2022

Optimisation of Wireless Disaster Telecommunication Network based on Network Functions Virtualisation under special consideration of Energy Consumption

Paguem Tchinda, Auberlin

http://hdl.handle.net/10026.1/20097

http://dx.doi.org/10.24382/408
University of Plymouth

Copyright Statement

Optimisation of Wireless Disaster Telecommunication Network based on Network Functions Virtualisation under special consideration of Energy Consumption

by

Auberlin Paguem Tchinda

A thesis submitted to University of Plymouth
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Engineering, Computing and Mathematics

In collaboration with
Frankfurt Node of the Centre for Security, Communications
and Network Research (CSCAN)

March 2022

Acknowledgements

First and foremost, I would like to thank my supervisors Prof. Bogdan Ghita and Prof. Armin Lehmann, for their comprehensive support and guidance during this research work. A special thanks to Prof. David Walker for his support in the mathematical formulation of the optimisation problem. He was not part of the supervisor's team but was always available for queries and his knowledge contributed to the results achieved.

Second, I would like to express the deepest gratitude to my supervisor Prof. Ulrich Trick for his continuous support throughout the research work. He is an exceptional contributor to the success of this thesis. I truly thank him for his encouragement, constructive critique and perpetual availability throughout the past years.

Warm thanks go to the members of both the graduate school and the CSCAN Network at Plymouth University, and special thanks also go to the members of the Research Group for Telecommunication at Frankfurt node for their experienced support especially during PhD seminars.

I wish to thank my family and friends for their encouragement and support offered throughout the whole time of this research. Studying abroad was not easy and I would like to take this opportunity to tell you that I missed you very much. Especially my fiancée Phallone Noel Nguetna Yienu, who has been waiting for our wedding for a few years.

Author's declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Doctoral College Sub-Committee.

Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment.

Relevant scientific seminars and conferences were regularly attended at which work was often presented, and several papers prepared for publication.

Publications:

- Paguem Tchinda, A., Lehmann, A. and Trick, U. (2016) 'Untersuchung von Wireless Mesh Network-Routing-Protokollen für den Einsatz in Netzen für Katastrophengebiete', Berlin: VDE Verlag GmbH, (ITG-Fachtagung (2016), Osnabrück).
- Lehmann, A., Paguem Tchinda, A. and Trick, U. (2016) 'Optimization of Wireless Disaster Network through Network Virtualization', in INC.
- Paguem Tchinda, A., Frick, G., Trick, U., Lehmann, A. and Ghita, B. (2017) 'Performance analysis of WMN routing protocols for disaster networks', in 2017 IEEE Symposium on Communications and Vehicular Technology (SCVT). IEEE, pp. 1–6.
- Frick, G., Paguem Tchinda, A., Trick, U., Lehmann, A., Frick, G., Tchinda, A. P. and Ghita, B. (2018) 'Distributed NFV Orchestration in a WMN-Based Disaster Network', in 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN). IEEE, pp. 168–173.
- Frick, G., Paguem Tchinda, A., Shala, B., Trick, U., Lehmann, A. and Ghita, B. (2019a) 'Requirements for a Distributed NFV Orchestration in a WMN-Based Disaster Network', in 2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM). IEEE, pp. 1–6.
- Frick, G., Paguem Tchinda, A., Trick, U., Lehmann, A. and Ghita, B. (2019b) 'NFV Resource Advertisement and Discovery Protocol for a Distributed NFV Orchestration in a WMN-based Disaster Network', in 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). IEEE, pp. 1–6.
- Paguem Tchinda, A., Frick, G., Trick, U., Lehmann, A. and Ghita, B. (2020) 'High Throughput WMN for the Communication in Disaster Scenario', in 2020 World Conference on Computing and Communication Technologies (WCCCT). IEEE, pp. 53–63.
- Frick, G., Paguem Tchinda, A., Trick, U., Lehmann, A. and Ghita, B. (2020) 'Possible Challenges and Appropriate Measures for a Resilient WMN-Based Disaster Network', in 2020 World Conference on Computing and Communication Technologies (WCCCT). IEEE, pp. 70–78.

Presentations and Conferences attended:

- 21st VDE ITG Mobilkomtagung, Osnabrück, Germany, May 2016
- Collaborative Research Symposium on Security, E-learning, Internet and Networking (SEIN 2016), Frankfurt, Germany, July 2016
- 11th International Network Conference (INC 2016), Frankfurt, Germany, July 2016
- 24th edition of IEEE Symposium on Communications and Vehicular Technology (SCVT 2017), Leuven, Belgium, November 2017
- Collaborative Research Symposium on Security, E-learning, Internet and Networking (SEIN 2019), Darmstadt, Germany, March 2019
- The 2020 World Conference on Computing and Communication Technologies (WCCCT 2020), Warsaw, Poland, May 2020

Word count of main body of thesis: 35.681

Signed ………………………………………

Date ……19.12.2022……………………

Optimisation of Wireless Disaster Telecommunication Network based on Network Functions Virtualisation under special consideration of Energy Consumption

Auberlin Paguem Tchinda

Abstract

A working communication network is a key element in saving human lives after a disaster event. However, analysis of past disaster events shows significant damage to common communication network infrastructures such as the mobile network or landline. Consequently, a new communication network (Emergency Communication Network (ECN)) must be established immediately after the disaster to support rescue operations (e.g., civil protection, police, and volunteers) and to enable communication between the affected people. The established network is subject to several requirements. These requirements can be divided into infrastructure and service requirements. Infrastructure requirements include rapid deployment of the communication network, complete coverage of the disaster area, access for most of the terminals in use, failure safety of the network infrastructure and QoS support for the provided services. Service requirements include the scalability and failure safety of the provided services, as well as the quick integration of new services.

This research work aims to design a communication network that meets the requirements in the event of a disaster. For this purpose, a new network architecture is proposed. The proposed network architecture improves the performance of a wireless disaster network (Wireless Mesh Network (WMN)) through integration with Network Functions Virtualisation (NFV). This improvement is achieved by (first) eliminating dedicated hardware equipment (e.g., vehicles with heavy proprietary communication middleboxes, servers, satellite, and TETRA phones) and replacing them with conventional wireless routers, (second) introducing NFV to address the unresolved requirements of service scalability and rapid integration of new services, and (third) optimising energy consumption and resource use to solve the network sustainability problem.

This thesis has three significant contributions. Firstly, it investigates the routing in NFV optimised WMN for disasters and compares the performance of different routing protocols. It proposes a two-layer architecture that combines the advantages of both layer 2 and layer 3 routing and enables routing in large networks. Secondly, it addresses the throughput in WMN and proposes a new channel allocation scheme. The proposed channel assignment method is cluster-based and addresses issues such as the optimal cluster size or the maximum number of wireless interfaces. Previous works have not investigated these issues. This thesis's third contribution and focus are to develop algorithms for energy-efficient placement of VNFs in WMN. Since the devices forming the network in case of a disaster are often battery-powered due to damage to the power grid, the choice of a location for a VNF directly impacts the energy consumption and thus on the network's lifetime. Besides the mathematical formulation of the optimisation problem as multi-objective optimisation, the proposed algorithms are implemented, and their performance is compared in different scenarios.

Contents

List of Figures

List of Tables

1 Introduction

Digitalisation has become an integral part of today's society. Its importance is even more apparent in the event of a disaster, where drones, telemedicine, sensors and various other applications for coordinating and managing rescue operations ensure the rescue of human lives. These applications need a solid network to operate. However, common communication infrastructures (e.g., Integrated Services Digital Network (ISDN) exchanges or Long Term Evolution (LTE) / 5th Generation (5G) mobile network base stations) are often damaged by disaster events or are not existing in the affected area. An Emergency Communication Network (ECN) has to be deployed in such cases. The built network is subject to infrastructure requirements such as fast deployment or high network coverage and service requirements such as failure safety or scalability of the provided services.

Several authors have proposed a Wireless Mesh Network (WMN) as a suitable network architecture to address the infrastructure challenge in disaster scenarios (e.g.,(Portmann and Pirzada, 2008; Yarali *et al.*, 2009; Lehmann *et al.*, 2016)). A WMN is a decentralised network architecture in which the devices (wireless routers) that build the network can communicate via a point-to-point link or multiple hops using wireless technology when they are not in transmission range of each other. According to the same authors, this network is predestined for disaster communication due to its self-organisation, self-configuration, and self-healing properties.

Network Functions Virtualization (NFV) is an emerging technology that aims to provide more flexibility, scalability, and programmability in telecommunication (ETSI ISG NFV, 2012). The NFV framework proposes separating network functions from the underlying hardware components to achieve this goal (ETSI GS NFV 002, 2013). This separation between the network functions, which now run as software components within virtual machines or containers, and the physical hardware components (servers with computing power, memories, and switches) on which they run, opens up new optimisation opportunities.

This work proposes integrating NFV in WMN to address infrastructure and service requirements in disaster scenarios. The focus is on optimising energy consumption as a key element for the longevity of battery-powered devices and thus the network.

1.1 Research goal

This work aims to develop an energy-efficient communication network to support rescue work after a disaster and provides emergency services to the affected population. Primarily, it investigates which network infrastructure is best suited for this purpose. Secondarily, how network services can best be provided in such a case. And finally, how to combine both solutions to fulfil infrastructure and service requirements in the event of a disaster.

This combination results in the following objectives for this research:

1. To identify issues that arise from the use of WMN as Network Functions Virtualisation Infrastructure (NFVI).

2. To provide a solution to address the data transport in NFV optimised WMN for disaster scenarios. The provided solution must fulfil requirements such as the support of the VNFs live migration.
3. To provide a solution to address the problem of channel assignment in WMN. The provided solution must fulfil requirements such as topology preserve or interference compliance.
4. To identify energy optimisation opportunities arising from NFV integration in WMN.
5. To provide a mathematical formulation of the energy-efficient placement problem of VNFs in WMN that considers the network's unique characteristics, such as the limited power supply of the mesh routers or the shared wireless communication medium.
6. To develop and evaluate different algorithms to solve the energy-efficient placement of VNFs in the WMN for disaster scenarios.

This work was structured to achieve these research objectives as described in the following section.

1.2 Thesis Structure

The thesis is structured as follows: Chapter 2 introduces an earthquake as typical use case of the proposed solution, highlights the challenges of providing an ECN, and introduces the theoretical backgrounds on WMN and NFV. Moreover, it identifies routing and channel assignment in WMN and the placement of VNFs in telecommunication networks as research issues.

Chapter 3, Section 3.1 examines the network architectures that have been proposed to address the communication challenges in disaster scenarios. Section 3.2 discusses the publications that have addressed channel assignment strategies in multi-radio WMN. Similarly, Section 3.3 evaluates the existing WMN routing protocols, and Section 3.4 analyses the publications dealing with the energy-efficient placement of VNFs in other communication networks.

The first section of Chapter 4 introduces the general concept of the proposed NFV optimised WMN architecture to address the ECN requirements and highlights its benefits. The second section describes the proposed architecture in detail. The third section concludes this chapter by presenting the open research questions of the proposed architecture, focusing on the research questions addressed in this thesis.

The literature review on channel assignment strategies in Chapter 3 shows the need to deepen the comparison through field measurements. Section 5.1 presents the results of measurements conducted on a physical open space outside the city to determine the transmission and interference range in WLAN. Since none of the existing link- and cluster-based channel assignment strategies can handle the interference and the limited number of non-overlapping channels in IEEE802.11 standard, a new solution is proposed that goes beyond the existing strategies by addressing the optimal cluster size and optimal number of interfaces in Section 5.2.

Chapter 6 investigates the routing in NFV optimised WMN. For this purpose, the performance of three routing protocols for WMN is tested in different communication scenarios. These scenarios include link and traffic changes in Section 6.2, network topology changes such as router loss in Section 6.3, and the influence of the network size in Section 6.4. The evaluation is done with a test environment developed for this work. Section 6.1 describes the test environment and validates its functionality.

Chapter 7 addresses the placement of VNFs in WMN. Section 7.1 validates the power consumption model of a mesh router through measurements and formulates the problem of energy-efficient allocation of VNFs in the mesh network. Since the formulated problem is a multi-objective optimisation problem, Section 7.2 proposes different algorithms to solve it. Finally, simulations are conducted in Section 7.3 to evaluate the performance of the proposed algorithms.

Chapter 8 concludes the thesis. Section 8.1 summarises the most important outcomes. Section 8.2 highlights the limitations, and finally, Section 8.3 gives suggestions for further research.

References are located at the end of this thesis, together with a list of published papers.

2 Use Case and Theoretical Background

This chapter presents the use case and summarises the theoretical backgrounds related to this research work. Section 2.1 presents the use case by introducing ECN and highlighting the challenges of providing a communication network in a disaster scenario. Section 2.2 and Section 2.3 introduce the theoretical background of WMN and NFV, respectively. Besides describing the WMN and NFV architecture concept, these sections also present the research questions this work addresses.

2.1 Use Case

Disaster events have been reported to be increased during the last decade (International Telecommunication Union (ITU), 2013). It, therefore, becomes essential for countries to prevent it and create structures and organisations to save lives in case of an emergency. To achieve this task, rescue organisations rely on technologies like drones, telemedicine, and various applications to coordinate the helpers on the field (e.g., Voice over Internet Protocol (VoIP), webserver, file sharing). For the use of these technologies and applications, a functioning communication network is essential. This section introduces the use case this research addresses and identifies the challenges of setting up a communication network in a disaster scenario.

