end
            /* segments from the same video are prioritized based on their
               temporal order                                               */
            else
                return $getSegmentPos(msg1) - getSegmentPos(msg2)$;
            end
        end
    end
end
```

6.3.3 Neighbor Discovery

Every DT-MDS node includes a module for advertising itself in the network and detect other DT-MDS nodes. This is performed by broadcasting periodic messages that contain information about the transport options that the node offers. These messages include information about available transport protocols (e.g., TCP) and their settings (e.g., port number). Additionally, these messages may also include information needed for routing (e.g., meeting probabilities). Furthermore, we use these messages to exchange static node identifiers which decouple nodes from their local network addresses using late-binding. This has the advantage that nodes can communicate without knowing the current network addresses of their communication partners. Instead, they use the static node identifier in all HTTP-DTN requests. These static node identifiers are mapped to real network addresses when the requests are sent to another hop. For instance, if a local network uses TCP/IP, the static node identifier of a node would be mapped to a socket address consisting of an IP address and TCP port. For further information, we refer to Section 6.5 where the format of the discovery beacons is described.

6.3.4 Related Work

Several previous works have studied multimedia delivery in the context of disrupted networks. Klaghstan et al. [64] study video delivery in DTNs using scalable video coding (SVC) where the content is divided into several quality layers. Based on the importance of the layer, the degree of redundancy is changed (e.g., the number of message copies is adapted). The authors conclude that SVC is better suited for DTNs than single layer codecs, since it allows to receive the content in a lower quality and then gradually improve viewing quality while more layers are received. In [65] the same authors improve the performance by segmenting the layers into smaller chunks in order to adapt the delivery to available contact times. In DT-MDS proactive segmentation is used (i.e., the content is segmented by the source). However, since SVC can also be used in an HAS system [48], SVC may be an option to increase the performance of DT-MDS. However, using SVC would also break our assumption that all segments can be decoded independently of each other.

The Bundle Streaming Service (BSS) [71] adds streaming support to the bundle protocol. Although BSS is mainly intended for inter-terrestrial communication, it may also be used for scenarios such as emergency responses. Any BSS-capable node has to provide at least one best-effort and one reliable delivery protocol. To reduce delivery delays, bundles are first sent via the best effort protocol. Since all bundles need to be acknowledged, BSS can detect transmission failures and then switch to reliable delivery. In contrast to BSS, our system uses HTTP-DTN instead of the Bundle Protocol for delivery. This design choice has been made since using HTTP-DTN requires fewer changes to standard HTTP adaptive systems, compared to using the Bundle Protocol.

Cabrero et al. [30] suggest a temporal video adaptation technique for DTNs where the quality of a video is adapted by reducing the frame rate. The goal of this adaptation is to provide a constant frame rate that depends on the available network resources. The adaptation technique also changes the order in which stored frames are forwarded in order to cover a bigger span of the recorded video. This adaptation technique is mainly useful for continuous recordings which have not been the focus of this work.

6.4 Evaluation

This section presents an evaluation of the multimedia delivery system in the chemical incident scenario (cf. Section 3.2).

6.4.1 Scenario Description and Evaluation Setup

Two nodes that move between the Incident Locations (ILs) and the Patients Waiting For Treatment Area (PWFTA) and one node that is located in the PWFTA itself, record videos that need to be delivered to a node in the Technical Operational Command (TOC) area. The videos could either be consumed by an incident commander at the TOC or sent to an off-site command center via a network gateway (e.g., via a satellite uplink).

Each video is made available in two representations[1] with an average bit rate of 2.5 Mbit/s and 500 kbit/s, respectively. The length of the videos is randomly distributed between 15 s and 60 s and videos are recorded in a randomly chosen interval between 120 s and 360 s. Videos are created from 500 s to 3500 s and the simulation is run for 4500 s to give the routing protocols some time to set up and to deliver the videos before the simulation ends. The message buffers of all nodes are unlimited (i.e., each node can buffer all generated segments).

[1] It can be assumed that one representation is recorded by an integrated camera, while the second representation is generated via live transcoding.

The simulations are performed using a combination of the OMNeT++ and the ONE simulators. In particular, we used OMNeT++ to prepare connectivity traces for different wireless transmission ranges that were imported into the ONE simulator (cf. Section 5.4.1). Each experiment is repeated 23 times.

In a set of evaluations we show how DT-MDS performs using different routing algorithms. In particular, we selected Epidemic Routing, PROPHET, Spray and Wait (SaW) and the two hybrid routing schemes that we presented in Section 4.4 and Section 4.5. We refer to the latter two approaches as E2E-SaF and CoMANDR.

To simulate networks with different connectivity characteristics, the transmission range is varied between 20 m and 60 m. Varying the transmission range allows us to evaluate how the multimedia delivery system performs in different scenarios from well-connected networks to sparse networks. Additionally, we also evaluate the multimedia-aware forwarding strategy that has been described in Section 6.3.2 and compare it to FIFO.

It is important to note that the evaluations focus on rather short video sequences since they are more frequently found in emergency response scenarios. One could argue that for this type of use a ‘download and play’ solution suffices and segmenting the videos is not needed. However, segmenting the videos into smaller parts is still beneficial for the performance of the system, since it reduces the number of partially transmitted messages in the presence of link disruptions. Thus, we also evaluate the effects of using different segment sizes and the case where the videos are not segmented at all. Additionally, the streaming capability of DT-MDS, which requires segmenting the video content, may be useful in other application scenarios.

The first metric that is used in the evaluation is the ratio between created and received videos (*video delivery ratio*). A video is considered as received only if all of its segments could be received. Additionally, the average *received bit rate* of the delivered videos is evaluated by calculating the average of all received segments of a video. If a segment has not been received, the bit rate for this segment is set to 0, otherwise it is set to the bit rate of the highest received representation. Hence, the average bit rate is a measure for the received quality, since high quality representations also have a higher bit rate. Finally, we also evaluate the *delay* which denotes the time that is needed to receive a recorded video at the destination.

Table 6.1: Simulation parameters for the routing protocols.

Parameters for PROPHET/CoMANDR	
$P_{init}(=\alpha)$	0.9
β	0.7
γ	0.995
Parameters for Spray and Wait	
No. of copies	8
Spraying scheme	binary (cf. Section 2.3.4)

Table 6.2: Connectivity characteristics

Transmission range (in m)	Connectivity degree CD (avg)	Largest connected component (avg)	Avg. node degree
20	0.15	7.49	2.04
30	0.35	12.79	3.48
40	0.57	17.76	4.85
60	0.75	21.67	8.54

6.4.2 Results

This section presents the evaluation results. All figures include arithmetic means and the error bars indicate the 95% confidence interval.

The connectivity characteristics of the network for the transmission ranges that have been used for the evaluations are presented in Table 6.2. As described in Chapter 3, we use following metrics. The node degree shows the arithmetic mean of the number of 1-hop neighbors. The largest connected component denotes the number of nodes that are in the largest partition and can communicate via end-to-end paths. Finally, the connectivity degree (CD) denotes the probability that two randomly selected nodes are in the same connected component (i.e., an end-to-end path between the two nodes exists). According to the connectivity characteristics presented in Table 6.2, it can be seen that the evaluation includes different scenarios from well-connected to sparsely connected ones.

The video delivery ratio of the system for different routing protocols and transmission ranges is shown in Figure 6.7. In this experiment FIFO was used as forwarding strategy (i.e., the segment buffered for the longest time is forwarded first). In well-connected

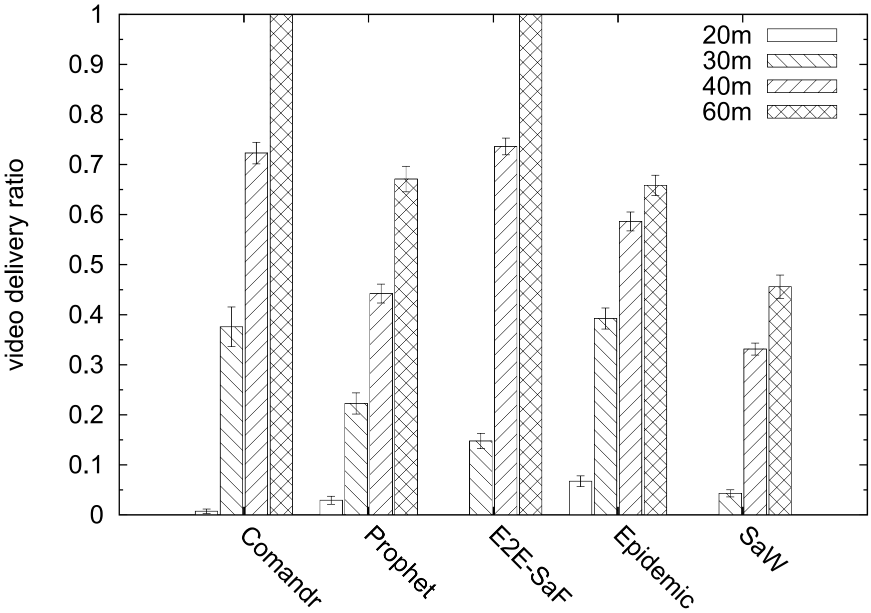


Figure 6.7: Video delivery ratio for different transmission ranges, using FIFO forwarding strategy (transmission bandwidth 2 Mbit/s, 2 s segments)

scenarios (i.e., transmission range of 60 m) all videos can be delivered using the hybrid MANET/DTN routing protocols, namely CoMANDR and E2E-SaF. The flooding based protocols PROPHET and Epidemic Routing introduce too much overhead and hence can only deliver about 65% of the videos. In the best connected scenario, Spray and Wait can deliver about 45% of the videos. The main reason for its poor performance compared to the other protocols is that the available message copies are often only distributed between nodes close to each other (e.g., the nodes in the PWFTA) which never get into contact with the destination node located in the command center.

In sparsely connected networks (i.e., transmission range of 20 m) less than 10% of the packets can be delivered by any protocol. This is due to the fact that only a few other nodes in the network get in contact with the node in the command center and hence there are only very few delivery opportunities. E2E-SaF cannot deliver any video in this case since the senders and the receiver are never in the same connected component. Similarly, Spray and Wait cannot deliver any video since the available message copies are never forwarded to nodes that get in contact with the node in the command center.

The multimedia-aware forwarding strategy (cf. Section 6.3.2) prioritizes lower-quality representations in order to increase the chance that a video is at least received in a basic quality. Figure 6.8 shows the video delivery ratio using this forwarding strategy. It can

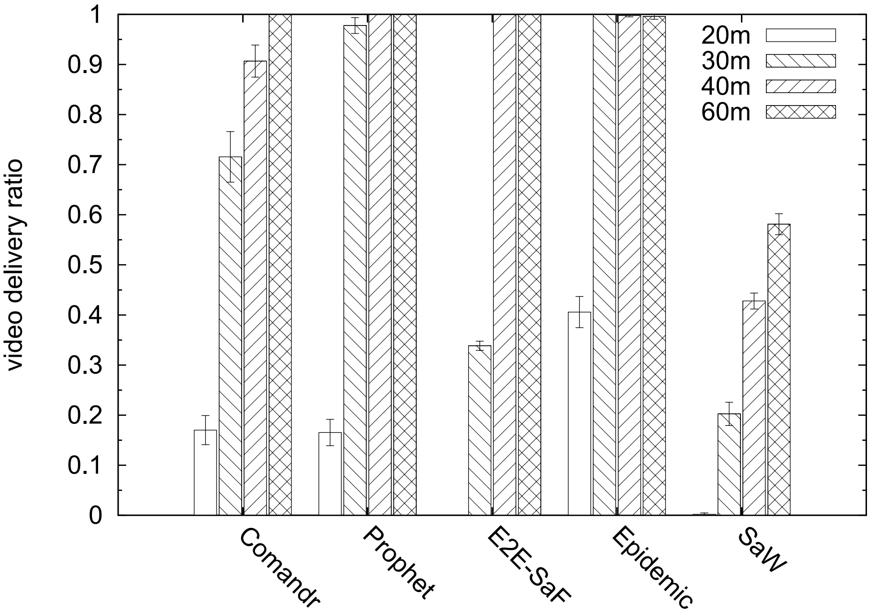


Figure 6.8: Video delivery ratio for different transmission ranges, using multimedia forwarding strategy (transmission bandwidth 2 Mbit/s, 2 s segments)