2.1.1 Emergency Communication Network (ECN)

A disaster is defined as a severe disruption of the functioning of a community or a society, causing widespread human, material, economic or environmental losses that exceed the ability of the affected community or society to cope using its own resources (UN/ISDR, 2004). According to the origin, disaster events are classified as naturally occurring and man-made (de Boer, 1990). Natural disasters result from natural processes and include earthquakes, floods, hurricanes, volcanic eruptions, avalanches, drought, meteoric collisions, and epidemics. In contrast, man-made disasters result from human activities. This includes explosions, the collapse of buildings, fires, and nuclear accidents and incidents. Since disasters vary significantly in their origins, sequences, and effects, it is difficult to define a fixed process for dealing with the disaster situation. This work addresses the case of an earthquake as a baseline scenario. After adaptations, the knowledge and insights gained can be applied to other disaster cases.

Saving human lives and protecting property in the event of an earthquake requires the cooperation of different organisations. For example, the following organisations are involved in rescue operations in Germany: Federal Agency for Technical Relief (THW), police, rescue services and hospitals, fire brigade, Red Cross, and volunteers. In rare cases, the military is also deployed. This was the case, for example, after the floods in June 2021 (RND, 2021).

The following description can be made for a disaster scenario: In its normal state, a community or society can be characterised by its geographical location, a population living and working in this area, a communication network infrastructure that serves the exchange of information between residents (e.g., the mobile communication network or the landline network) and the presence of other infrastructures such as roads, buildings and power supply (see Figure 2.1). The functioning of this normal state is usually affected by a disaster event (earthquake). This event leads to a differentiation in the population. A typical differentiation consists of people who have lost their lives, people in need (e.g. injured), helpers from different organisations, and other affected persons. Another consequence of the disaster event is the partial or complete destruction of infrastructures within the affected region. This includes the infrastructure of the communication network (see Figure 2.1).

The management of the rescue response leads to some infrastructure and service demands across the different population groups. The focus of this thesis is set on the communication demand, which can be described as follow:

- People in need require a way to make an emergency call.
- Helpers require depending on their organisation, a way to communicate with the different leaders in the command chain, a way to share information with other organisations, a way to do monitoring of the team deployment inside the disaster area, a way to use and communicate with helper devices (e.g., drones, medical robots). Volunteers have similar communication needs. An important difference with helpers who belong to an organisation such as the Civil Protection is that they also need a way to organise themselves into groups and to inventory the resources at their disposal.
- Other affected people are usually interested in receiving information on how to behave and answers to the question “Where can I find something (e.g., water, food, accommodation)”.

An ECN must be built immediately after the disaster event to meet these communication needs. This communication network is subject to particular challenges. These challenges are discussed in the following subsection.

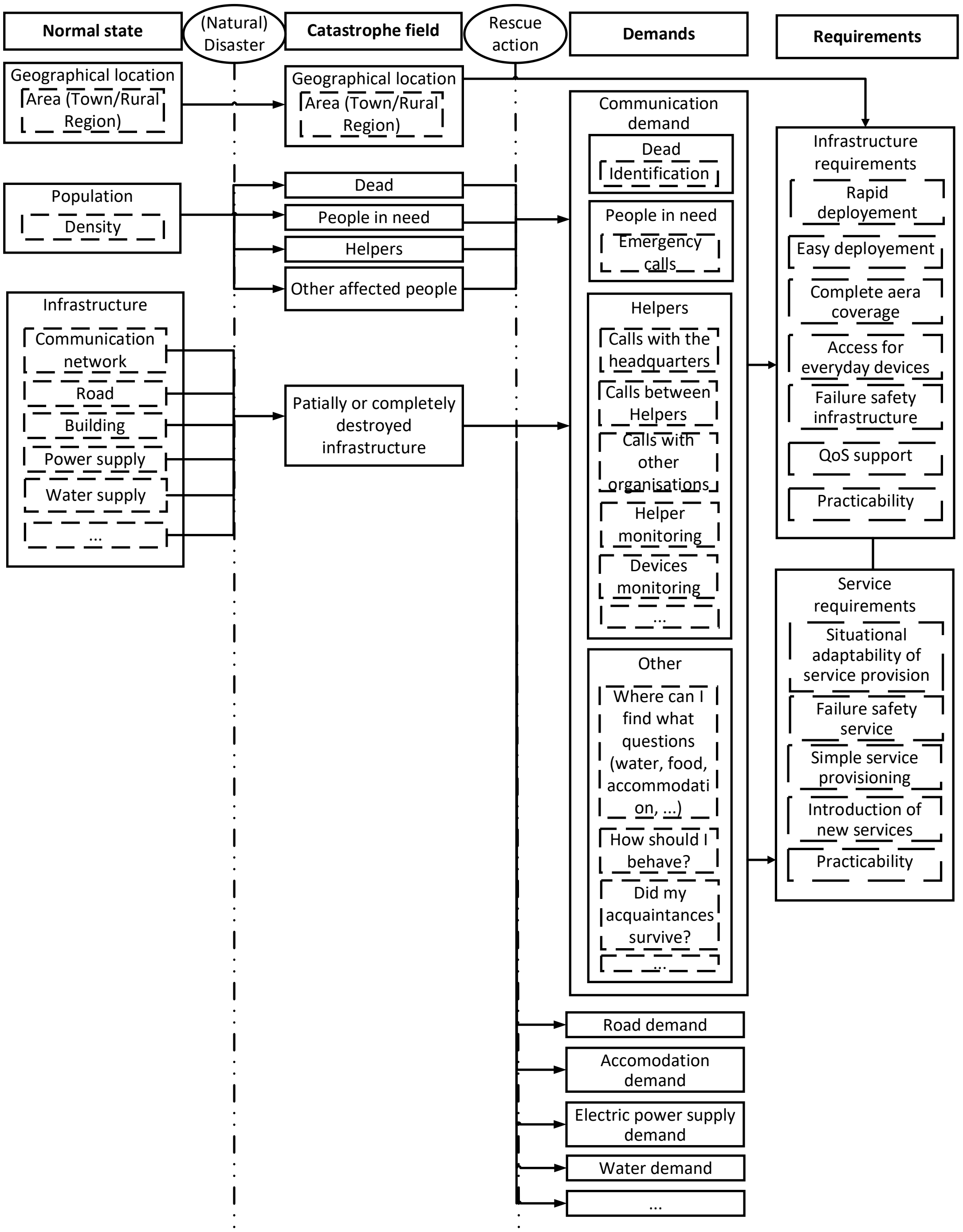


Figure 2.1: Network infrastructure and service requirements

2.1.2 ECN challenges

There are two significant challenges in setting up a communications network to support post-disaster rescue operations. The first challenge concerns the network infrastructure. Based on communication demand introduced in the previous subsection and previous works in (Nelson *et al.*, 2011; Huang and Lien, 2012; Ali *et al.*, 2015), the following requirements can be defined for the network infrastructure:

- Rapid deployment: Every minute is vital for people in need. Therefore the disaster network has to be deployed as quickly as possible.
- Easy deployment: The helpers must have no communication network knowledge to establish the network in the disaster area. Therefore the complexity of this process has to be as low as possible.
- Complete area coverage: The deployed network has to provide full coverage of the affected region to assure access to all user groups.
- Access for everyday devices: To ensure that the majority of users (people in need, helpers and other affected people) can access the network, the network entry has to be guaranteed by a common technology such as WLAN.
- Failure safety infrastructure: This requirement describes the network's capability to ensure the communication for the total duration of the rescue operation or until the regular network is restored. This resilience is not limited to failures due to physical damage to the equipment that makes up the network (e.g. aftershocks), but also and in particular includes failures due to lack of power in battery-powered equipment.

- QoS support: The network infrastructure should provide high throughput, low latency, and low packet loss to support the provided services.
- Practicability: The ECN should be constructed under a limited budget. Therefore cost inexpensive hardware is privileged.

The second challenge concerns the provided network services. The following requirements apply to these services (Souza Couto *et al.*, 2014; Viriyasitavat *et al.*, 2014; Ali *et al.*, 2015; Seo *et al.*, 2017):

- Situational adaptability of service provision: Depending on the scale of the disaster (earthquake) and the size of the affected area, the network services provided need to be adequately planned both in terms of their number (e.g. a call server for each team on site) and the number of requests they handle.
- Failure safety service: The failure of network services (e.g. due to lack of energy or physical damage to the devices) must be recognised and remedied as quickly as possible. This can be achieved, for example, through backup network services.
- Simple service provisioning: Services must be provided and configured automatically, if possible, to minimise the complexity and technical expertise required for the task.
- Introduction of new services: Innovation and progress are essential in rescue operations. The network must therefore be continuously updated to include new services.
- Practicability: Continuous updating of the network services provided incurs costs that must be kept low to accommodate the often limited budget for building the ECN.

In addition to the above-listed requirements, access to the network infrastructure and the provided services needs to be protected from malicious attacks by implementing security mechanisms. Due to time constraints, this research work does not address the security requirement.

2.2 Wireless Mesh Network

This thesis uses a WMN to address the network infrastructure challenge of ECN introduced in Section 2.1. The WMN architecture is considered the most appropriate network architecture to build the communication network after the disaster event due to its self-organisation, self-configuration and self-healing properties. This section introduces the WMN network architecture, explains the theoretical background of the routing process in WMN and presents the research questions addressed in this thesis.

2.2.1 WMN architecture

A WMN is a decentralised network architecture. Along with Smartphone Ad hoc Network (SPAN), Vehicular Ad hoc Network (VANET), and Wireless Sensor Network (WSN), it belongs to the family of Wireless Ad hoc Network (WANET). The term WANET refers to any network architecture where the devices, that build the network, are connected in a direct point-to-point manner using wireless technology (e.g. 802.11, 802.15, or 802.16) (Bradonjié and Kong, 2007). The differentiation between categories of WANETs is made depending on the devices, which build the network. In SPAN, the network is built using smartphones. In VANET, the network is created by cars. In WSN, the network consists of sensors. In contrast to SPANs and VANETs where the network devices´ mobility is of great importance. It is assumed that the sensors in WSN are static. WMNs are typically used to provide broadband internet access in rural regions (Yarali *et al.*, 2009). The WMN network consists of fixed routers or routers with low mobility. There are three types of WMN (Akyildiz and Xudong Wang, 2005):

- Infrastructure/Backbone WMN: The infrastructure mesh consists of wireless routers and gateways. The main objective of this mesh type is to connect multiple networks, for example, over a city. The infrastructure mesh is often linked to external networks (e.g., Internet or mobile network) and extends the connectivity (see Figure 2.2).

- Client WMN: The client mesh is built with user-end devices like smartphones, laptops or printers. This type of WMN is typically used to connect multiple devices without cabling (see Figure 2.2). One example of client mesh can be the ad hoc connection between the devices of a fire department team during the rescue operation.

- Hybrid WMN: The hybrid mesh combines infrastructure and client mesh segments (see Figure 2.2).

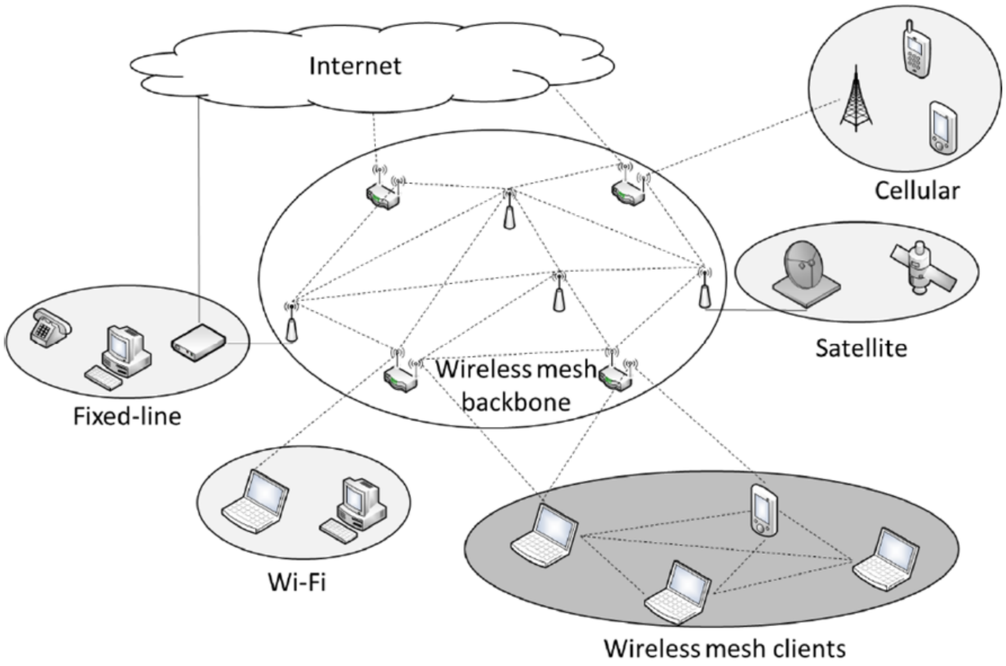


Figure 2.2: Wireless Mesh Network architecture (Lehmann *et al.*, 2016)

The standard classification of devices inside a mesh network differentiates between mesh point (MP), mesh portal point (MPP) and mesh access point (MAP) (see, e.g. (Bari *et al.*, 2012)). A MP is a wireless device which forwards data packets according to the implemented routing protocol. If a MP provides access point functionalities (e.g., over an additional WLAN interface) so that client devices can connect to the mesh over it, it is called MAP. A MPP is a MP that provides connectivity to another mesh or an external network. These three device types are referenced in the rest of this document as mesh routers if nothing else is mentioned.

This thesis remains on a hybrid WMN architecture to build the ECN. Since it combines both infrastructure and client mesh, it can provide a gapless coverage of the disaster area. The backbone part is set up by mesh routers distributed by the helpers (e.g., civil protection) over the disaster area immediately after the disaster event. These routers are battery-operated due to damage to the power supply network. All organisations, and victims use the infrastructure mesh. The several client meshes are set up by each organisation with its equipment and are used to extend coverage (e.g., firefighters working in a burning building). In the following of this thesis, the focus is set on the infrastructure segment since client devices often do not have enough resources to provide services (see Chapter 4). However, the results obtained can be applied to a client mesh when this restriction no longer applies.

This research work proposes using the WLAN technology to realise the infrastructure segment. However, the solutions developed can also be applied to other wireless technologies. The WLAN standard is specified in IEEE802.11 (IEEE, 2016). This technology is chosen for the following reasons:

- Many works have dealt with a WLAN-based WMN (e.g., (Raniwala and Chiueh, 2005; Skalli *et al.*, 2007; Portmann and Pirzada, 2008; Bari *et al.*, 2012; Mamechaoui *et al.*, 2013).). There are publications, various implementations (e.g., WLAN Chip Drivers, simulation, and emulation tools), and routing protocols on the subject.
- WLAN enables a high data rate compared to other wireless technologies like Long Range (LoRa) (Centenaro *et al.*, 2016) or Bluetooth (IEEE, 2002). This means that the WMN can support numerous applications (see network infrastructure requirements in Section 2.1).
- The WLAN hardware are inexpensive to acquire. Low hardware costs are essential for a later approach in disaster situations (see network infrastructure requirements in Section 2.1).

IEEE802.11b/g/n defines 14 channels with a bandwidth of 5MHz in 2.4GHz frequency range (2401-2495MHz). Of these channels, 3 to 4 are non-overlapping, depending on the current jurisdiction of the country in which the WLAN is operated. In IEEE802.11a/n/ac, 23 more non-overlapping channels with a bandwidth of 20MHz in the 5GHz frequency range (5030-5990MHz) are defined in the Germany (EUR-Lex, 2005; 2007; IEEE, 2016).

2.2.2 WMN routing protocols

Inside a WMN, mesh routers can communicate together in a point-to-point manner. If a point-to-point communication cannot be established (e.g., due to the limited transmission range of WLAN antenna), a routing protocol is used to determine a path over multiple hops. Therefore, the routing protocol directly influences the performance of the WMN. Due to this importance, routing protocols have been widely investigated for WMN, and more than 100 protocols were proposed (Junhai *et al.*, 2009; Ahmeda and Esseid, 2010; Dodke *et al.*, 2016; Lavanya *et al.*, 2017). This subsection introduces the common routing mechanisms. Figure 2.3 shows the list of these mechanisms. A routing protocol can implement only one feature. For example, it can be either a link state or a distance vector based protocol.

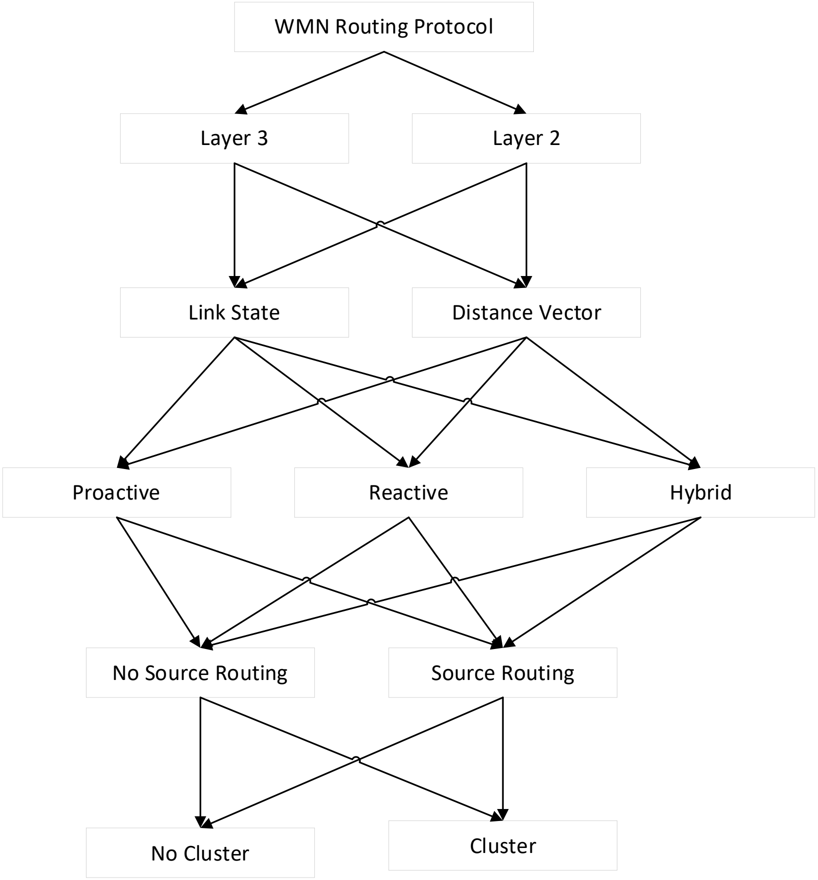


Figure 2.3: Routing protocol features

Layer 2 and 3 routing: Common routing protocols implement a layer 3 based routing scheme. This means packets are transmitted between the source and destination mesh routers based on their IP addresses. Due to the flat topology of WMN, the use of IP addresses has lost one of its most significant advantages, namely the ability to address network packets to a specific segment. The ability to address packets within a network reduces the overhead caused by the routing protocol, as the information about each device does not need to be transmitted across the entire network, but only the information about the segment to which it belongs. Since IP use within a flat topology offers no real advantage, a new generation of routing protocols such as B.A.T.M.A.N. advanced (Open-Mesh, 2022b) and HWMP (IEEE, 2016)has been developed. These protocols transmit packets based on their MAC addresses. They are therefore referred to as Layer 2 routing or forwarding protocols.

Link state and distance vector routing: In link-state routing protocols, each router determines the quality of the connection with its neighbouring routers (link state). This information is then sent to all nodes within the network. Based on this, each node can recover the entire network topology and calculate the shortest route (next node on the way) to the destination and the expected metric. This calculation is usually performed using Dijkstra's algorithm (Dijkstra, 1959). Distance-vector protocols work in a different way. Each node regularly shares its routing table with its neighbouring nodes (1-hop neighbours). The neighbouring nodes that receive this information update their own routing table and, under certain conditions (e.g. the announced route is previously unknown, the announced route is more recent than the route stored in its own routing table, or the announced metric is better than the current one), select the node that announces the route as the next node to reach a destination. The major advantage of distance vector routing compared to link state routing is that a complete knowledge of the network topology and intensive path computation is not required. The disadvantage is that loop can be crated during the forwarding process (Count-To-Infinity effect (Kurose and Ross, 2008)).

Proactive, reactive and hybrid routing: Proactive routing protocols (e.g. DSDV (Perkins and Bhagwat, 1994) or OLSR (Clausen and Jacquet, 2003)) determine and maintain a current communication path between each existing source and destination pair within the mesh network. The advantage of this routing strategy is that the delay at the start of communication can be avoided. The main disadvantage is that the communication path is determined and maintained even when it is not in use. This leads to an unnecessary overhead of the routing protocol. Reactive routing protocols (e.g. AODV (Perkins *et al.*, 2003) or DSR (Johnson *et al.*, 2001)) offer a solution to this problem. With reactive routing protocols, the communication path is determined on demand. When the source wants to communicate with a particular destination, the process to determine the optimal communication path is started. This strategy reduces the overhead of the routing protocol in uncongested networks (networks with low communication volume). Still, it delays at the beginning of the communication (time required to determine the communication path). Hybrid routing protocols (e.g. HWMP (IEEE, 2016) or ZRP (Haas and Pearlman, 1998)) combine proactive and reactive routing strategies to merge the advantages of each mechanism. The goal of this approach is to predict the expected network traffic. This prediction is used to define a region or specific nodes that will use a proactive routing scheme when determining the communication route to other nodes or areas on demand.

Source routing: In source routing protocols, an additional header is added to all packets from the source node to define the communication path. This header consists of a partial or complete list of routers on the path to the destination. Source routing is used by WMN routing protocols such as DSR (Johnson *et al.*, 2001). A primary use case of source routing is the implementation of multiple communication paths (e.g. AODV-PA (Gwalani *et al.*, 2003), MP-OLSR (Yi *et al.*, 2008)).

Cluster-based routing: WMNs have a flat network topology. Due to this characteristic, routing packets cannot be addressed. They are therefore transmitted via broadcast over the entire network. The ability to address packets within a network reduces overhead because packets such as route requests do not have to be sent over the whole network but only to the segment they belong to. One solution to the addressing problem in WMN is to divide the network into several domains or clusters (e.g. (Jiang, 1999; Singh *et al.*, 2011; Kaushal *et al.*, 2012)). An intra-cluster routing protocol is used to determine the communication path within a cluster. An inter-cluster routing protocol is used to determine the communication path for communication between nodes in different clusters. In most cases, this process involves a cluster head (a node that stores information about all destinations within the cluster) and one or more cluster gateways (nodes that belong to multiple clusters).

2.2.3 WMN challenges

This research work aims to address the following challenges:

Limited throughput: One major challenge in WMN is the network throughput which depends on the number n of mesh routers interfering together $1/\sqrt{n \log n}$ (Gupta and Kumar, 2000). Interferences appear in WMN when multiple mesh routers are running on the same physical channel due to the sharing nature of the wireless medium. To avoid the collision between the data frames, the IEEE802.11 standard implements the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) method (Molisch, 2011; IEEE, 2016). The drawback of this solution is that only one mesh router can send a packet at a time. As a result, the network throughput decreases. There are two main approaches to solve this problem: the first one is an improvement of the medium access method to support multiple channels. This approach is described in the literature as single-radio multi-channel WMN (e.g., (So and Vaidya, 2004; Jia and Zhang, 2007; Lin *et al.*, 2011)). In (So and Vaidya, 2004), for example, two mesh routers that want to exchange packets with each other try to negotiate a channel in advance. This way, the transmission no longer interferes with the neighbouring routers, which can now simultaneously transmit on another non-overlapping channel. The main disadvantage with this solution is that it is challenging to because it requires constant synchronisation between the mesh routers to determine which channel to use. The second approach consists of using multiple radio interfaces running on non-overlapping channels. This solution requires less changes to the medium access method (Choi *et al.*, 2006; Nan *et al.*, 2007; Liu and Wu, 2010) and has become more popular in recent years because the cost of an additional WLAN interface has decreased. For example, an additional WLAN interface can be achieved on most devices using a WLAN USB stick. The usage of multiple interfaces leads to the problem of channel assignment. This problem will be addressed in Section 3.2, where a literature review of existing channel assignment strategies is conducted.

Based on the ECN requirements introduced in Section 2.1 and the research works in (Skalli *et al.*, 2007; Alim Al Islam *et al.*, 2016), the following requirements can be defined for the channel assignment procedure:

- Topology preserve: When assigning channels, link breaks have to be avoided. A link break is the loss of a point-to-point connection between two routers within the transmission range of each other. Link breaks during the CA process can only be avoided if each router has as many interfaces as neighbouring routers or can communicate with several routers via one interface. Link breaks must be avoided because they can lead to connectivity loss or network partition.
- Interference compliance: This requirement describes the ability of the CA procedure to take into account the interference occurring in WMN by providing a

suitable distance for the repetition of already allocated channels. According to the authors in (Raniwala and Chiueh, 2005), this distance is two times the transmission range.

- Scalability and complexity: High scalability and low complexity are two further requirements imposed on the CA strategy. The used strategy should be applicable in both small and large networks (see ECN requirements in Section 2.1). Dynamic synchronisation procedures such as negotiating a free channel between two mesh routers must be avoided.
- Throughput: The throughput depends on the number of mesh routers that interfere with each other. To maximise the link data rate, the number of routers communicating over the same channel must be minimised. In an optimal case, a channel is only used for communication between two routers.
- Wireless standard compliance: Standard compliance is the ability of the CA method to use the limited number of non-overlapping channels defined in the communication standard. For example, the IEEE802.11 standard defines 3 or 23 channels in 2.4GHz or 5GHz frequency ranges, respectively (see Section 2.2). A CA strategy that would require more than 3 or 23 channels would not be compatible with this standard.

Routing of packets: Another challenge that this thesis aims to address is the routing of packets. Although several research papers are available on using a WMN to establish a communication network after a disaster event, only a few publications have addressed the problem of routing in WMN for disaster scenarios (e.g., (Baraković and Baraković, 2010; Alamsyah *et al.*, 2018; Jahir *et al.*, 2019)). In (Reina *et al.*, 2011), the authors investigate the performance of the routing protocols AODV, DSR and AOMDV for use in an ad-hoc network for disaster response. The comparison is based on throughput, packet delivery fraction, normalised routing load, and average end-to-end delay. The simulation results show a better outcome for the AODV protocol in networks with high mobility. The DSR and AOMDV routing protocols show better results in networks without mobility.

In this work, the evaluation of routing protocols is carried out based on the following requirements (Ahmeda and Esseid, 2010; Owczarek and Zwierzykowski, 2013; Chauhan and Sharma, 2016; Paguem Tchinda *et al.*, 2016):

- Decentralised routing: To avoid single point failure (e.g. due to aftershocks after an earthquake), the routing process should be performed in a decentralised manner. This requirement results from the failure safety requirement of the network.
- Dynamic routing: This requirement describes the ability of the routing protocol to react quickly to dynamic changes in the network. These changes include the failure of a mesh router, the discovery of a new router, or important changes in connection quality.
- Number of end devices: Depending on the size of the affected area and the communication use cases (e.g., IoT devices), the excepted number of connected devices can be significant. The performance of the routing protocol should not be affected by this number.
- Path computation: Depending on the chosen routing mechanism, the difficulty of path calculation may vary. Due to the limited computing resources on the mesh routers and the need to minimise the power consumption, extensive calculations must be avoided.