be seen that this strategy significantly improves the number of delivered videos compared to FIFO, by better utilizing the available bandwidth in order to deliver more segments of a video. For instance, even in the least connected scenario, about 40% of the videos can be delivered using Epidemic Routing, compared to the 7% that were achieved using FIFO strategy. These results show the importance of the forwarding strategy and that it is useful to take the semantic of the messages into account when deciding the order in which to transfer buffered segments.

In the last section we argued that segmenting the multimedia content is beneficial for the performance of the system. To support this claim, the effect of the segment length on the video delivery ratio is shown in Figure 6.9. It can be seen that the video delivery ratio decreases for all protocols when no segments are used (i.e., for each video only one segment with the duration of the video is created). We retrieved similar results for other transmission ranges and bandwidths. We also evaluated the effects of the segment length when using the multimedia forwarding strategy. Here the segment size has a lower impact on the video delivery ratio and in many cases we could not find statistically significant differences. However, if the received video bit rate is considered, segmenting is still beneficial as it improves the overall quality of the received videos (see Figure 6.10).

The delay for receiving a video is another important metric for evaluating the video

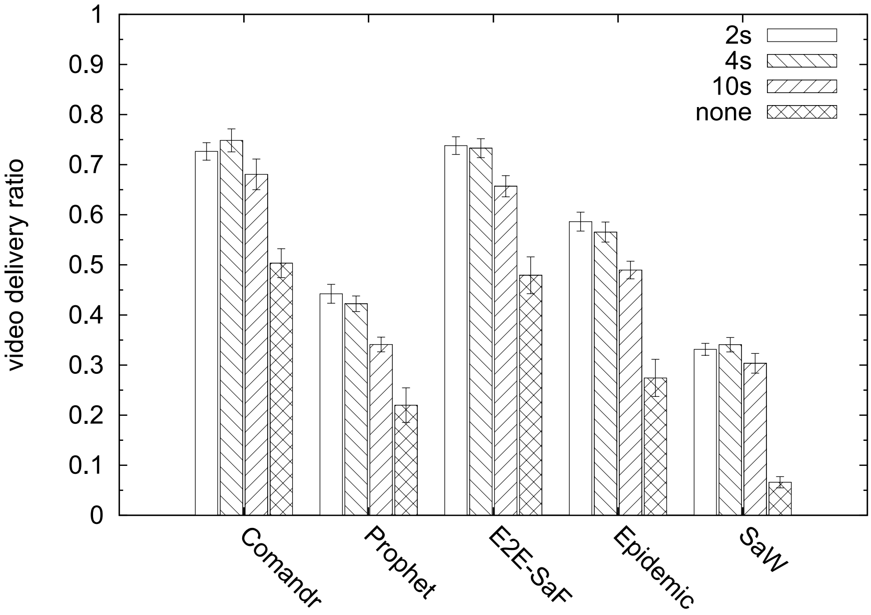


Figure 6.9: Video delivery ratio for different segment sizes (FIFO forwarding strategy, transmission bandwidth 2 Mbit/s, transmission range 40 m)

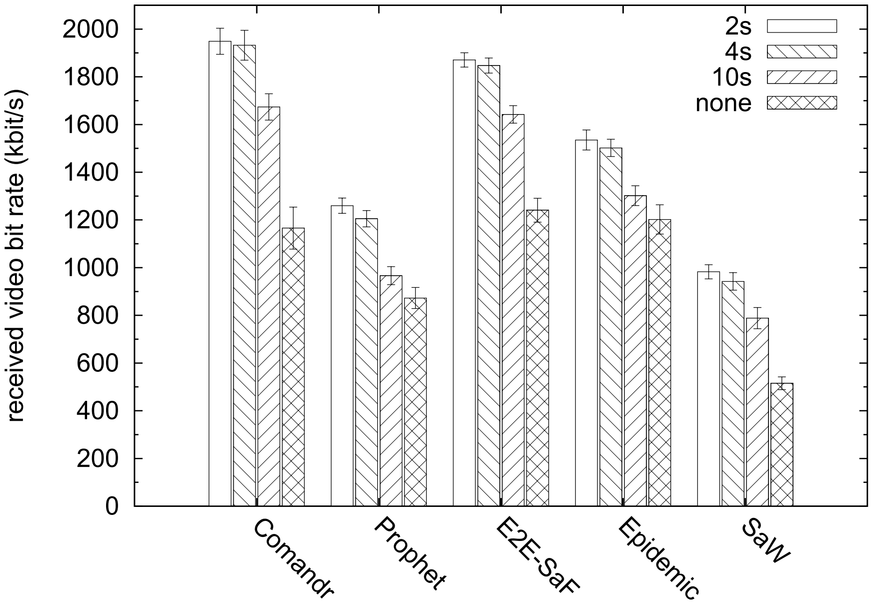


Figure 6.10: Received video bit rate for different segment sizes (multimedia forwarding strategy, transmission bandwidth 2 Mbit/s, transmission range 40 m)

delivery system. The overall delay for receiving a video is calculated by taking the maximum of the delivery delays of all segments of a video, since we assume that the video can only be consumed when all segments have arrived. The delay of a segment is calculated by measuring the time between segment creation and segment reception. Figure 6.11 shows the mean video delay for a transmission range of 60 m using the multimedia forwarding strategy, where most evaluated protocols could deliver all videos (cf. Figure 6.8). Since all videos are made available in two representations, the delivered quality of a video may change over time, while segments providing a higher quality are received. Thus, two delay values are calculated. First, the delay for receiving the videos in a basic quality. That means if both representations for a segment are received, the delay is calculated based on which representation has been received first. Second, the delay for receiving the best representation. The hybrid protocols E2E-SaF and CoMANDR achieve the lowest delay. On average, all segments of a video are received in less than two minutes and it takes about five minutes until the quality of the video is not increased anymore. For PROPHET and Epidemic Routing the difference between receiving videos in a basic quality and receiving them in the best quality is relatively large. These differences are a result of the large transmission overheads, since both protocols flood the network. Thus, it takes more time until the higher quality representations can be delivered. Contrary to the other protocols, Spray and Wait cannot deliver all videos. Thus, we also calculated the delay including missing segments (i.e., segments that could not be delivered in any representation) by setting the received time to the end of the simulation. This represents the case where the missing segments are delivered after the response is over and all nodes return to the entrance of the facility, where they can send the videos to the TOC. In this case the average delay for delivering all videos is about 1235 s and the average delay to deliver the best quality is about 1377 s.

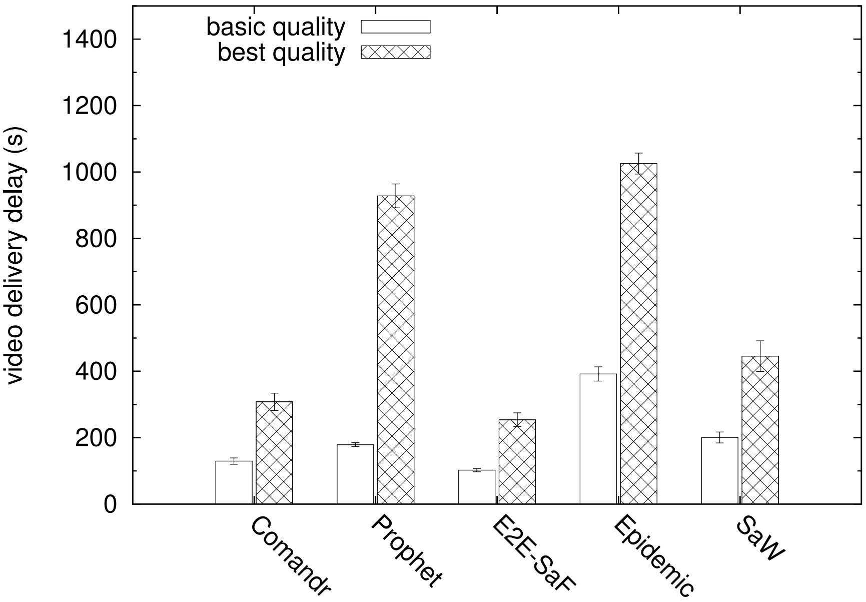


Figure 6.11: Video delivery delay for receiving the videos in a basic quality and for receiving the videos in the best available quality (multimedia forwarding strategy, segment length 2 s, transmission bandwidth 2 Mbit/s, transmission range 60 m)

6.5 Prototype Implementation

In this section we describe a prototype implementation of the DT-MDS system for the Android platform. The system consists of a library that provides HTTP-DTN communication, a mobile DASH encoder for creating multimedia content and a video player for playback.

6.5.1 HTTP-DTN Library

The HTTP-DTN library is the core of the system and provides all functionality that applications need in order to use HTTP-DTN as transport protocol. The main component is an Android Service that is responsible for the communication between the sub-modules of the library and also between the library and applications that use it. For instance, the HTTP-DTN library is included into the mobile MPEG-DASH encoder that acts as producer of video content and the ExoPlayer [47] that is used as consumer in the prototype system. In the following, the modules of the library are described in more detail.

Transport Module

Each node provides an HTTP server that is based on NanoHttp [51]. We extended this HTTP server to handle the additional *Content-** headers in order to process HTTP-DTN requests. The server also supports plain HTTP requests. In the current implementation, the HTTP server only supports GET and PUT requests which are needed in order to transfer files via HTTP(-DTN).

When an HTTP request is received, the node first checks if the request contains a *Content-Destination* header, to determine whether it is a plain HTTP or an HTTP-DTN request. If the header is available, the request is forwarded to an HTTP-DTN handler. If the value of the *Content-Destination* field targets the node itself, it is checked whether a local file is available that matches the URI that is given in the request. If the file exists, it is sent to the requesting node, otherwise the node creates a response with result code 404, indicating that an unknown file has been requested. On the other hand, if the request targets another node, the request is cached and the requesting node is informed that the file is currently not available (i.e., an HTTP response with result code 404 is sent).

There are also two special forms of GET requests in HTTP-DTN. First, the HTTP-DTN specification [129] states that if a GET request has an empty *Host* header, the request has a special semantic. In that case the node receiving the GET request will send a list of files that could be served by this node to the requesting node. Hence, this request can be used to get an overview about the currently cached files. It is important to note that only the metadata of the files will be sent and not the content itself.

Additionally, we also implemented another GET request with special semantics in order to receive information about delivered files. In particular, if the URL of the GET requests has the form `http://<node-id>/delivered` the node that receives the request will send a list of files that are known to be delivered. This allows nodes to exchange information about delivered files which may be deleted in order to free buffers.

If the node receives an HTTP-DTN PUT request, the payload of the file is stored in the local storage and related metadata (e.g., the values of *Content-Source*, *Content-Destination*) is stored in a metadata database. We use SQLite as database system since it is already included in the Android OS.

Neighbor Discovery Module

This module is responsible for detecting other HTTP-DTN nodes in the network and exchanging information about available transport options. The module regularly broadcasts discovery beacons via UDP broadcasts. Each beacon includes the addresses of the available interfaces as well as the static node identifier. The exact format of the discovery beacons is shown in Figure 6.12. Each packet starts with a four bytes header containing the total length of the packet and a sequence number. The sequence number is used to identify the most current beacon and is incremented whenever a node generates a new beacon. The static node identifier (i.e. the *node identifier* field) is an ASCII string whose length is given in the *identifier length* field. Additionally, each beacon contains information about the available sockets. A socket entry consists of the *socket length* field that contains the total length of the entry, the *type* field that determines the type of the socket and the socket data itself. The format and semantic of the socket data is determined by its type. For instance in the case of a TCP/IPv4 socket, the entry will have a length of six bytes, where the first four bytes contain the IP address and the last two bytes contain the port number. In the case of a TCP/IPv6 socket, the entry will contain 16 bytes for the IP address and two bytes for the port number.

Whenever a node joins a local network, its socket information has to be updated since the network address and potentially also the transport protocols may change. However, since the static node identifier will remain the same, it is still possible to route data to this node. The beacons are also used as a heartbeat mechanism to signal the presence of nodes in the network. In particular, since nodes transmit beacons regularly, other nodes can detect when nodes join the local network and also remove them from their neighbor list when several consecutive beacons are missed.

HttpDtnService

The core of the HTTP-DTN library is an Android Service (*HttpDtnService*) that runs in the background and manages the communication between the different modules of the library and also the communication with applications that send or receive files via HTTP-DTN. Applications can register themselves at the service in order to get informed when files are received or when other HTTP-DTN nodes are discovered. Applications also use the service to send files to other nodes. Communication is performed via asynchronous message passing.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Packet length         |        Sequence number        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Identifier len.|             Node identifer                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
/                     identifier (cont.)                        /
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|  Socket len.  |      Type     |      Socket information       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
/                    Socket information (cont.)                 /
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Socket len.  |      Type     |      Socket information       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
/                    Socket information (cont.)                 /
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                                               /
```