- Routing overhead: The number of packets used by the routing protocol for its operations has to be minimised due to the limited throughput in WMN and the necessity to reduce the energy consumption.
- License-free: The communication network in a disaster scenario is built under a limited budget. The used routing protocol should therefore be license free.

In Addition to these requirements, the following requirements are introduced to take care of the NFV optimisation proposed in this work:

- VNF live migration support: Live migration of VNFs is an important use case in the proposed NFV-optimised WMN architecture. For example, the migration of VNFs can be used to increase the lifetime of the network by reducing the energy consumption (see Section 7). The routing protocol should implement a mechanism to avoid communication interruptions when a VNF changes its hosting mesh router to enable this migration.
- Service aware traffic routing: In contrast to conventional WMNs, in which packets are forwarded based on the destination IP or MAC address (layer 2 and 3 routing), data packets in an NFV optimised WMN must additionally be transmitted depending on the QoS (Quality of Service) of the network service to which the packets belong.

2.3 Network Function Virtualisation

This thesis proposes the use of Network Functions Virtualisation (NFV) to address the challenge of network service provisioning in ECN. The concept of NFV was introduced in 2012 at the SDN OpenFlow Congress by a consortium of service providers. NFV aims to address current challenges in the telecommunication branch like the scalability of network services and at the same time reduce deployment costs and application time-to-market by introducing more flexibility and programmability in the communication network (NFV White Paper, 2012). To achieve this goal, a specification group was created in 2013 at the European Telecommunication Standards Institute (ETSI), and the ETSI NFV Framework was released a few months later. The proposed framework remains on virtualisation to provide complete separation between hardware components and network functions, which are now implemented as Virtual Network Functions (VNFs) (Chayapathi *et al.*, 2016). This section introduces the ETSI NFV Framework, presents different virtualisation technologies as a key element for NFV development, and highlights the placement of VNFs as the main challenge to increase the energy efficiency of the communication network in the disaster scenario.

2.3.1 ETSI NFV Framework

The goal of the ETSI NFV framework is to provide a guideline for the development of NFV, which guarantees the interoperability between VNFs of different vendors and the independence from hardware manufacturers. The framework consists of three main components, as shown in Figure 2.4:

Figure 2.4: NFV framework (ETSI GS NFV 002, 2013)

- **Network Functions Virtualisation Infrastructure (NFVI):** The NFVI describes the hardware components (servers with computing resources, memory and switch). It uses a virtualisation technology (represented in Figure 2.4 through the virtualisation layer) to abstract and to create separated virtualisation resources (virtual computing, storage, and network interfaces) that are necessary to run the virtual network functions (ETSI GS NFV 002, 2013).

- **Virtualised Network Functions (VNFs):** a VNF is a software implementation of a network function (e.g., firewall, NAT or router) running inside a virtual machine. It must be developed to run on top of any hardware with adequate computing, storage, and network interfaces. However, the developer can specify the minimum resources necessary to run the VNF (Chayapathi *et al.*, 2016).

- **NFV Management and Orchestration (MANO):** MANO is responsible for the resources allocation and configuration of VNFs. Therefore, it interacts as well with NFVI as with the VNFs. To achieve this task, it is subdivided into three blocks. The first one, the Virtualised Infrastructure Manager (VIM), manages and controls physical and virtual resources in a single domain. The second block is built by the VNF Managers (VNFMs). They are required to handle the live cycle of one or more VNFs. It can also communicate with the VIM to scale the resources allocated to the VNF. The last block consists of the NFV Orchestrator (NFVO). It bridges the current Operational and Billing Support System (OSS/BSS) and the two other blocks. It analyses the OSS/BSS request and communicates the required elements to the VIM and VNFM to build an end-to-end network service (ETSI GS NFV 002, 2013).

2.3.2 Virtualisation Technologies

One of the main drivers for the development of NFV is the progress in Information Technology (IT) during the last years, particularly in virtualisation technologies. Unlike the common NFV use cases, this project aims to deploy VNFs outside the data center on hardware with limited resources (mesh routers). This leads to some constraints regarding resource usage and hardware compatibility for the used virtualisation technology. Two virtualisation technologies exist:

Virtual Machine-based virtualisation: In Virtual Machine (VM) based virtualisation, a hypervisor provides an abstraction of the underlying resources. It is differentiated between two types of hypervisors: type-1 (see Figure 2.5 b)) and type-2 hypervisor (see Figure 2.5 a)). A type-2 hypervisor (e.g., Qemu, or Oracle VirtualBox) is software installed on top of the host machine's operating system (OS). A type-1 hypervisor (e.g., VMWare ESXi, Xen, or Microsoft Hyper-V) is an operating system specially developed for virtualisation purposes. Because there are no elements between the hardware and the hypervisor, this type of virtualisation shows a better result than type-2 hypervisors in terms of resource efficiency. However, because the implementation of type-1 hypervisors involves the implementation of the hardware-dependent associated OS, this type of hypervisors are reputed to be more challenging to implement than type-2 hypervisors (Chayapathi *et al.*, 2016).

Container-based virtualisation: For many applications, the isolation provided by a VM is not needed. In these cases, containers offer a good alternative. Unlike VMs, containers do not require a hypervisor (see Figure 2.5 c)). The user space of the working host is modified to allocate resources to each container (Chayapathi *et al.*, 2016). Due to the absence of the guest OS, containers are more resource-efficient than VMs. Another advantage is that containers can be started and stopped in a few milliseconds. One major disadvantage of container virtualisation is that a kernel update for a unique container is impossible. In addition, containers present more security issues than VMs due to their architecture (Barik *et al.*, 2016). Common container-based solutions include open source solutions like LXD and Docker.

Due to the limited resources of mesh routers and the need to enable live migration of VNFs to support rescue operations, this research remains on container-based virtualisation technologies.

Figure has been removed due to Copyright restrictions.

Figure 2.5: (a) Type-2 hypervisor (b) Type-1 hypervisor (c) Docker-based container virtualisation (Chayapathi et al., 2016)

2.3.3 NFV challenges

There are several research questions related to the integration of NFV in telecommunication networks (Mijumbi *et al.*, 2016). One of these questions is the placement of VNFs on the network infrastructure NFVI. Because the location of a network function is no longer bound to a physical location (hardware), this location can be optimised to achieve goals such as low latency or maximum throughput for the services provided. In this work, the location of the VNFs has to be optimised in order to minimise the energy consumption of the network on the one hand and to maximise the lifetime of the network on the other hand (function time of the network without failure of a router due to too low residual energy).

The energy consumption of a mesh router depends on two components, namely the forwarding and the processing component. The forwarding component of energy consumption is the consumption that arises from the forwarding of packets. The processing component of energy consumption is caused by the processing of service requests by the VNFs running on the router. Because the location of the VNFs can influence both components of energy consumption, optimal positioning of the VNFs is crucial to optimise the network's energy consumption.

The first step in optimising the placement of VNFs in the network is to develop a suitable model. A model is a simplified representation of the network to be optimised. This means that only specific processes and relationships are described, e.g. energy consumption, hardware resource constraints or the communication behaviour of the users. A suitable model must map the following properties (Soualah *et al.*, 2017; Agarwal *et al.*, 2019; Tajiki *et al.*, 2019; Nemeth *et al.*, 2021):

Service-specific properties:

- Distributed service requests: The service requests to the VNFs (e.g., requests sent to a webserver) are sent from different locations in the network (different access points). In comparison, for example, in a data center, all the service requests have the same ingress/egress port and the same communication path through the network infrastructure.

- Dynamic service requests: The number of service requests sent from a specific access point is dynamic (changes over time) due to the mobility of the helpers (progress in the rescue operation) and other users.

Infrastructure-specific properties:

- Limited computing resources: The VNFs run on wireless routers with limited resources (CPU and memory). This limitation is an important difference to data centres, where powerful servers are used.
- Dynamic network infrastructure: The network infrastructure in a disaster scenario is subject to changes (e.g., router loss or new router).
- Battery-powered routers: Many routers which build the network in disaster scenarios are battery-powered. Therefore, optimisation should not be limited to the energy consumption but should also consider and model the total lifetime of the network.

Wireless-specific properties:

- Shared communication medium: The link quality in WMN has no fixed capacity. The speed at which data can be transferred over a link depends on the number of stations using the same channel and if they have data to send.
- Change in the link quality: The link quality (and therefore the link capacity) in WMN is subject to different changes over time (e.g., environmental changes or interferences).

3 ECN Architectures, Channel Assignment Strategies, Routing Protocols, and Energy-Efficient Placement of VNFs in WMN

This chapter consists of four sections, each dedicated to one of the following research topics introduced in Chapter 2: ECN architectures, channel assignment strategies, routing protocols, and energy-efficient placement of VNFs in WMN. Section 3.1 examines the works that propose a solution for building a disaster communication network. A distinction is made between mesh and non-mesh based solutions. Section 3.2 analyses the strategies for channel allocation in multi-radio WMN. These methods can be classified into two groups, namely link and cluster-based methods. In section 3.3, the most widely used WMN routing protocols are investigated for their use in disaster situations. Finally, Section 3.4 examines the research works that have been done on the energy-efficient placement of VNFs in telecommunication networks. At the end of each section, the proposed solutions are evaluated based on the requirements in Chapter 2. From this evaluation, it is decided whether the existing solutions fit the primary objective of this thesis, whether confirmation through simulations, field tests, or measurements is necessary, or whether elaboration of a new solution is required.

3.1 Related Work on Current Network architectures for communication in disaster scenarios

This section presents the network architectures that have been proposed to address the communication needs in disaster situations. A distinction is made between mesh and non-mesh based architectures. This literature review aims to define the current development in disaster communication. Therefore, the focus is on publications and research projects that have taken place in recent years. Finally, these publications and projects are evaluated based on the infrastructure and service requirements defined in Section 2.1.

3.1.1 Mesh-based ECN architectures

A mesh is a promising network architecture that can be used to build a recovery network after a disaster. Several projects remain on this architecture due to its characteristics highlighted in Section 2.2.

The research project **SPIDER** (Security System for Public Institutions in Disastrous Emergency scenaRios) aims to develop an intelligent communication and information system to enable efficient emergency process management of all stakeholders (e.g. police, fire brigade, red cross societies and hospitals) in case of natural disasters and other major catastrophes. To build the network, they use an IEEE 802.11 based ad hoc network. The network consists of small WLAN routers called Dropped Units. The proposed network should support the rescue teams by their operations on the disaster field. To facilitate the construction of the network, the project proposes to bring the routers directly on the equipment (e.g. water hose) (see Figure 3.1) so that the time necessary to deploy the network can be saved (Wolff *et al.*, 2012). This avoids supplementary workforce to build the network and unnecessary delay in the rescue response. Due to the critical character of information exchanged during the disaster, a particular focus of the project was set on the security of the proposed ad hoc network. To achieve this goal, a new secure WMN routing protocol PASER (Position AwareSecure and EfficientRoute Discovery Protocol), was proposed in (Sbeiti *et al.*, 2016). This protocol was evaluated by comparing with the protocols AODV, DYMO (Dynamic Manet On-demand), B.A.T.M.A.N., and OLSR in (Sbeiti *et al.*, 2012). The third contribution of this project is the Interference Avoidance Algorithm (IAA) presented in (Wolff, 2013), which disables redundant routers to reduce interferences. SPIDER highlights the importance of information sharing between different organisations in the disaster scenario. To solve this problem, the project proposes the XML-based Protection and Rescue Markup Language (PRML) in (Subik *et al.*, 2010), which defines a format for the information that has to be shared between the IT systems of the involved organisations. PRML is used to manage access to these data according to specifically defined rules. The main shortcoming of this project is that the proposed network solution can only be used in the event of local damage, e.g., a fire in a stadium. The coverage of the network is limited to small areas. Communication after major disasters like earthquakes, when no connection to the public network can be established, is not considered. Moreover, the cooperation between the organisations is limited to data sharing. Services such as telephony between team members of different organisations are not provided.

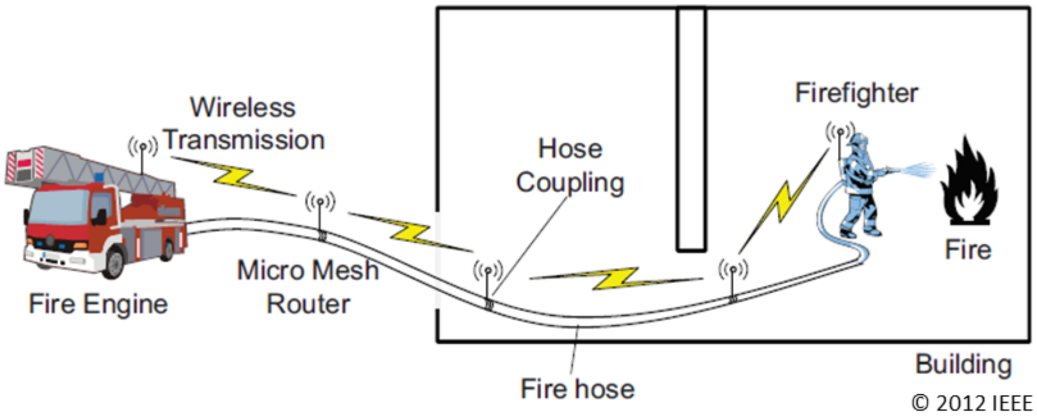


Figure 3.1: Process-Oriented Incident Network Deployment (Wolff *et al.*, 2012)

The **NICER** (Networked Infrastructureless Cooperation for Emergency Response) project was funded by the Hessia state ministry for higher education, research, and the arts (NICER, 2022). It is divided into three main research areas. The first one examines the usage of cyber-physical help systems like robots. The second area focuses on the communication network. It aims to provide a delay-tolerant network architecture to support rescue operations. The third research area of NICER deals with services and applications in disaster scenarios. This research area aims to develop basic services for disaster communication. The focus is on the distribution of services so that they can function equally in the different locations and the overall network. Figure 3.2 shows the architecture of the proposed solution in (Nguyen *et al.*, 2015). It consists of three layers: on-site responders, on-site coordinators and coordination platform. The coordination platform is the central headquarter. It typically receives the emergency call, decides to send the fire trucks from different locations by large damages and coordinates their operations. The second layer consists of the fire trucks. They use the internet to connect to the central headquarter and act as a bridge for communication with the firefighter on-site. The fire trucks are also used to manage the communication between the firefighters in a specific location. They are equipped with an onboard communication system that provides data buffering or information synchronisation services. The onboard communication system allows delay-tolerant communication between the different layers. The last layer is built by the firefighters on-site. They are equipped with devices like smartphones and tablets, which are used to collect information. The major contribution of this project is the introduction of a delay-tolerant communication based on publish/subscribe queuing between different layers of the responders' hierarchy. In contrast to SPIDER, the NICER solution provides an on-site ad hoc network for the coordination and information sharing between firefighters' different departments. This is necessary when communication with the central headquarter cannot be established. However, NICER proposes to use LoRa to bridge long distances between the fire trucks in different locations. This is a bottleneck for communication due to the low bitrate of the LoRa protocol (Centenaro *et al.*, 2016).

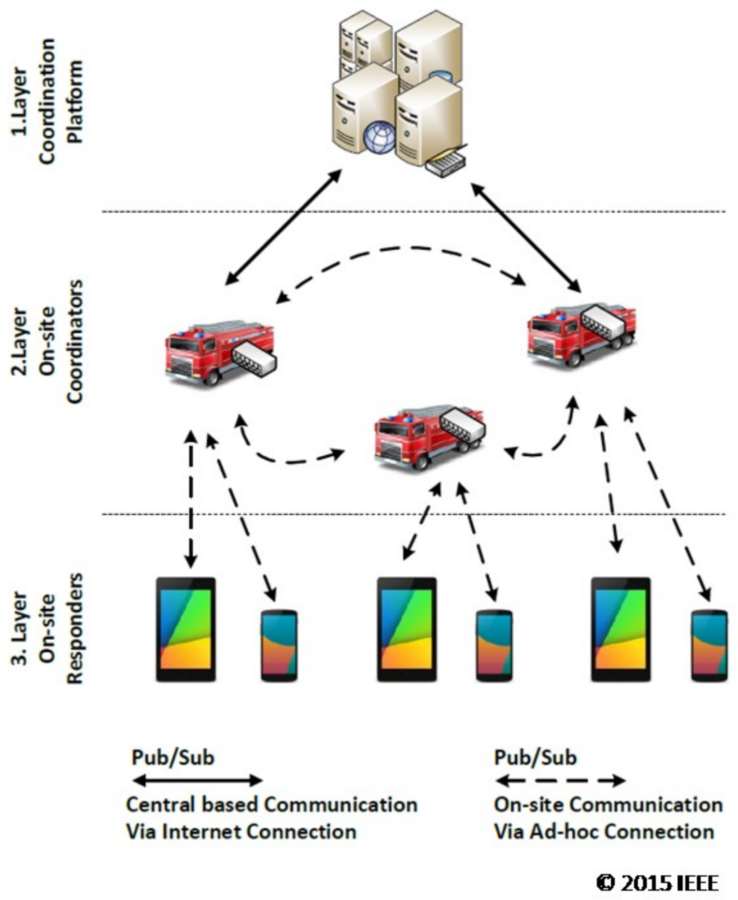
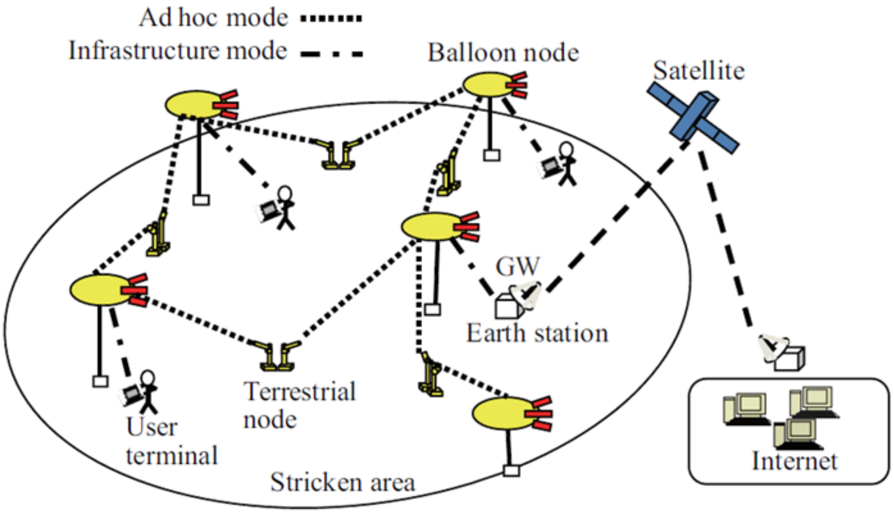


Figure 3.2: NICER overall architecture (Nguyen *et al.*, 2015)

In (Suzuki *et al.*, 2006), the authors propose **SKYMESH**, a wireless mesh network for large-scale disasters. In SKYMESH, the network is built using wireless routers located 50-100 meters high over the ground (see Figure 3.3). To bring and maintain the routers to this altitude, they propose to use balloons. The main contribution of the proposed solution is the reduction of the interference between the mesh routers. As a result, the WMN can be used to cover large areas. However, in contrast to NICER and SPIDER, SKYMESH does not provide a communication system to support the responders on-site. That means the total traffic has to be routed over the WMN to a mesh gateway. The same applies to communication from the outside to the helpers and people in the disaster area. This data traffic must also be routed via the gateway. This reduces the capacity of the mesh. Another issue of the proposed solution in SKYMESH is the security aspect. Access to the network is protected by a password alone. No mechanism has been proposed to restrict access to the network for a given user group (e.g., the access to specific applications cannot be restricted for a user group like “firefighter”). The prioritisation of the communication in SKYMESH is also not addressed.



© 2012 IEEE

Figure 3.3: An overview of SKYMESH (Okada *et al.*, 2012)

3.1.2 Other ECN architectures

In addition to mesh networks, other network architectures have been developed for disaster response. These network architectures often use technologies such as Terrestrial Trunked Radio (TETRA), mobile network, or satellite communication.

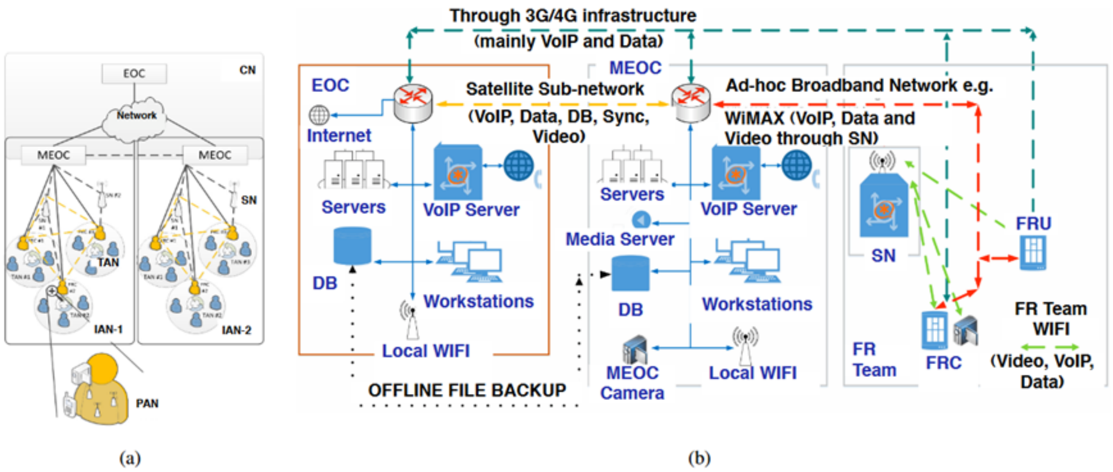
One of these architectures is the solution proposed by the EU (European Union) -project WISECOM (Wireless Infrastructure over Satellite for Emergency Communications)

(Berioli *et al.*, 2007). WISECOM aims to design and test a reference telecommunication system architecture for disaster sites. To build the network, the project remains on satellite communication. Figure 3.4 shows the proposed framework. It consists of two main parts: the Disaster-Safe Segment and the On-Disaster-Site Segment. Both segments are connected through a Transport Domain, which can be built using different wireless technologies (e.g., satellite). The On-Disaster-Site Segment is built by user end devices (e.g., smartphones, or laptops), local access networks (e.g., WiMax, WiFi, or 3G), and a WISECOM client, which acts as a bridge between different access networks and the transport domain. The Disaster-Safe Segment consists of a WISECOM Server necessary to control the access to the transport domain, a public networks domain (e.g. internet) and the organisation networks domain. One major contribution of the WISECOM project is the differentiation between network access technology and network transport technology. This enables the use of a common technology such as WLAN for network access and thus guarantees access to most end devices. In the WISECOM architecture, access to the public network or other network services is possible through the WISECOM server (Fazli *et al.*, 2008). The proposed framework is modular to integrate a technology update easily. The major limitation of WISECOM is that the proposed architecture does not incorporate a service platform to support the rescue teams on the disaster site. In addition, satellite is used for the transport domain. This technology has a high latency and represents the bottleneck of the architecture.

Figure has been removed due to Copyright restrictions.

Figure 3.4: WISECOM functional architecture (Berioli *et al.*, 2007)

E-SPONDER is another EU-funded project focusing on disaster scenarios (Campana *et al.*, 2014). E-SPONDER aims to offer a scalable and adaptive telecommunication architecture to support the rescue response. Figure 3.5 a) shows the proposed network architecture, which consists of three main segments: the first segment is built by First Responders (FR) like police officers and firefighters on the disaster field. They are equipped with FRUs (First Responder Units), consisting of a smartphone, a local position sensor, and environmental and biomedical sensors. In addition, the architecture describes a Special Node (SN), which other FRU uses to connect the Mobile Emergency Operations Center (MEOC). The second segment consists of several MEOCs. A MEOC is a vehicle with communications equipment, computers and display systems. It hosts, e.g., the servers for the applications required by the rescue teams (see Figure 3.5 b)). It is connected to the Emergency Operations Center (EOC) via the public 3G/4G network if available, or via satellite if the public network is not available. The last segment is the EOC. It is responsible for managing and controlling the complete rescue operations (Campana *et al.*, 2014). In contrast to WISECOM, this network architecture can provide the adequate QoS necessary to run real-time applications. However, a high budget is required to build the network because every team on the disaster field needs a fully equipped vehicle (MEOC).

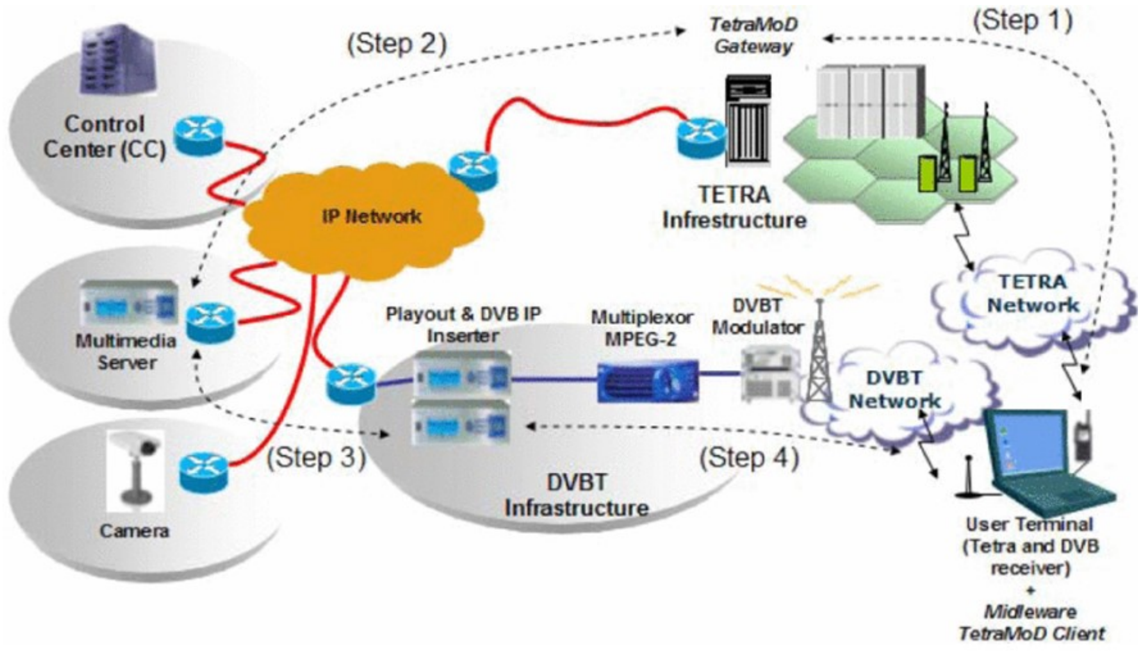


© 2014 IEEE

Figure 3.5: a) E-SPONDER architectural network b) Complete communication network and information system (Campana *et al.*, 2014)

The authors in (Belda *et al.*, 2008) propose a Multimedia on Demand system (**TetraMoD**) to support both Video on Demand Service and File Transfer Service in disaster scenarios. The proposed solution is based on the integration of TETRA and DVB-T networks. Figure 3.6 shows the proposed architecture. The TETRA network is used for media presentation retrieval and transmission control. Due to its broadcasting capability, the

DVB-T network is used for the transmission of the desired media. For the clients to participate in the communication, they need a middleware software called a TetraMoD client in addition to a TETRA and a DVB receiver. A TetraMoD Gateway is used as an interface between TETRA and DVB-T networks. The TetraMoD gateway receives requests from the clients and forwards them to the content server, which delivers the specified content over DVB-T. The main advantage of TetraMoD is that the platform is designed to allow multiple users to receive the audio-visual information requested by one of them.