Figure 6.12: Neighbor discovery beacon format.

The service also listens to changes of the Wi-Fi interface in order to control (e.g., start or stop) the discovery module.

6.5.2 Mobile MPEG-DASH Encoder

For recording videos we use a mobile MPEG-DASH encoder for Android [66, 101]. The mobile MPEG-DASH encoder records multimedia content via Android's standard APIs for media recording. The multimedia content is then segmented and multiplexed into ISO Base Media File Format container files, which are stored in the local storage. Additionally, the mobile MPEG-DASH encoder creates an MPD file that describes the structure of the content and how to retrieve it. Originally, the mobile MPEG-DASH encoder used peer-to-peer streaming for video delivery. We exchanged this module with the HTTP-DTN library, in order to serve the recorded multimedia files via HTTP and HTTP-DTN.

6.5.3 Multimedia Playback

For the playback of multimedia content the ExoPlayer [47] for Android is used. ExoPlayer is an open source media player by Google that supports different codecs and transport mechanisms to play back local and remote multimedia content. ExoPlayer has been chosen since it already provides support for MPEG-DASH and is also extensible. In particular, we added the HTTP-DTN library to the ExoPlayer in order to retrieve multimedia data via HTTP-DTN.

6.6 Conclusion

In this chapter we presented a multimedia delivery system called DT-MDS for delay-/disruption-tolerant networks which is based on HTTP adaptive streaming. This design choice has been made since HAS offers several characteristics that are beneficial in DTNs. In particular, as discussed in Section 6.2.3, the segmentation of videos into self-contained pieces and the simple control flows make HAS very suitable to deliver multimedia data in DTNs. DT-MDS uses a modified version of HTTP (i.e., HTTP-DTN) where nodes offer HTTP client and HTTP server functionality for delivering the multimedia content in disrupted networks. HTTP-DTN is well-suited for this purpose since it is based on HTTP which makes integration with HAS systems straightforward. This practicability has been shown by presenting a prototype implementation for Android systems. Furthermore, evaluation results show that our system works well in a realistic emergency response scenario, especially in combination with hybrid MANET/DTN routing strategies.

CHAPTER 7 Conclusion

In this thesis, we showed how to improve wireless networking in emergency response scenarios. Many existing works in the domain of wireless networking and especially wireless mobile ad-hoc networks (MANETs) see this application domain as very promising but most of them do not take the specifics of this domain into account. In contrast, in this thesis we particularly focused on realistic emergency response scenarios. In the following, we recapitulate the major contributions of this thesis.

Modeling and analysis of wireless networking in realistic emergency scenarios: We presented a modeling framework and two realistic emergency response scenarios in Chapter 3 and also evaluated the specifics of these scenarios in terms of connectivity. The first scenario describes an emergency response operation after an incident in a chemical facility. The scenario is based on a mobility model for first responders and takes also into account that first responders may have to temporarily work indoors. The second scenario models a real-world, full-scale exercise that took place in Risavika, Norway. We could use the modeling framework to model the important aspects of the exercise scenario, which shows that the selected models and tools are applicable to real-world scenarios. Evaluation results for the connectivity characteristics of both scenarios showed that both scenarios are diverse in terms of connectivity. In particular, some parts of the network are well connected, whereas other parts of the networks are very sparse and thus the network is often partitioned. We showed that this is a challenge for existing MANET routing protocols by performing several simulation-based evaluations.