© 2008 IEEE

Figure 3.6: TetraMoD system architecture (Belda *et al.*, 2008)

3.1.3 Evaluation of existing ECN architectures

In this subsection, the network architectures and research projects presented in Subsections 3.1.1 and 3.1.2 are evaluated regarding the infrastructure and service requirements defined in Section 2.1. Table 3.1 summarises the results of the evaluation. According to these results, the objectives of this research work are clarified.

Infrastructure requirements

Rapid deployment: This requirement is fulfilled by all the projects examined. Because all network architectures were developed focusing on emergencies, the speed with which the network is set up plays a crucial role. One example is the installation of the hardware directly on the equipment of the fire brigades as proposed by SPIDER.

Easy deployment: All the solutions examined are user-friendly and can be set up by helpers without knowledge of telecommunications networks. The configuration of the devices takes place in advance, and the use of special hardware such as directional antennas was avoided.

Complete area coverage: Network coverage for large-scale disaster situations such as earthquakes is addressed by the NICER, SKYMESH, WISECOM, E-SPONDER and TetraMoD projects. For example, the NICER network uses LORA technology to enable communication between remote operational sites (network bridges). WISECOM and E-SPONDER rely on satellite communication to realise the transport domain. With SKYMESH, a WMN network is set up in the sky. This allows a longer distance between the mesh routers. TetraMoD is based on TETRA and DVB-T, two technologies with very high coverage. SPIDER alone relies on mobile communications, which is often damaged by major disaster events and is therefore unavailable.

Access for everyday devices: Except TetraMoD, all the architectures studied use one or more of the most common wireless technologies (WLAN, Bluetooth, cellular) to connect the client. These networks are therefore accessible to most devices.

Failure safety infrastructure: While the issue of resilience is not addressed in non-mesh-based solutions (WISECOM, E-SPONDER and TetraMoD), it is simply assumed in mesh-based solutions through the mesh structure and the use of a suitable routing protocol. It is not taken into account that the communication devices are battery-powered in the event of a disaster due to damage to the power grid. Since the problem of limited power supply is not addressed by any of the architectures examined, they are all considered non-failsafe.

QoS support: To ensure complete coverage of the disaster area, NICER, WISECOM, E-SPONDER and TetraMoD rely on high coverage technologies such as satellite, LORA, TETRA, or DVB-T. However, this high coverage is achieved through compromises in delay (satellite), throughput (LORA, TETRA) or transmission direction (DVB-T). In NICER and E-SPONDER, the proposed architectures give the possibility to realise time-critical applications directly on-site, but the limited bandwidth of LORA and the time delay of satellite communication remain a problem for multi-site communication. SKYMESH alone pursues the goal of forming a broadband network over the entire disaster area. The authors propose a WMN for this purpose. However, the interference problem from routers operating on the same channel is not addressed.

Practicability: The network solutions proposed in SPIDER, NICER, and SKYMESH can be built under a limited budget because they are based on technologies such as WLAN or LORA. The solutions in E-SPONDER are costly because it requires a vehicle with special network equipment, and in TetraMoD, it requires the development of new clients with both a TETRA and a DVB-T interface.

Service requirements

Situational adaptability of service provision: This requirement is fulfilled by TetraMoD only. In TetraMoD, the clients can communicate directly with the services located outside the disaster area thanks to the long range of TETRA and DVB-T technologies. The structure of the teams is thus flexible and can be adapted to any situation. In SPIDER, NICER, WISECOM, and E-SPONDER, the number of teams depends on available vehicles with running communication equipment. This number cannot be adjusted to the current disaster situation. In SKYMESH, the clients can communicate directly with the services outside the network, but the realisation of these services is not addressed.

Failure safety service: The investigated architectures do not address the failure of services. However, it is assumed in the evaluation that services running outside the disaster area are fail-safe. This requirement is therefore assessed as fulfilled for SKYMESH, WISECOM and TetraMoD.

Simple service provisioning: Except SKYMESH, where the realisation of services was not addressed, the users in the examined projects do not need to have knowledge in the field of telecommunication networks to use the services (e.g., automatic IP address reference via DHCP, DNS ...). This requirement is therefore assessed as fulfilled in these projects (see Table 3.1).

Introduction of new services: This requirement is fulfilled by none of the solutions examined. The integration of new services can only be realised by updating the equipment. This must be carefully planned and should function for several years.

Practicability: The acquisition of new equipment when integrating new services and the disproportionate dimensioning of resources for the services provided lead to high acquisition and operating costs.

Table 3.1: Evaluation of existing ECN architectures

Requirements		**ECN architecture**					
		SPIDER	**NICER**	**SKYMESH**	**WISECOM**	**E-SPONDER**	**TetraMoD**
Infrastructure	Rapid deployment	+	+	+	+	+	+
	Easy deployment	+	+	+	+	+	+
	Complete area coverage	-	+	+	+	+	+
	Access for everyday devices	+	+	+	+	+	-
	Failure safety infrastructure	o	o	o	n/a	n/a	n/a
	QoS support	-	-	o	-	-	-
	Practicability	+	+	+	-	-	-
Service	Situational adaptability of service provision	-	-	n/a	-	-	+
	Failure safety service	-	-	+	+	-	+
	Simple service provisioning	+	+	+	+	+	+
	Introduction of new services	-	-	-	-	-	-
	Practicability	-	-	-	-	-	-

Assessment notation: + satisfied, o partially satisfied, - not satisfied, n/a not addressed

In summary, mesh-based solutions show better results in terms of infrastructure requirements compared to other network architectures. SKYMESH proposes setting up the WMN a few meters above the surface to avoid shielding by buildings and other obstacles. This allows a greater distance between the mesh routers. A similar concept is followed in this work. The routers are placed at height on tripods, balloons, or the roof of buildings. In addition, the unmet requirements (Failure safety and QoS support) are addressed as follows:

- Failure safety infrastructure: This work aims to increase the failure safety of the network on the one hand by optimising the energy consumption (see Chapter 7) and, on the other hand, by investigating a suitable routing protocol for use in the event of a disaster (see Chapter 6).
- QoS support: This work aims to realise QoS support for as many services as possible through a multi-radio multi-channel WMN. In this way, mesh routers within the interference range of each other should be transmitted simultaneously (see Chapter 5).

Regarding the service requirements, the previous research works perform poorly. The proposed architectures are inflexible and, except TetraMoD, cannot be adapted to the situation in the disaster field. Because the services provided run on proprietary hardware, integrating new services is costly and often requires a complete update of the network equipment. The resources are disproportionately dimensioned to ensure that the necessary services function flawlessly, even in large-scale operations. As a result, the acquisition and operating costs are very high. This thesis aims to meet these requirements through integration with NFV (see Chapter 4).

3.2 Related Work on Current Channel Assignment Strategies in WMN

There are several ways to classify channel assignment (CA) strategies. In (Skalli *et al.*, 2007), the authors differentiate between static or fixed, dynamic and hybrid CA strategies. A constant channel is set to each interface by static or fixed CA strategies. By dynamic CA strategies, the channel allocation change (e.g. to adapt to the measured interferences or the changes in the network traffic). The hybrid CA is a combination of the two other strategies. This means that a static channel is assigned for some interfaces, and for others, the channel allocation is optimised over time. In (Ko *et al.*, 2007), the CA strategies are classified in centralised and distributed mechanisms. Centralised strategies require the presence of a central element that knows the entire network topology. This element performs the channel allocation and distributes this information over the whole network. Each node allocates channels to its interfaces using the locally available information in decentralised CA strategies. In this thesis, a distinction is made between link-based and cluster-based CA strategies, as these characteristics have the greatest influence on the CA strategy requirements defined in Section 3.3, as shown in the following subsections.

3.2.1 Link-based channel assignment strategies

In link-based CA strategies (e.g. (Ko *et al.*, 2007) and (Kyasanur and Vaidya, 2006)), each interface is set to a specific channel for communication with each neighbour. This strategy has the benefit of maximising the network throughput and has three significant drawbacks. First, it requires many radio interfaces (one interface for each neighbour router) to preserve the network topology (topology preservation). For example, inside a WMN where each router communicates with four neighbour routers, four interfaces are required to maintain the network topology. If each router does not have four interfaces, additional calculations and optimisations are required to maintain network connectivity and avoid network segmentation. These additional optimisations represent the second drawback of link-based CA strategies. The last drawback is the important number of non-overlapping channels required to build the network. Looking at the network topology in Figure 3.7, where each router has a communication link with its four neighbours, at least 16 non-overlapping channels are required to build the network. This value is determined by assuming that the interference range of a wireless router can be considered to be two times its transmission range (Raniwala and Chiueh, 2005). The routers (black dots) in Figure 3.7 are less than 2 hops away from each other. They need 4 non-overlapping channels each for their interfaces ($4\,routers\ \times 4\ interfaces = 16\ channels$)

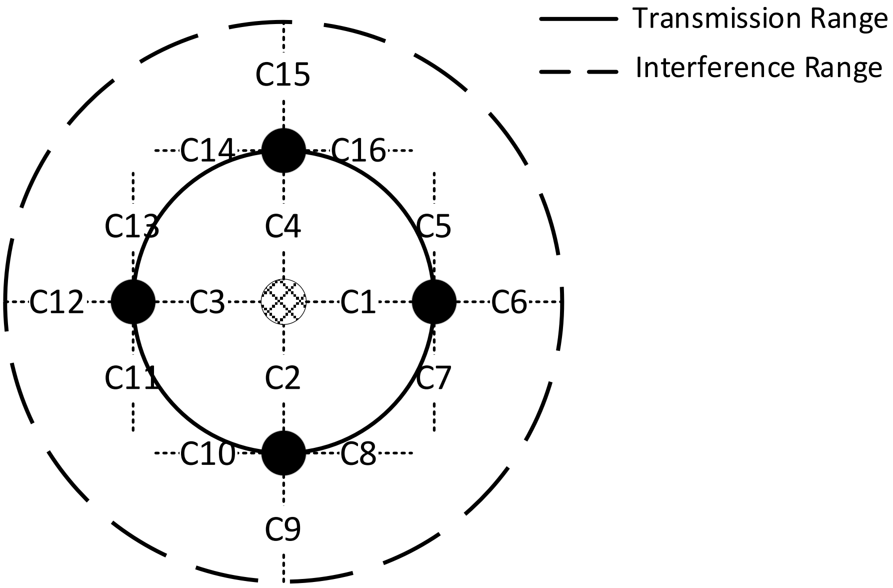


Figure 3.7: Example of link-based channel assignment

3.2.2 Cluster-based channel assignment strategies

The number of wireless routers communicating on the same wireless link or channel in the cluster-based CA strategies is not limited to two. Many routers inside a cluster are using the same channel. The advantage of this strategy is that only few interfaces are required, the network topology is preserved, and the number of non-overlapping channels required is lower than with link-based CA strategies. Few research works have addressed the CA problem in multi-radio WMN using the cluster-based solution. In (Naveed *et al.*, 2007), the authors propose the Cluster-based Multipath Topology control and Channel assignment scheme (CoMTaC). The CA in CoMTaC is performed in three steps. The network is parsed in clusters using a spanner algorithm in the first step. This process assumes that the traffic in the network is directed to the gateways and can lead to the loss of existing links. In the second step, interfaces are assigned to the neighbours. The third step is the channel assignment step. In this step, the default interface of each cluster member is assigned to a common default channel. After that, the second interface of each border router is set as a common channel to the interface in the neighbour cluster. This channel is different from the channels used inside the cluster. Finally, the CA for the other interfaces of the cluster members is performed (see Figure 3.8). This CA strategy can lead to the topology partition because a border router can provide a connection to more neighbour clusters than the number of interfaces that it has. This problem is addressed by the authors in (Athota and Negi, 2015), who propose the cluster-based channel assignment (CBCA). To avoid the partition of the network, CBCA starts the CA process with the border routers. Additionally, the connection between border routers in CBCA is not limited to P2P. The same channel can be used to communicate with more than one neighbour cluster.