Combining MANET/DTN routing to improve routing in emergency response scenarios: To tackle the aforementioned challenges that wireless networks for emergency response scenarios face, we proposed to use a combination of traditional end-to-end routing for MANETs and routing for delay-/disruption-tolerant networking (DTN). In Chapter 4 we gave an overview and classification of such approaches. Furthermore, we also proposed two combined routing schemes that apply DTN routing mechanisms on top of MANET routing.

The novelty of these approaches is that information available from the MANET routing protocol is used in the DTN mechanisms. Both approaches prefer end-to-end routing when available and use DTN mechanisms as a fall-back. Thus, the approaches are robust to disruptions of the network infrastructure. However, there are also some differences between the approaches. The first one applies packet buffering on top of MANET routing in order to bridge temporal disruptions and short-time link failures. The second approach additionally uses utility-based forwarding which makes it possible to bridge permanent partitions by selecting custodian nodes.

Evaluation of combined MANET/DTN routing in emergency response scenarios: In Chapter 5, we evaluated the aforementioned combined routing schemes in a series of simulations in the context of the emergency response scenarios. To the best of our knowledge, there are no other works that performed such evaluations in emergency response scenarios. Apart from this contribution, we also compared the combined approaches with existing state-of-the-art routing protocols from the MANET and the DTN domains. The evaluation results show that combining MANET and DTN routing achieves delivery ratios comparable to flooding-based DTN routing schemes, while needing less resources. Furthermore, results show that the approaches perform well over a broad range of networks from sparse to well-connected. We believe that this is an important feature, since the connectivity will greatly vary between different emergency response scenarios. Hence, it is important that the deployed routing protocol covers a broad range of networks.

Multimedia delivery in disrupted networks: In the last part of this thesis we proposed a multimedia delivery system for disrupted-networks, called DT-MDS (see Chapter 6). Based on a discussion about existing real-world studies about the usage of multimedia in emergency response scenarios, we derived some requirements for DT-MDS. In the context of this work, one of the important findings of these studies is that multimedia is used as a form of asynchronous communication in emergency response operations. In other words, multimedia for emergency response scenarios is delay-tolerant which makes DT-MDS applicable. We then analyzed two techniques for video delivery, namely Real Time Streaming (RTP) and HTTP Adaptive Streaming (HAS) and concluded that the latter is better suited for disrupted networks. Additionally, we adopted existing ideas for modifying HTTP in order to be used as a delay-/disruption-tolerant delivery protocol for DT-MDS. We evaluated the multimedia delivery system in the chemical incident scenario and also described a prototype implementation for Android systems to show the applicability of our ideas. Based on the evaluation results and our experiences with the Android prototype, we believe that such a system could provide an additional means for communication in emergency response scenarios which may help to increase the situational awareness.

There are several directions for future work. As described in Section 5.6, one topic for future work is to compare the proposed algorithms with other state-of-the-art hybrid MANET/DTN protocols. Additionally, we considered a specific type of emergency response scenarios in this thesis, where first responders move on an incident area with restricted size and all communication takes place on the incident site. However, there are scenarios where the incident area includes entire metropolitan areas and hence local area networks do not suffice. An interesting topic for future work would be to model such large-scale scenarios, which requires using other mobility and wireless models as well as considering other communication patterns. It would then be interesting to evaluate how the proposed algorithms would scale up and what aspects would need to be changed in order to adapt the algorithms to this type of emergency response scenarios.

Concerning the evaluation of the multimedia delivery system, we assumed that recorded videos have a short duration (e.g., up to a minute) and that they are consumed after all segments have been received. However, there may be emergency response scenarios where longer video sequences are recorded and hence may also need to be streamed while they are recorded. For instance, in a forest fire scenario, first responders may deploy cameras to monitor certain locations. In such cases, more intelligent adaptation techniques are needed that provide a trade off between the quality of the content and the delivery delay. In recent years, a lot of multimedia adaptation algorithms for HTTP-based delivery have been proposed. However, the main challenge when developing such adaptation algorithms in the context of disrupted networks is the presence of potentially large delays. This makes it very hard to control the multimedia session since there is no closed control loop available. Instead, adaptation algorithms would need to take imperfect information and uncertainties into account. Another topic for future work is the design of advanced user interfaces and playback options. For instance, consumers need to get information about which parts of the stream have already been received and which parts are still missing. Additionally, the user needs to be able to control how to consume the content (e.g., wait for a segment to arrive, or skip it and proceed with subsequent segments). Thus, adapting the system to support this type of usage is another interesting topic for future research.

Bibliography

[1] M. Abolhasan, T. A. Wysocki, and E. Dutkiewicz. A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks*, 2(1):1–22, 2004.

[2] *HTTP Dynamic Streaming Specification (Version 3.0 final)*. Adobe Systems Incorporated, 2013. `http://wwwimages.adobe.com/content/dam/Adobe/en/devnet/hds/pdfs/adobe-hds-specification.pdf`, accessed: Mar 2015.

[3] A. Al-Akkad and C. Raffelsberger. How do I get this app? A discourse on distributing mobile applications despite disrupted infrastructure. In *Proceedings of the 11th International Conference on Information Systems for Crisis Response and Management (ISCRAM '14)*, pages 560–564. The Pennsylvania State University, USA, 2014.

[4] A. Al-Akkad, C. Raffelsberger, A. Boden, L. Ramirez, and A. 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 '14)*, pages 657–666. The Pennsylvania State University, USA, 2014.

[5] A. Al-Akkad, L. Ramirez, A. Boden, D. W. Randall, and A. 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 (CHI '14)*, pages 1485–1494. ACM, 2014.

[6] E. Alotaibi and B. Mukherjee. A survey on routing algorithms for wireless ad-hoc and mesh networks. *Computer Networks*, 56(2):940–965, Feb. 2012.

[7] A. Ariza-Quintana. INETMANET 2.0 code repository. `https://github.com/aarizaq/inetmanet-2.0`, accessed: Mar 2015.

[8] A. Ariza-Quintana, E. Casilari, and A. Cabrera Triviño. Implementation of MANET routing protocols on OMNeT++. In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops (Simutools '08)*. ICST, 2008.

[9] D. Arora, E. Millman, and S. W. Neville. Assessing the performance of AODV, DYMO, and OLSR routing protocols in the context of larger-scale denser MANETs. In *Proceedings of the 2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PacRim '11)*, pages 675 –679. IEEE, 2011.

[10] N. Aschenbruck, E. Gerhards-Padilla, M. Gerharz, M. Frank, and P. Martini. Modelling mobility in disaster area scenarios. In *Proceedings of the 10th ACM Symposium on Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWiM '07)*, pages 4–12. ACM, 2007.

[11] N. Aschenbruck, C. de Waal, and P. Martini. Distribution of nodes in disaster area scenarios and its impact on topology control strategies. In *Proceedings of the 2008 IEEE International Conference on Computer Communications Workshops (INFOCOM Workshops '08)*, pages 1–6, 2008.

[12] N. Aschenbruck, E. Gerhards-Padilla, and P. Martini. Modeling mobility in disaster area scenarios. *Performance Evaluation*, 66(12):773–790, 2009.

[13] N. Aschenbruck, R. Ernst, E. Gerhards-Padilla, and M. Schwamborn. Bonnmotion: A mobility scenario generation and analysis tool. In *Proceedings of the 3rd International ICST Conference on Simulation Tools and Techniques (SIMUTools '10)*, pages 51:1–51:10. ICST, 2010.

[14] A. Asp, Y. Sydorov, M. Valkama, and J. Niemela. Radio signal propagation and attenuation measurements for modern residential buildings. In *Proceedings of the IEEE Globecom Workshops (GC Wkshps '12)*, pages 580–584. IEEE, 2012.

[15] M. Asplund, S. Nadjm-Tehrani, and J. Sigholm. Emerging information infrastructures: Cooperation in disasters. In *Critical Information Infrastructure Security*, volume 5508 of *Lecture Notes in Computer Science*, pages 258–270. Springer, 2009.

[16] C. Aung, P. Chong, and R. J. Cai. Hybrid opportunistic routing in highly dynamic MANET. In *Proceedings of the 23rd International Conference on Computer Communication and Networks (ICCCN)*, pages 1–6. IEEE, 2014.

[17] F. Bergstrand and J. Landgren. Information sharing using live video in emergency response work. In *Proceedings of the 6th International Conference on Information Systems for Crisis Response and Management (ISCRAM '09)*, pages 1–5, 2009.

[18] C. Bettstetter. Mobility modeling in wireless networks: Categorization, smooth movement, and border effects. *SIGMOBILE Mob. Comput. Commun. Rev.*, 5(3):55–66, July 2001.

[19] C. Bettstetter. On the minimum node degree and connectivity of a wireless multihop network. In *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc '02)*, pages 80–91. ACM, 2002.

[20] C. Bettstetter and C. Wagner. The spatial node distribution of the random waypoint mobility model. In *1. Deutscher Workshop über Mobile Ad-Hoc Netzwerke (WMAN '02)*, pages 41–58. GI, 2002.

[21] C. Bettstetter, G. Resta, and P. Santi. The node distribution of the random waypoint mobility model for wireless ad hoc networks. *IEEE Transactions on Mobile Computing*, 2(3):257–269, July 2003.

[22] C. Bettstetter, H. Hartenstein, and X. Prez-Costa. Stochastic properties of the random waypoint mobility model. *Wireless Networks*, 10(5):555–567, 2004.

[23] M. Betz and V. Wulf. Emergencymessenger: A text based communication concept for indoor firefighting. In *Proceedings of the 32nd ACM Conference on Human Factors in Computing Systems (CHI '14)*, pages 1515–1524. ACM, 2014.

[24] S. Biswas and R. Morris. ExOR: Opportunistic multi-hop routing for wireless networks. *SIGCOMM Comput. Commun. Rev.*, 35(4):133–144, Aug. 2005.

[25] A. Boukerche. Performance evaluation of routing protocols for ad hoc wireless networks. *Mobile Networks and Applications*, 9(4):333–342, Aug. 2004.

[26] A. Boukerche, B. Turgut, N. Aydin, M. Ahmad, L. Bölöni, and D. Turgut. Routing protocols in ad hoc networks: A survey. *Computer Networks*, 55(13):3032–3080, Sept. 2011.

[27] BRIDGE project homepage. `http://www.bridgeproject.eu`, accessed: Mar 2015.

[28] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '98)*, pages 85–97, New York, NY, USA, 1998. ACM.

[29] J. Burgess, B. Gallagher, D. Jensen, and B. Levine. Maxprop: Routing for vehicle-based disruption-tolerant networks. In *Proceedings of the 25th IEEE International Conference on Computer Communications (INFOCOM '06)*, pages 1–11. IEEE, April 2006.

[30] S. Cabrero, X. Paneda, R. Garcia, D. Melendi, and T. Plagemann. Dynamic temporal scalability: Video adaptation in sparse mobile ad-hoc networks. In *Proceedings of the 8th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '12)*, pages 349–356. IEEE, 2012.

[31] T. Camp, J. Boleng, and V. Davies. A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing*, 2(5):483–502, 2002.

[32] Y. Cao and Z. Sun. Routing in delay/disruption tolerant networks: A taxonomy, survey and challenges. *IEEE Communications Surveys & Tutorials*, 15(2):654–677, Feb. 2013.

[33] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss. Delay-tolerant networking architecture. IETF RFC 4838, 2007.

[34] I. Chakeres and C. Perkins. Dynamic MANET on-demand routing protocol. Internet Draft draft-ietf-manet-dymo-10, 2007.

[35] O. Chipara, W. G. Griswold, A. N. Plymoth, R. Huang, F. Liu, P. Johansson, R. Rao, T. Chan, and C. Buono. WIISARD: A measurement study of network properties and protocol reliability during an emergency response. In *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services (MobiSys '12)*, pages 407–420. ACM, 2012.

[36] T. Clausen and P. Jacquet. Optimized link state routing protocol (OLSR). IETF RFC 3626, 2003.

[37] S. Dabideen and R. Ramanathan. FansyRoute: Adaptive fan-out for variably intermittent challenged networks. *SIGMOBILE Mobile Computing and Communications Review*, 18(1):37–45, Feb. 2014.

[38] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris. A high-throughput path metric for multi-hop wireless routing. In *Proceedings of the 9th Annual International*

Conference on Mobile Computing and Networking (MobiCom '03), pages 134–146. ACM, 2003.

[39] L. Delosieres and S. Nadjm-Tehrani. Batman store-and-forward: The best of the two worlds. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops '12)*, pages 721–727. IEEE, 2012.

[40] M. Demmer and K. Fall. DTLSR: delay tolerant routing for developing regions. In *Proceedings of the 2007 Workshop on Networked Systems for Developing Regions (NSDR '07)*, pages 1–6. ACM, 2007.

[41] P. J. Denning. Hastily formed networks. *Communications of the ACM*, 49(4):15–20, Apr. 2006.

[42] A. W. Eide, I. M. Haugstveit, R. Halvorsrud, and M. Borén. Inter-organizational collaboration structures during emergency response: A case study. In *Proceedings of International Conference on Information Systems for Crisis Management and Response (ISCRAM '13)*, pages 94 – 104, 2013.

[43] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee. Hypertext transfer protocol - HTTP/1.1. IETF RFC 2616, 1999.

[44] H. Friis. A note on a simple transmission formula. *Proceedings of the IRE*, 34(5): 254–256, May 1946.

[45] P. Fuhr and N. Hedroug. Wireless: Tracking wireless. *InTech Magazine*, Apr. 2008.

[46] V. K. Garg. *Wireless Communications and Networking.* Morgan Kaufmann, 2007. ISBN 9780123735805.

[47] Google Inc. ExoPlayer code repository. `https://github.com/google/ExoPlayer`, accessed: Mar 2015.

[48] M. Grafl, C. Timmerer, H. Hellwagner, W. Cherif, and A. Ksentini. Evaluation of hybrid scalable video coding for HTTP-based adaptive media streaming with high-definition content. In *Proceedings of the 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM Workshops '13)*, pages 1–7. IEEE, 2013.

[49] S. Grasic, E. Davies, A. Lindgren, and A. Doria. The evolution of a DTN routing protocol - PRoPHETv2. In *Proceedings of the 6th ACM Workshop on Challenged Networks (CHANTS '11)*, pages 27–30. ACM, 2011.

[50] Z. Haas. A new routing protocol for the reconfigurable wireless networks. In *Proceedings of the 6th International Conference on Universal Personal Communications (ICUPC '97)*, volume 2, pages 562–566 vol.2. IEEE, Oct 1997.

[51] P. Hawke. NanoHttpd code repository. `https://github.com/NanoHttpd/nanohttpd`, accessed: Mar 2015.

[52] A. L. Hughes, L. A. A. St. Denis, L. Palen, and K. M. Anderson. Online public communications by police & fire services during the 2012 hurricane Sandy. In *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems (CHI '14)*, pages 1505–1514. ACM, 2014.

[53] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (IEEE Std 802.11-2012)*. Institute of Electrical and Electronics Engineers, Inc., Feb. 2012.

[54] *IEEE Standard for Definitions of Terms for Antennas (IEEE Std 145-2013)*. Institute of Electrical and Electronics Engineers, Inc., Dec. 2013.

[55] ISO/IEC 23009-1:2014. *Information technology – Dynamic adaptive streaming over HTTP (DASH) – Part 1: Media presentation description and segment formats*, 2014.

[56] S. Jain, S. Gopinath, and D. Raychaudhuri. STAR: Storage aware routing protocol for generalized delay tolerant networks. In *Proceedings of the 12th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '11)*, pages 1 –4, 2011.

[57] M. Jentsch, L. Ramirez, L. Wood, and E. Elmasllari. The reconfiguration of triage by introduction of technology. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services (MobileHCI '13)*, pages 55–64. ACM, 2013.

[58] X. Jiang, N. Y. Chen, J. I. Hong, K. Wang, L. Takayama, and J. A. Landay. Siren: Context-aware computing for firefighting. In *Pervasive Computing*, volume 3001 of *Lecture Notes in Computer Science*, pages 87–105. Springer, 2004.

[59] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark. Scenario-based performance analysis of routing protocols for mobile ad-hoc networks. In *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom '99)*, pages 195–206. ACM, 1999.

[60] D. Johnson and G. Hancke. Comparison of two routing metrics in OLSR on a grid based mesh network. *Ad Hoc Networks*, 7(2):374–387, Mar. 2009.

[61] D. Johnson, N. Ntlatlapa, and C. Aichele. A simple pragmatic approach to mesh routing using BATMAN. In *Proceedings of the 2nd IFIP International Symposium on Wireless Communications and Information Technology in Developing Countries (WCITD '08)*, pages 1–10. IFIP, 2008.

[62] D. B. Johnson, D. A. Maltz, and J. Broch. DSR: The dynamic source routing protocol for multihop wireless ad hoc networks. In C. E. Perkins, editor, *Ad Hoc Networking*, pages 139–172. Addison-Wesley, Boston, MA, USA, 2001.

[63] A. Keränen, J. Ott, and T. Kärkkäinen. The ONE simulator for DTN protocol evaluation. In *Proceedings of the 2nd ICST International Conference on Simulation Tools and Techniques (SIMUTools '09)*, pages 55:1–55:10. ICST, 2009.

[64] M. Klaghstan, D. Coquil, N. Bennani, H. Kosch, and L. Brunie. Enhancing video viewing-experience in opportunistic networks based on SVC, an experimental study. In *Proceedings of the 24th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '13)*, pages 3563–3567. IEEE, 2013.

[65] M. Klaghstan, N. Bennani, D. Coquil, H. Kosch, and L. Brunie. Contact-based adaptive granularity for scalable video transmission in opportunistic networks. In *Proceedings of the 10th International Wireless Communications and Mobile Computing Conference (IWCMC '14)*, pages 773–778. IEEE, 2014.

[66] M. Klusch, P. Kapahnke, X. Cao, B. Rainer, C. Timmerer, and S. Mangold. MyMedia: Mobile semantic peer-to-peer video search and live streaming. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MOBIQUITOUS '14)*, pages 277–286. ICST, 2014.

[67] C. Kretschmer, S. Ruhrup, and C. Schindelhauer. DT-DYMO: Delay-tolerant dynamic MANET on-demand routing. In *Proceedings of the 29th IEEE International*

Conference on Distributed Computing Systems Workshops (ICDCSW '09), pages 493–498. IEEE, 2009.

[68] J. Lakkakorpi, M. Pitkänen, and J. Ott. Adaptive routing in mobile opportunistic networks. In *Proceedings of the 13th ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWIM '10)*, pages 101–109. ACM, 2010.

[69] J. Landgren and F. Bergstrand. Mobile live video in emergency response: Its use and consequences. *Bulletin of the American Society for Information Science and Technology*, 36(5):27–29, 2010.