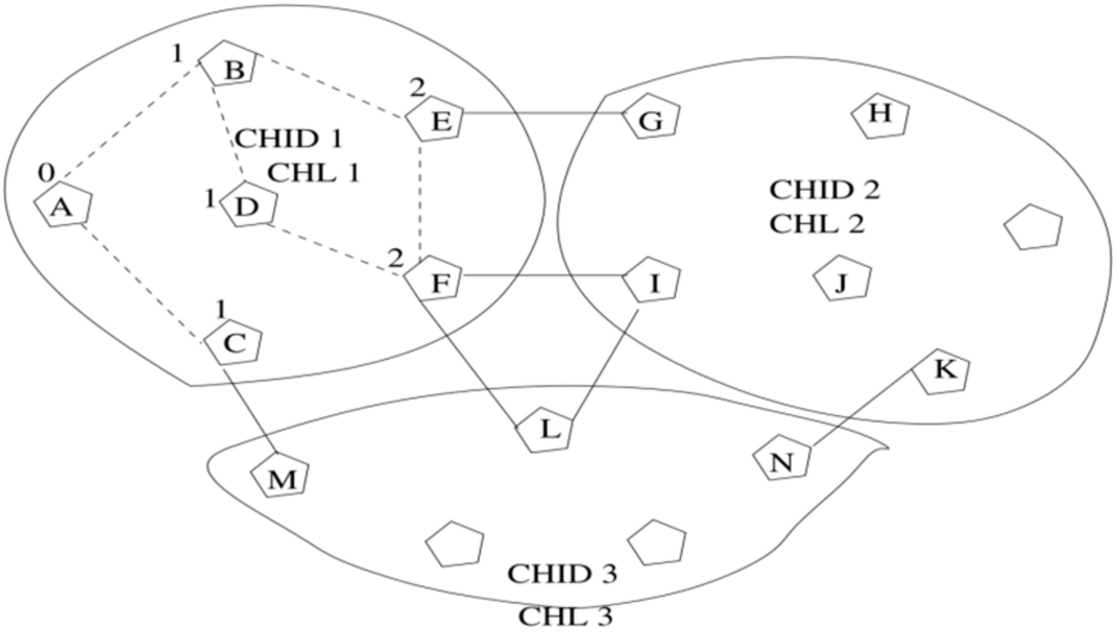


Figure 3.8: Example of inter-cluster connectivity using border nodes in **CoMTaC** (Naveed *et al.*, 2007)

The main objective of the cluster-based channel assignment strategy proposed by (Makram and Gunes, 2008) is to avoid information over the channel usage being distributed over the whole network. To achieve this goal, a head of cluster heads is introduced. It defines which channels can be used inside which cluster and distribute this information to other cluster heads. The cluster heads can then process the channel allocation to the cluster members.

3.2.3 Evaluation of existing channel assignment strategies

Table 3.2 resumes the evaluation results according to the requirements for the CA strategy.

Link-based (Lb) CA strategies, as proposed by the authors in (Ko *et al.*, 2007) and (Kyasanur and Vaidya, 2006), keep the network topology only if the number of wireless interfaces at each router is equal to or higher than the number of neighbour routers. In this scenario, the number of required non-overlapping channels is higher than the number available in IEEE802.11. This scenario is referenced in Table 3.2 as Lb (high). If the number of available interfaces is reduced to comply with the number of channels existing in the IEEE802.11 standards, the topology can no longer be preserved. This leads to high complexity of the channel assignment. This second scenario is referenced in Table 3.2 as Lb (low).

In CoMTaC (Naveed *et al.*, 2007), the proposed channel assignment strategy preserves the intra-cluster topology by using a default channel. A peer link with the neighbour cluster is assumed for inter-cluster communication. Because a border router can have lass interfaces than the number of neighbour cluster, a network partition can occur. CoMTaC not really deals with interferences or uses any interference model. The cluster size is not specified. The authors recommend the formation of 2-hops clusters, as they assume the interference range to be two times the transmission range. How the data rate behaves in a two hops WMN is investigated by field measurements in Chapter 5.

CBCA (Athota and Negi, 2015) is a modification of CoMTaC, which aims to solve the problem of network partition. This CA strategy therefore fulfils the topology preserve requirement. Both strategies have the same characteristics concerning interference compliance, scalability, and complexity.

In CCA (Makram and Gunes, 2008), the network is parsed in clusters using a clustering algorithm. The node with the highest number of links is selected to become the cluster head in each cluster. In a second step, a head of cluster heads is selected. This node distributes the available channels to the different clusters that it manages. The distribution of the available channels is performed depending on each cluster's size (number of members). The authors do not specify the used clustering algorithm or the size of the clusters. The proposed CA strategy maintains a distance of two clusters between clusters using the same channel set (list of channels assigned to a specific cluster by the head of cluster heads).

It is important to mention that none of the above-described CA strategies has addressed the problems of cluster sizing, network coverage, or wireless standard usage. They also assume that interferences are reduced by using multi-channels but do not provide evidence that the strategy they propose is the best. These questions are explored in Chapter 5.

Table 3.2: Evaluation of existing CA strategies

Requirements	**CA strategy**				
	Lb(high)	**Lb(low)**	**CoMTaC**	**CBCA**	**CCA**
Topology preserve	+	-	o	+	o
Interference compliance	n/a	n/a	n/a	n/a	n/a
Scalability and complexity	+	-	+	+	+
Throughput	+	+	n/a	n/a	n/a
Wireless standard compliance	-	+	+	+	+

Assessment notation: + satisfied, o partially satisfied, - not satisfied, n/a not addressed

3.3 Related Work on Routing Protocols in WMN

This section examines the performance of the most widely used routing protocols in a WMN for disasters. First, these protocols and their functions are briefly explained. Then they are evaluated based on the routing protocol requirements defined in Section 2.2.

3.3.1 Existing routing protocols for WMN

In recent years, numerous protocols have been developed to solve the routing problem in WMN. The following protocols are the most frequently mentioned in the literature:

Hybrid Wireless Mesh Protocol (HWMP): HWMP was standardised in IEEE802.11s (IEEE, 2016). It is a layer 2 routing protocol. That means it uses MAC instead of IP-addressing for packet delivery. It is also a hybrid protocol because it allows each mesh participant to use proactive, reactive, or a combination of both mechanisms for path discovery. Each node willing to communicate with another one inside the mesh network during the reactive process starts a path request (*PREQ*). Neighbouring routers broadcast this request up to the destination. The routers between the source and the destination router, which receive the *PREQ,* learn the shortest path to the request's initiator. Then, the destination's reply can be sent as a unicast path reply (*PREP*) to the initiator of the communication. If a mesh participant is configured to work proactively, it periodically broadcasts a root announcement (*RANN*) or a path request (*PREQ*). Each router that receives this message ignores it if the metric it contains is worse than the current metric to reach the initiator. If the metric it contains is better than the current metric or if the sequence number is newer than the current sequence number, it selects the neighbouring router that sent this message as the next node to reach the root node and broadcasts the message. To determine the best path quality between two routers, HWMP uses the airtime link metric. The airtime link metric is calculated as follows:

$$COST = \frac{1}{(1 - e_p)}\left(O + \frac{B_t}{R}\right) \tag{3.1}$$

It is given by the Expected Transmission Count (ETX) metric (see equation (3.2)), which is corrected through the multiplication with another factor. The new factor takes the cost (delay) of the channel access O (channel access overhead, which includes frame headers, training sequences, access protocol frames, etc. (IEEE, 2016)) as well as the test frame size B_t and the data rate R used by the router to transmit the test frame into consideration.

Babel: Babel is a proactive layer 3 routing protocol that was defined in RFC6126 (Chroboczek, 2011). Babel messages are defined using the Type-Length-Value (TLV) model and are transported inside UDP packets. Multiple Babel messages can be combined and sent inside one UDP packet to reduce the protocol overhead. Each Babel router periodically broadcasts a Hello message. This message is received only by routers, which are located in the transmitter's range and will not be forwarded. Hello messages are used for the neighbour discovery and the link quality estimation. The metric used in Babel is the ETX metric:

$$COST = \frac{1}{(1-e_p)} \tag{3.2}$$

e_p is the packet error probability. It is calculated by the router, which gets the Hello message based on its information. The calculated packet error probability is transmitted to the sender using an I-Heard-You (*IHU)* message. Additional to the *Hello* and *IHU* messages, each router periodically broadcasts *Update* messages. For each known subnetwork and its metric, one *Update* message is generated. Each neighbouring router, which receives this message updates its routing table if the update is feasible and accordingly broadcasts the message. If a router wants to communicate with a given prefix and the information in the routing table is not up-to-date enough, it can use a *Route* or a *Seqno Request* to request and update this information.

Better Approach to Mobile Ad-hoc Networking advanced (B.A.T.M.A.N. advanced): B.A.T.M.A.N. advanced is a layer 2 proactive routing protocol (Open-Mesh, 2022b). Each B.A.T.M.A.N. advanced node periodically broadcasts an originator message (*OGM*) with an incrementing sequence number. Each mesh router that receives an *OGM* updates its path table. Then it broadcasts the message only if it was received from the neighbouring router, which is currently selected as the next hop to reach the original initiator of the *OGM*. To select the best next node to reach a given originator, each OGM contains a Transmission Quality metric field (TQ). Each router updates its value before it forwards the OGM. The new TQ value is calculated based on the normalised link-local transmission quality multiplied by a link asymmetry penalty (see equation 3.3).

$$COST = TQ = \frac{RQ}{EQ} \qquad (3.3)$$

RQ is the fraction of OGMs received during a given time frame (window size) from the neighbour router, and EQ is the fraction of the own OGMs rebroadcasted by the given neighbour router. The developers of B.A.T.M.A.N. advanced IV assume that *OGMs* propagate faster over a non-overloaded path or with less packet loss. B.A.T.M.A.N. advanced attaches an additional header from up to 32 Byte on all frames working over the network to perform its forward operations.

In B.A.T.M.A.N. advanced V(Open-Mesh, 2022a), the developers try to decouple maintenance operations like neighbour discovery or link metric calculation from the spread of information necessary for the routing process. *OGMs* are no longer used to determine the path quality. The metric used in B.A.T.M.A.N. advanced V is based on the measured throughput. *OGMs* are used to transmit routing information over the mesh. This information is contained inside a list of one or more fields attached to the *OGM* message. These fields are structured using the Type Version Length Value (TVLV) model.

Zone Routing Protocol (ZRP): ZRP (Haas and Pearlman, 1998) is a hybrid routing protocol. This means that it combines both proactive and reactive properties. ZRP defines a perimeter (zone) around each node in the network. Within this zone, routes are determined proactively. This zone encloses nodes with a distance less than a hop count *k* from the source. Routes are determined reactively for nodes outside this zone by the source node sending a route request to its edge node. Since ZRP does not specify either the proactive intra-zone routing protocol (IARP) or the reactive inter-zone routing protocol (IERP), performance analysis is difficult to realise. The hybrid nature of ZRP allows the protocol to be used in large networks.

Dynamic Source Routing (DSR): DSR is a reactive Mobile Ad hoc Network (MANET) routing protocol. This means that the route between the source and the destination is only generated when required. It was specified and published by the IETF in RFC 4728

(Johnson *et al.*, 2001). DSR belongs to the source routing protocols. This means that the data packets to be transmitted receive a complete route description with respect to the destination node at the sender node. This description contains the IP address of all nodes to be passed through, which leads to an enlargement of the packet header. DSR is difficult to use in combination with IPv6 (128-bit addresses) for large networks because the overhead becomes too large (list of routers over which the packet must be routed). Due to the "on-demand" path determination in DSR, the protocol can be classified as energy-efficient in no overloaded networks. In addition, the route request in the route discovery mechanism enables the learning of different routes to a destination. This has two advantages. On the one hand, it enables the implementation of load balancing at the routing protocol level. This means that successive packets can be sent via different routes to better distribute the energy consumption over the network and thus extend the network lifetime. This advantage has led to numerous energy- and load-aware protocols based on DSR (Stojmenovic and Xu Lin, no date; Xu Li *et al.*, no date; Garcia *et al.*, 2003; Tamilarasi *et al.*, 2008; Talooki *et al.*, 2010). On the other hand, DSR can increase resilience in the emergency network by sending packets over two different paths simultaneously (e.g. packets with a high priority, as in real-time video support for a surgeon in the disaster area). The Link Quality Source Routing (LQSR) (Draves *et al.*, 2004) protocol and the SrcRR protocol (Aguayo *et al.*, 2005) are two extensions of DSR for the WMN architecture. Both protocols use the ETX metric. This metric takes into account the errors that occur during transmission in wireless networks to determine the communication path.

Ad hoc On-Demand Distance Vector (AODV): AODV (Perkins *et al.*, 2003) is a reactive routing protocol analogous to DSR. However, the sender of the packet does not add a complete route description for the destination. Instead, each node decides which node is best suited to reach the destination after the packet reception. Besides its reactive nature, additional mechanisms are described in the literature (Gupta and Kumar, 2000; Jin-Man Kim and Jong-Wook Jang, 2006) to save energy when using AODV. Although AODV in its original version does not allow load balancing, several extensions to the protocol have been proposed, such as the Ad hoc On-demand Multipath Distance Vector (AOMDV) (Marina and Das, no date), which allows the simultaneous determination of multiple paths between two nodes. AODV also supports multicast.

Destination-Sequenced Distance Vector (DSDV): DSDV is a proactive protocol (Perkins and Bhagwat, 1994). This means that each node permanently determines its route to all possible destinations in the network. In this way, the time delay when establishing new connections can be reduced. DSDV is an older protocol and is no longer used today. Numerous studies in recent years have shown the poor performance of DSDV compared to more up-to-date protocols such as AODV or Babel (Baraković and Baraković, 2010; Morshed *et al.*, 2010).