[70] M. Latonero and I. Shklovski. Emergency management, twitter, and social media evangelism. *IJISCRAM*, 3(4):1–16, 2011.

[71] S.-A. Lenas, S. Burleigh, and V. Tsaoussidis. Reliable data streaming over delay tolerant networks. In *Proceedings of the International Conference on Wired/Wireless Internet Communications (WWIC '12)*, pages 358–365. Springer, 2012.

[72] M. Lindeberg, S. Kristiansen, T. Plagemann, and V. Goebel. Challenges and techniques for video streaming over mobile ad hoc networks. *Multimedia Systems*, 17(1): 51–82, 2011.

[73] A. Lindgren, A. Doria, and O. Schelén. Probabilistic routing in intermittently connected networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 7:19–20, July 2003.

[74] F. B. Luqman and M. L. Griss. Overseer: A mobile context-aware collaboration and task management system for disaster response. In *Proceedings of the 8th International Conference on Creating, Connecting and Collaborating through Computing (C5 '10)*, pages 76–82. IEEE, 2010.

[75] V. Manfredi, M. Crovella, and J. Kurose. Understanding stateful vs stateless communication strategies for ad hoc networks. In *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking (MobiCom '11)*, pages 313–324. ACM, 2011.

[76] A. Martín-Campillo, J. Crowcroft, E. Yoneki, and R. Martí. Evaluating opportunistic networks in disaster scenarios. *J. Netw. Comput. Appl.*, 36(2):870–880, Mar. 2013.

[77] M. Mauve, J. Widmer, and H. Hartenstein. A survey on position-based routing in mobile ad hoc networks. *IEEE Network*, 15(6):30–39, Nov 2001.

[78] K. Mayer and W. Fritsche. IP-enabled wireless sensor networks and their integration into the Internet. In *Proceedings of the 1st International Conference on Integrated Internet Ad Hoc and Sensor Networks (InterSense '06)*, pages 1 – 9. ACM, 2006.

[79] C. Mbarushimana and A. Shahrabi. Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks. In *Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW '07)*, pages 679 –684. IEEE, 2007.

[80] A. Monares, S. F. Ochoa, J. A. Pino, V. Herskovic, J. Rodriguez-Covili, and A. Neyem. Mobile computing in urban emergency situations: Improving the support to firefighters in the field. *Expert Systems with Applications*, 38(2):1255–1267, Feb. 2011.

[81] D. Murray, M. Dixon, and T. Koziniec. An experimental comparison of routing protocols in multi hop ad hoc networks. In *Proceedings of the 2010 Telecommunication Networks and Applications Conference (ATNAC '10)*, pages 159–164. IEEE, 2010.

[82] M. Musolesi, S. Hailes, and C. Mascolo. Adaptive routing for intermittently connected mobile ad hoc networks. In *Proceedings of the 6th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '05)*, pages 183–189. IEEE, 2005.

[83] S. C. Nelson, A. F. Harris, III, and R. Kravets. Event-driven, role-based mobility in disaster recovery networks. In *Proceedings of the 2nd ACM Workshop on Challenged Networks (CHANTS '07)*, pages 27–34. ACM, 2007.

[84] A. Neumann, C. Aichele, M. Lindner, and S. Wunderlich. Better approach to mobile ad-hoc networking (B.A.T.M.A.N). Internet Draft draft-openmesh-b-a-t-m-a-n-00, 2008.

[85] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu. The broadcast storm problem in a mobile ad hoc network. In *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '99)*, pages 151–162. ACM, 1999.

[86] olsrd: An adhoc wireless mesh routing daemon. `htxtp://www.olsr.org`, accessed: Mar 2015.

[87] OMNet++. `http://www.omnetpp.org`, accessed: Mar 2015.

[88] J. Ott, D. Kutscher, and C. Dwertmann. Integrating DTN and MANET routing. In *Proceedings of the ACM Workshop on Challenged Networks (CHANTS '06)*, pages 221–228. ACM, 2006.

[89] L. Palen, S. Vieweg, S. B. Liu, and A. L. Hughes. Crisis in a networked world: Features of computer-mediated communication in the April 16, 2007, Virginia Tech Event. *Social Science Computer Review*, 27(4):467–480, 2009.

[90] R. Pant, A. Tunpan, P. Mekbungwan, R. Virochpoka, and K. Kanchanasut. DTN overlay on OLSR network. In *Proceedings of the 6th Asian Internet Engineering Conference (AINTEC '10)*, pages 56–63. ACM, 2010.

[91] R. Pantos. HTTP live streaming. Internet Draft draft-pantos-http-live-streaming-14, 2014.

[92] R. Pathak, P. Hu, J. Indulska, M. Portmann, and W. L. Tan. Towards efficient opportunistic communications: A hybrid approach. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops '13)*, pages 255–260. IEEE, 2013.

[93] C. E. Perkins. Ad hoc networking: An introduction. In *Ad Hoc Networking*, pages 1–28. Addison-Wesley, Boston, MA, USA, 2001. ISBN 0-201-30976-9.

[94] C. E. Perkins and E. M. Royer. The ad hoc on-demand distance-vector protocol. In *Ad Hoc Networking*, pages 173–219. Addison-Wesley, Boston, MA, USA, 2001. ISBN 0-201-30976-9.

[95] S.-Y. Perng, M. Bscher, L. Delano-Wood, R. Halvorsrud, M. Stiso, L. Ramirez, and A. Al-Akkad. Peripheral response: Microblogging during the 22/7/2011 norway attacks. *IJISCRAM*, 5(1):41–57, 2013.

[96] C. Raffelsberger and H. Hellwagner. Evaluation of manet routing protocols in a realistic emergency response scenario. In *Proceedings of the 10th International Workshop*

on Intelligent Solutions in Embedded Systems (WISES '12), pages 88 – 92. IEEE, 2012.

[97] C. Raffelsberger and H. Hellwagner. A hybrid MANET-DTN routing scheme for emergency response scenarios. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops '13)*, pages 505 – 510. IEEE, 2013.

[98] C. Raffelsberger and H. Hellwagner. Overview of hybrid MANET-DTN networking and its potential for emergency response operations. In *Proceedings of the Combined workshop on Self-organizing, Adaptive, and Context-Sensitive Distributed Systems and Self-organized Communication in Disaster Scenarios (SACS/SoCoDiS '13)*, pages 1 – 12, Berlin, Germany, mar 2013. Electronic Communications of the EASST (ECE-ASST).

[99] C. Raffelsberger and H. Hellwagner. Combined mobile ad-hoc and delay/disruption-tolerant routing. In *Proceedings of the 13th International Conference on Ad-hoc, Mobile, and Wireless Networks (ADHOC-NOW '14)*, volume 8487 of *Lecture Notes in Computer Science*, pages 1–14. Springer, 2014.

[100] C. Raffelsberger and H. Hellwagner. A multimedia delivery system for delay-/disruption-tolerant networks. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops '15)*, pages 534 – 540. IEEE, 2015.

[101] B. Rainer, C. Timmerer, P. Kapahnke, and M. Klusch. Real-time multimedia streaming in unstructured peer-to-peer networks. In *Proceedings of the 10th IEEE Consumer Communication and Networking Conference (CCNC '14)*, pages 1136–1137. IEEE, 2014.

[102] L. Ramirez, T. Dyrks, J. Gerwinski, M. Betz, M. Scholz, and V. Wulf. Landmarke: An ad hoc deployable ubicomp infrastructure to support indoor navigation of firefighters. *Personal Ubiquitous Computing*, 16(8):1025–1038, Dec. 2012.

[103] D. Reina, S. Toral, F. Barrero, N. Bessis, and E. Asimakopoulou. Evaluation of ad hoc networks in disaster scenarios. In *Proceedings of the 3rd International Conference on Intelligent Networking and Collaborative Systems (INCoS '11)*, pages 759–764. IEEE, 2011.

[104] D. Reina, S. Toral, F. Barrero, N. Bessis, and E. Asimakopoulou. Modelling and assessing ad hoc networks in disaster scenarios. *Journal of Ambient Intelligence and Humanized Computing*, 4(5):571–579, 2013.

[105] I. Rodriguez, H. Nguyen, N. Jorgensen, T. Sorensen, and P. Mogensen. Radio propagation into modern buildings: Attenuation measurements in the range from 800 mhz to 18 ghz. In *Proceedings of the 80th Vehicular Technology Conference (VTC Fall '14),*, pages 1–5, Sept 2014.

[106] E. Royer and C.-K. Toh. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications*, 6(2):46–55, Apr 1999.

[107] M. Sakurai, R. Watson, C. Abraham, and J. Kokuryo. Sustaining life during the early stages of disaster relief with a frugal information system: Learning from the great east Japan earthquake. *IEEE Communications Magazine*, 52(1):176–185, January 2014.

[108] H. Schulzrinne, A. Rao, and L. R. Real time streaming protocol (RTSP). IETF RFC 2326, 1998.

[109] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: A transport protocol for real-time applications. IETF RFC 3550, 2003.

[110] K. Scott and S. Burleigh. Bundle protocol specification. IETF RFC 5050, 2007.

[111] I. Sodagar. The MPEG-DASH Standard for Multimedia Streaming Over the Internet. *IEEE MultiMedia*, 18(4):62–67, 2011.

[112] C. Sommer, D. Eckhoff, R. German, and F. Dressler. A computationally inexpensive empirical model of IEEE 802.11p radio shadowing in urban environments. In *Proceedings of the 8th International Conference on Wireless On-Demand Network Systems and Services (WONS '11)*, pages 84–90. IEEE, 2011.

[113] T. Spyropoulos, K. Psounis, and C. S. Raghavendra. Spray and wait: An efficient routing scheme for intermittently connected mobile networks. In *Proceedings of the ACM Workshop on Delay-tolerant Networking (WDTN '05)*, pages 252–259. ACM, 2005.

[114] T. Spyropoulos, K. Psounis, and C. S. Raghavendra. Efficient routing in intermittently connected mobile networks: the single-copy case. *IEEE/ACM Trans. Netw.*, 16(1): 63–76, Feb. 2008.

[115] T. Spyropoulos, R. N. Rais, T. Turletti, K. Obraczka, and A. Vasilakos. Routing for disruption tolerant networks: Taxonomy and design. *Wireless Networks*, 16(8): 2349–2370, Nov. 2010.

[116] F. Steinhäusler. Deliverable D03.1: Modelling of structure. Public Project Deliverable `http://www.bridgeproject.eu/en/bridge-results/deliverables/d031`, 2012. accessed: Mar 2015.

[117] T. Stockhammer. Dynamic adaptive streaming over HTTP: Standards and design principles. In *Proceedings of the 2nd Annual ACM Conference on Multimedia Systems (MMSys '11)*, pages 133–144. ACM, 2011.

[118] J. Sutton, L. Palen, and I. Shlovski. Back-channels on the front lines: Emerging use of social media in the 2007 southern California wildfires. In *Proceedings of the 5th International Conference on Information Systems for Crisis Response and Management (ISCRAM '08)*, 2008.

[119] M. Tarique, K. E. Tepe, S. Adibi, and S. Erfani. Survey of multipath routing protocols for mobile ad hoc networks. *Journal of Network and Computer Applications*, 32(6): 1125 – 1143, 2009.

[120] X. Tie, A. Venkataramani, and A. Balasubramanian. R3: Robust replication routing in wireless networks with diverse connectivity characteristics. In *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking (MobiCom '11)*, pages 181–192. ACM, 2011.

[121] M. Y. S. Uddin, D. M. Nicol, T. F. Abdelzaher, and R. H. Kravets. A post-disaster mobility model for delay tolerant networking. In *Proceedings of the 2009 Winter Simulation Conference (WSC '09)*, pages 2785–2796. WSC, 2009.

[122] A. Vahdat and D. Becker. Epidemic routing for partially-connected ad hoc networks. Technical Report CS-2000-06, Duke University, July 2000.

[123] A. Varga and R. Hornig. An overview of the OMNeT++ simulation environment. In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops (Simutools '08)*, pages 60:1–60:10. ICST, 2008.

[124] L. Viennot, P. Jacquet, and T. H. Clausen. Analyzing control traffic overhead versus mobility and data traffic activity in mobile ad-hoc network protocols. *Wireless Networks*, 10(4):447–455, July 2004.

[125] Y.-K. Wang, R. Even, T. Kristensen Tandberg, and J. R. RTP payload format for H.264 video. IETF RFC 6184, 2011.

[126] J. Whitbeck and V. Conan. HYMAD: Hybrid DTN-MANET routing for dense and highly dynamic wireless networks. *Computer Communications*, 33(13):1483–1492, Aug. 2010.

[127] M. A. Wister, P. Pancardo, F. D. Acosta, and D. Arias-Torres. Performance evaluation of AODV and DYMO as a plattform for rescue task applications in MANETs. In *Proceedings of the 2011 Workshops of the IEEE International Conference on Advanced Information Networking and Applications (WAINA '11)*, pages 670–675. IEEE, 2011.

[128] A. Wolff and C. Wietfeld. Process-oriented deployment of ad-hoc networks in emergency scenarios. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops '12)*, pages 728–733. IEEE, 2012.

[129] L. Wood and P. Holliday. Using HTTP for delivery in delay/disruption-tolerant networks. Internet Draft draft-wood-dtnrg-http-dtn-delivery-09, June 2014.

[130] L. Wood, P. Holliday, D. Floreani, and I. Psaras. Moving data in DTNs with HTTP and MIME. In *Proceedings of the International Conference on Ultra Modern Telecommunications Workshops (ICUMT '09)*, pages 1–4, 2009.

[131] A. Zambelli. IIS smooth streaming technical overview. White paper, Microsoft Corporation, Mar. 2009. `http://www.microsoft.com/en-us/download/confirmation.aspx?id=17678`, accessed: Mar 2015.

[132] Z. Zhang. Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: Overview and challenges. *IEEE Communications Surveys & Tutorials*, 8(1):24–37, Jan. 2006.

APPENDIX A Definition of Tactical Areas

This appendix gives details about how to reproduce the mobility traces for the chemical incident and Risavika scenarios using the BonnMotion tool [13].

A.1 Chemical Incident Scenario

This section includes the definitions of tactical areas for the chemical incident scenario that has been introduced in Section 3.2.

```
Model: DisasterArea
Duration (-d): 7200
Seconds to skip (-i): 5000
Number of nodes (-n): 25
Area width(-x): 400
Area height (-y): 300
Prevent ambulances in areas other than APP (-K)
Random seeds (-R):
[114701,985702,687203,3957504,9704205,5668106,8296607,6296608,1842509,
4153310,1288311,1264012,9637413,85014,17215,203016,80617,973518,81019,
508420,269921,25522,490823,658424,729725,41626,457427,794028,236129,
582530,542931]

Incident Location:
Shape: ("310,100,350,100,350,200,310,200")
Entry/exit: ("325,200,325,200")
No of nodes: 4
No of transport nodes:  4
```

```
Incident Location:
Shape: ("130,150,260,150,260,180,130,180")
Entry/exit: ("200,180,200,180")
No of nodes: 4
No of transport nodes:  4

Patients Waiting For Treatment Area:
Shape: ("130,180,150,180,150,240,130,240")
Entry/exit: ("150,210,130,210")
No of nodes: 8
No of transport nodes:  4

Casualties Clearing Station:
Shape: ("50,200,70,200,70,230,50,230")
Entry/exit: ("60,230,50,210")
No of nodes: 2
No of transport nodes:  0

Casualties Clearing Station:
Shape: ("70,200,90,200,90,230,70,230")
Entry/exit: ("80,230,80,230")
No of nodes: 2
No of transport nodes:  0

Technical Operational Command:
Shape: ("35,250,50,250,50,260,35,260")
Entry/exit: ("40,250,40,250")
No of nodes: 1
No of transport nodes:  0

Ambulance Parking Point:
Shape: ("50,250,90,250,90,280,50,280")
```

```
Entry/exit (sim area): ("0,245,0,235")
Entry/exit: ("60,250,60,255")
No of nodes: 4
No of transport nodes:  4

Obstacles:
Shape: ("130,70,300,70,300,120,130,120")
Shape: ("100,0,120,0,120,240,100,240")
Shape: ("100,250,120,250,120,300,100,300")
Shape: ("300,0,400,0,400,100,300,100")
Shape: ("360,100,400,100,400,230,360,230")
Shape: ("230,240,400,240,400,300,230,300")
```

A.2 Risavika Exercise Scenario

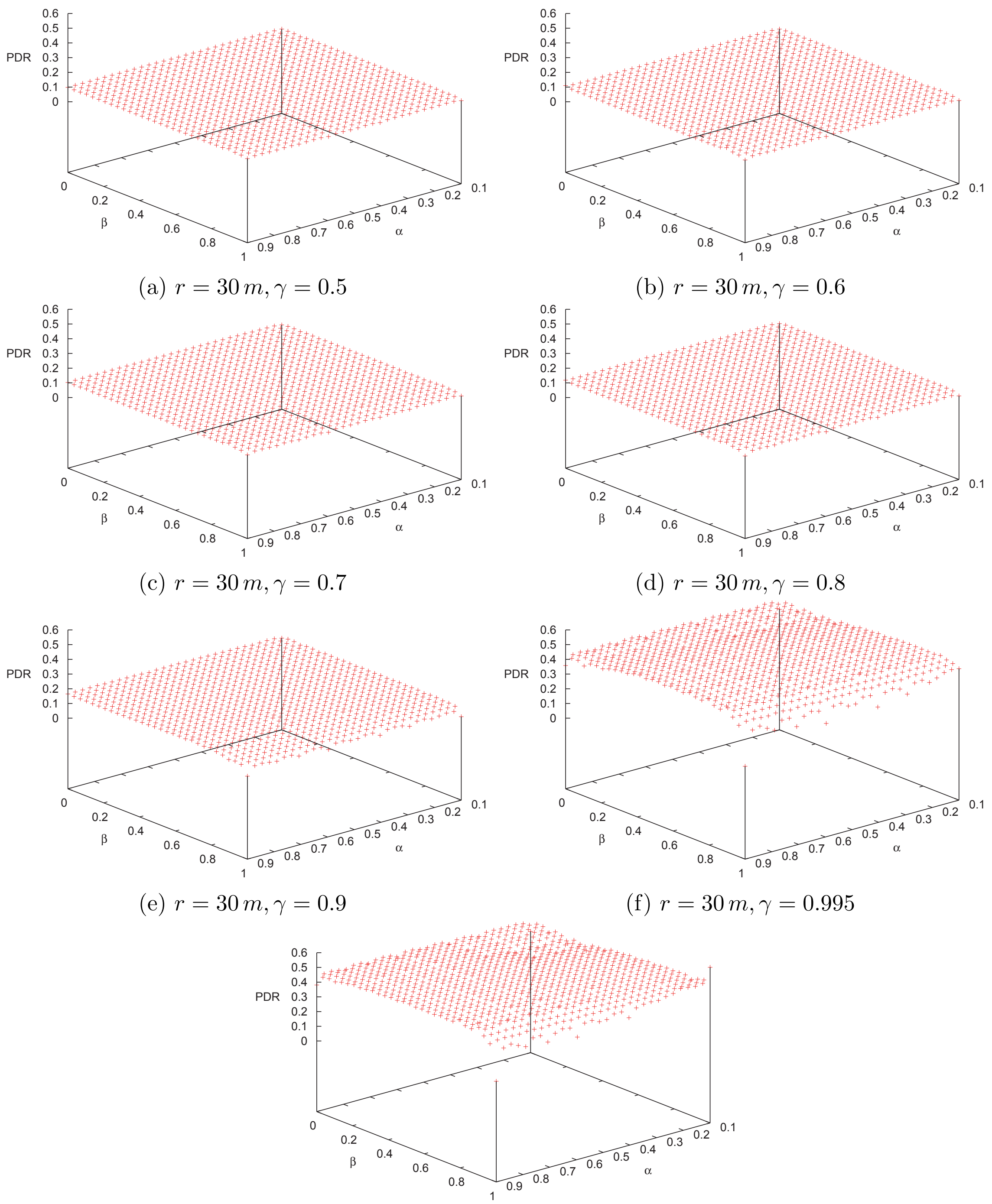
This section includes the definitions of tactical areas for the Risavika exercise scenario that has been introduced in Section 3.3. Please note that we changed the behavior of transport nodes in the implementation of the disaster area model in BonnMotion as described in Section 3.3.1. In particular, transport nodes choose the nearest tactical area instead of a random one, which better mimics the behavior of first responders during the real-world exercise.

```
Model: DisasterArea
Duration (-d): 7200
Seconds to skip (-i): 5000
Number of nodes (-n): 65
Area width(-x): 300
Area height (-y): 300
Prevent ambulances in areas other than APP (-K)
Random seeds (-R):
[114701,985702,687203,3957504,9704205,5668106,8296607,6296608,1842509,
4153310,1288311,1264012,9637413,85014,17215,203016,80617,973518,81019,
508420,269921,25522,490823,658424,729725,41626,457427,794028,236129,
582530,542931]

Incident Location:
Shape: ("250,110,265,110,265,180,250,180")
Entry/exit: ("250,130,250,130")
No of nodes: 10
No of transport nodes:  10

Patients Waiting For Treatment Area:
Shape: ("235,140,245,140,245,160,235,160")
Entry/exit: ("245,150,235,150")
No of nodes: 10
No of transport nodes:  8

Casualties Clearing Station:
Shape: ("170,70,195,70,195,85,170,85")
Entry/exit: ("245,150,235,150")
No of nodes: 5
No of transport nodes:  0

Incident Location:
Shape: ("200,50,215,50,215,75,200,75")
Entry/exit: ("200,72,200,72")
No of nodes: 10
No of transport nodes:  10

Patients Waiting For Treatment Area:
Shape: ("185,50,195,50,195,65,185,65")
Entry/exit: ("190,65,190,65")
No of nodes: 5
No of transport nodes:  4

Incident Location:
```

```
Shape: ("20,20,65,20,65,35,20,35")
Entry/exit: ("65,35,65,35")
No of nodes: 10
No of transport nodes:  10

Patients Waiting For Treatment Area:
Shape: ("70,20,90,20,90,45,70,45")
Entry/exit: ("70,35,80,45")
No of nodes: 10
No of transport nodes:  8

Technical Operational Command:
Shape: ("70,125,80,125,80,135,70,135")
Entry/exit: ("80,130,80,130")
No of nodes: 1
No of transport nodes:  0

Ambulance Parking Point:
Shape: ("95,125,150,80,160,90,105,135")
Entry/exit (sim area): ("265,265,265,270")
Entry/exit: ("105,135,160,90")
No of nodes: 4
No of transport nodes:  0

Obstacles:
Shape:  ("120,120,220,120,220,290,120,290")
```

APPENDIX B CoMANDR Parameter Evaluations

In this appendix we present evaluation results for CoMANDR using different settings for α, β and γ and different transmission ranges for the Risavika exercise scenario. The results presented in Figure B.1 and Figure B.2 show that γ has the highest impact on the packet delivery ratio (PDR). Based on these results it can be concluded that setting γ to 0.995 offers the best delivery ratio for the evaluated transmission ranges. On the other hand, α and β have a lower impact on the PDR. However, certain combinations of α and β should be avoided. For instance, setting both parameters to a value close to 1 has a negative impact on the PDR. We also performed such parameter studies for the other scenarios presented in this thesis and obtained similar results.



(a) $r = 30\,m, \gamma = 0.5$

(b) $r = 30\,m, \gamma = 0.6$

(c) $r = 30\,m, \gamma = 0.7$

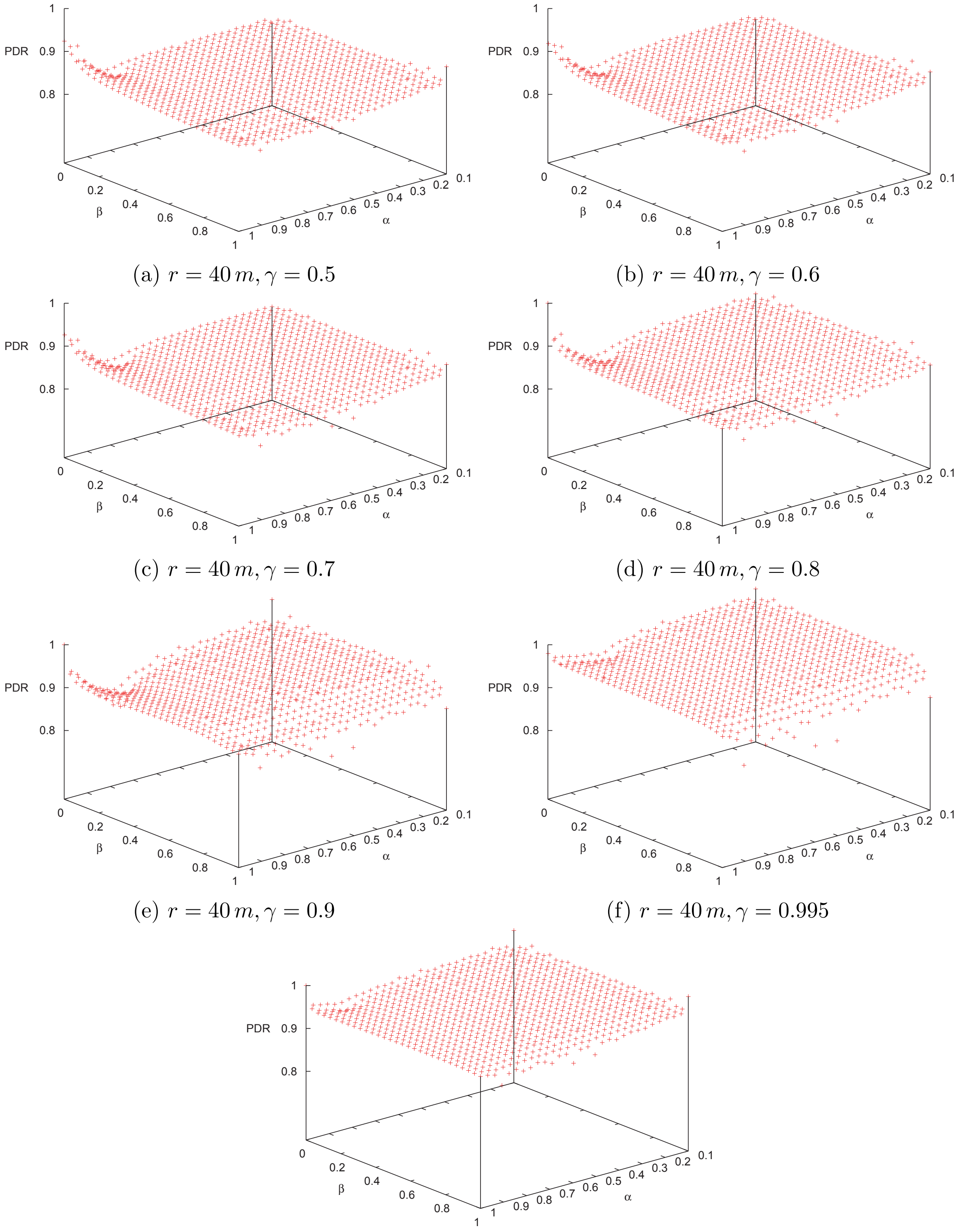
(d) $r = 30\,m, \gamma = 0.8$

(e) $r = 30\,m, \gamma = 0.9$

(f) $r = 30\,m, \gamma = 0.995$

(g) $r = 30\,m, \gamma = 0.999$

Figure B.1: Packet delivery ratio (PDR) of CoMANDR for different parameter settings and a transmission transmission range (r) of 30 m.



(a) $r = 40\,m, \gamma = 0.5$

(b) $r = 40\,m, \gamma = 0.6$

(c) $r = 40\,m, \gamma = 0.7$

(d) $r = 40\,m, \gamma = 0.8$

(e) $r = 40\,m, \gamma = 0.9$

(f) $r = 40\,m, \gamma = 0.995$

(g) $r = 40\,m, \gamma = 0.999$

Figure B.2: Packet delivery ratio (PDR) of CoMANDR for different parameter settings and a transmission range (r) of 40 m.