Optimized Link State Routing (OLSR): OLSR is a proactive link-state routing protocol for a MANET. OLSR was standardised in RFC 3626 (Clausen and Jacquet, 2003). In 2014, a new version of this protocol was published that adds a metric to the protocol to take link quality into account. OLSR is often used in WMNs (e.g. Freifunk (Freifunk, 2022)). Numerous mechanisms are described in the literature to save energy in networks when using OLSR (Clausen and Jacquet, 2003; Kunz, 2008). Security mechanisms are also mentioned in (Selvi, 2014). With OLSR, each node has knowledge of the complete topology and can therefore calculate the most effective route to the destination using

Dijkstra's algorithm. For this, the node requires additional memory and computing capacity.

3.3.2 Evaluation of existing routing protocols

This subsection evaluates the routing protocols presented in subsection 3.3.1 based on the requirements in disaster scenarios (see Section 2.2). Table 3.3 summarises the results of the evaluation.

Decentralised routing: This requirement is fulfilled by the routing protocols DSR, AODV, HWMP, Babel, OLSR and BATMAN. The routing protocol ZRP can also be classified as decentralised because each router's proactive area is defined independently of the others. This means that there is no central element.

Dynamic routing: The following properties of the routing protocol influence its ability to detect changes in the network as quickly as possible:

- Link state and distance vector routing: Concerning the ability of the routing protocol to provide a quick response to dynamic changes inside the network, link state protocols seem to perform better than distance vector protocols.
- Proactive, reactive, and hybrid routing: Reactive routing protocols have a small delay at the beginning of each new communication. They, therefore, perform worse than proactive routing protocols concerning this scenario. However, when it comes to mesh router failure, reactive protocols often implement a mechanism such as "error message" to detect the failure as quickly as possible. It is therefore

difficult to determine which feature is most important for achieving this requirement.

In addition to these properties, the ability of a routing protocol to react to changes in the network depends on the metrics used. Because of this, a comparison of routing protocols is not feasible by a literature search alone (see Table 3.3). In chapter 6, this comparison is extended by simulations.

Number of end devices: The number of end devices connected when using a layer 2 routing scheme is limited. This is because the overhead of the routing protocol increases with the number of end devices. In comparison, the performance of a layer 3 routing protocol is independent of the number of connected end devices. The end devices connected via a mesh router belong to the same subnet and can be addressed. Therefore, this requirement is rated as fulfilled for all routing protocols except for the HWMP and BATMAN protocols.

Path computation: The following properties influence the difficulty of path computation of the routing protocol:

- Link state and distance vector routing: Nodes running a link-state routing protocol (e.g., OLSR) must perform a path calculation algorithm after receiving the network topology information. This calculation process requires additional computing resources, which depend on the size of the network.
- Source routing: Writing and reading the additional header in source routing comes with an additional computational cost (e.g., DSR).

Routing overhead: Clustering the WMN into multiple routing domains is optimal to reduce the number of packets generated during the routing process. It is important to note that the size of such clusters must be as large as possible to avoid a high number of clusters. This can lead to a problem of scalability of the inter-cluster routing protocol. In addition to the clustering of the WMN, the following properties also play a role in protocol overhead:

- Layer 2 and 3 routing: The routing protocol overhead when using a layer 2 routing protocol is higher than when using a layer 3 protocol. The reason for this is the additional ARP messages generated to link IP and MAC addresses. These messages are forwarded across the entire network. Thus, the overhead with HWMP and BATMAN is higher than with other protocols.
- Link state and distance vector routing: Inside a large network, if the interval T between two updates in a link state and a distance vector routing protocol is assumed to be the same, the overhead generated by the link state protocol is higher because the link states are transmitted over the whole network while the routing table used by distance vector protocol is just transmitted to the direct neighbour nodes.
- Proactive, reactive and hybrid routing: The reactive routing scheme generates a lower protocol overhead than the proactive one inside a no overloaded network. When the network load increases, all tree schemes seem to generate a similar overhead.
- Source routing: Because an additional header is added to each data packet, the protocol overhead of a source routing protocol is higher than no source-based protocols.

License-free: This requirement is fulfilled by all the routing protocols evaluated.

VNF live migration support: Using a layer 2 routing scheme allows VNF to be migrated while keeping the same IP address when the host mesh router changes. When migrating a web server, for example, the server's IP address changes when a layer 3 routing protocol is used. The entry in the DNS must therefore be adjusted, as well as the entries in the end devices. With a layer 2 routing protocol, these changes are not necessary. Thus, only HWMP and BATMAN fulfil this requirement.

Service aware traffic routing: Source routing can be used to determine the communication path depending on the required service. Although the DSR routing protocol does not provide this function, it can be used as described by the authors in (Quinn *et al.*, 2018; Li *et al.*, 2019) to realise service-aware routing in WMN. The other protocols examined do not fulfil this requirement.

Table 3.3: Evaluation of existing routing protocols for WMN

Routing requirements	**WMN routing protocols**							
	DSR	**AODV**	**OLSR**	**DSDV**	**ZRP**	**HWMP**	**Babel**	**B.A.T.M.A.N. advanced**
Decentralised routing	+	+	+	+	+	+	+	+
Dynamic routing	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Number of end devices	+	+	+	+	+	-	+	-
Path computation	-	+	-	+	n/a	+	+	+
Routing overhead	-	o	+	-	+	o	-	-
License free	+	+	+	+	+	+	+	+
VNF live migration	-	-	-	-	-	+	-	+
Service aware traffic routing	o	-	-	-	-	-	-	-

Assessment notation: + satisfied, o partially satisfied, - not satisfied, n/a not addressed

According to the performed evaluation, the HWMP protocol is particularly promising. Compared to BATMAN, it has a higher adaptability, i.e., it reacts faster to node failures. Furthermore, the protocol can be adapted to no longer proactively determine the route to the gateways, but to the nodes that offer functionalities such as web servers after NFV integration. In Chapter 6, HWMP is compared to BATMAN and Babel, which also provide good results, for some scenarios in disaster situations.

3.4 Related Work on Energy-Efficient Placement of VNFs

This section examines the publications that have dealt with the energy-optimised placement of VNFs in telecommunication networks. After a brief description of the work carried out in these researches, the models described there are evaluated to see whether they fulfil the properties relevant in the WMN for disaster situations.

3.4.1 Existing works on the energy-efficient placement of VNFs

The following papers have dealt with the issue of energy-efficient placement of VNFs:

The work in (Soualah *et al.*, 2017) aims to solve the problem of energy-efficient placement and chaining of VNFs in data centres. The problem is formulated mathematically using a decision tree model to achieve this goal. The data center is represented as a graph consisting of nodes and a set of edges. A node is characterised by its capacity (e.g., computing power) and type (server, switch or physical network function). The edges are links with a fixed maximum capacity. A linear model is assumed for the power consumption of a node, which depends on its basic power consumption and its current CPU load. Finally, the Energy Efficient Tree search-based Chain placement Algorithm (EE-TCA) developed by the authors is applied to determine a possible optimal location for the VNFs. EE-TCA is inspired by Monte Carlo Tree Search (MCTS). The algorithm aims to minimise the number of servers and switches used. Energy-efficient Severs are privileged as possible hosts for the VNFs.

The authors in (Yang *et al.*, 2016) also address the problem of energy-efficient placement of VNFs in data centers. There, the optimisation problem is formulated as binary integer programming. The model assumes a fat-tree data centre topology in which the servers are connected via switches. When modelling the server's power consumption, a linear dependence on the CPU load is assumed. It is considered that the switches' power consumption depends on the number of active ports. The goal of the optimisation is to concentrate the traffic and the provision of VNFs on a minimum number of servers and switches. The authors propose the Merge-RD algorithm. The proposed algorithm uses a Relation Degree (RD) metric to quantify the intensity of interaction between VNFs. Thus, VNFs with a high RD value are placed on the same server or neighbouring servers.

The authors in (Xu *et al.*, 2018) address both the problem of energy-efficient placement of VNFs and the problem of routing between VNFs in wired telecommunication networks in general. The paper's focus is the realisation of Service Function Chain (SFC) (Halpern and Pignataro, 2015). Here, the problem is formulated as Integer Linear Programming (ILP). The objective function is to minimise the power consumption in the network. Constraints are parameters such as the limited server and link capacities and the order in which the data traffic must be processed by the VNFs that belong to an SFC. When modelling the power consumption, it is assumed that the servers are directly connected via links. A linear dependency is assumed for both the servers and the links with the current CPU load and the current bandwidth utilisation, respectively. Because the problem formulated in this way is NP-Hard, the authors use a Markov approximation to find a near-optimal solution.

In (Kaur *et al.*, 2019), the authors simultaneously address the energy-efficient placement of containers and load balancing in data centres. The optimisation problem is mathematically formulated as a Multi-Objective Optimisation Problem (MOOP). The first objective is to minimise power consumption. It is assumed that the power consumption of a server depends on its base power consumption and the power consumption of the containers running on it. The authors do not consider the power consumption resulting from the transmission of data in their model. The second objective is to distribute the load as evenly as possible across all servers to avoid overload cases. To achieve this, they try to minimise the sum of the standard deviation from the average server load. Constraints include the limited resources on the servers and the limited link capacity. To solve the MOOP, the authors proposed an online solution based on an incremental exploration of the solution space to map containers on the available servers.

Finally, in (Nemeth *et al.*, 2021), the authors investigate the problem of the allocation of VNFs in 5G networks. As a use case, the case of autonomously driving mobile robots in a harbour is considered. These robots have additional computing capacity that extends the cloud and edge computing infrastructure when providing services. Although the objective of the optimisation is to minimise the cost, the authors have considered the limited coverage of wireless technologies and the limited energy supply to the robots as constraints in the mathematical formulation of the optimisation problem. The authors propose a heuristic algorithm to solve the so formulated problem.

3.4.2 Evaluation of existing models for the energy-efficient placement of VNFs

This subsection evaluates the models proposed by the research works in subsection 3.4.1 based on the requirements in disaster scenarios (see Section 2.3). Table 3.4 summarises the results of the evaluation. These results can be explained as follows:

Distributed service requests: Only the work in (Soualah *et al.*, 2017) considers that a VNF can be responsible for handling requests coming from different locations within the network (different egress nodes). However, this fact is not considered when finding the optimal location for this VNF within the network. Only the traffic is forwarded to it, and no further instance is created if the network capacity allows it.

Dynamic service requests: The work in (Nemeth *et al.*, 2021) and in (Kaur *et al.*, 2019) considers the time dependency on the number of service requests that need to be handled by a VNF. There, the network is modelled as a dynamic system in which the traffic that must be handled by each VNF changes over time, and the optimisation must be performed repeatedly.

Limited computing resources: Although the resources (e.g., CPU and memory) on a mesh router are much more limited than on a data centre server, there is no difference in modelling. All the models studied take into account that these resources are limited when choosing the optimal location for the VNFs.

Dynamic network infrastructure: This property is considered by the model in (Nemeth *et al.*, 2021) alone, as the work deals with the energy-efficient placement of VNFs in a mobile environment that integrates mobile devices (robots).

Battery-powered routers: This requirement is not addressed in the previous works. The work in (Nemeth *et al.*, 2021) is an exception, but the model is limited to detecting the battery level and migrating the VNFs when the device they are running on has too little residual energy. Nothing is done to keep the devices alive when energy levels fall.

Shared communication medium: This requirement was not modelled in previous work.

Change in the link quality: Previous works have not modelled this property.

Table 3.4: Evaluation of previous works with the focus on the energy-efficient placement of VNFs

Model requirements	**Literature**				
	(Nemeth *et al.*, 2021)	(Xu *et al.*, 2018)	(Soualah *et al.*, 2017)	(Yang *et al.*, 2016)	(Kaur *et al.*, 2019)
Distributed service requests	-	-	o	-	-
Dynamic service requests	+	-	-	-	+
Limited computing resources	+	+	+	+	+
Dynamic network infrastructure	+	-	-	-	-
Battery-powered	o	-	-	-	-
Shared communication medium	-	-	-	-	-
Change in the link quality	-	-	-	-	-

Assessment notation: + satisfied, o partially satisfied, - not satisfied, n/a not addressed

In summary, according to the above evaluation, none of the earlier formulations of the optimisation problem applies to the specific scenario of a WMN in a disaster. This results from the unique properties of the network, such as the battery supply of the hardware, the shared wireless communication medium, the high dynamics of the WMN (e.g., link quality changes, router loss, network extension, changes in the distribution of service requests), or the distribution of service requests. These properties represent requirements for the model and have not been considered or have been considered very little in previous works. In Chapter 7, a model will be developed by mathematically formulating the optimisation problem, and different algorithms will be proposed to solve it.

4 Proposed NFV optimised WMN Architecture

This chapter proposes a network architecture that aims to improve the performance a disaster network by (i) replacing the dedicated hardware equipment (e.g., a vehicle with heavy proprietary communication middleboxes, servers, satellite and TETRA phones) with common wireless routers, (ii) introducing NFV to address service scalability, cost to build the network, and required time to integrate new services, (iii) optimising the energy consumption and resource usage to address the problem of the network sustainability. Section 4.1 introduces the general concept and highlights its benefits by comparing it with state of the art WMN deployment in a disaster scenario. Section 4.2 describes the architecture, focusing on the power consumption in the network. Section 4.3 summarises and clarifies the challenges addressed by this research work.

4.1 General Concept and Benefits of the Proposed Architecture

Figure 4.1 shows a state-of-the-art communication network as expected after a disaster according to the literature review in Section 3.1. It consists of four main segments: the user segment, the access segment, the core segment, and the disaster safe segment.

User segment: The user segment consists of user devices such as smartphones, laptops, sensors, or drones. These devices require services provided by the other network segments to communicate. In some cases, they can be directly connected and form an ad hoc network to increase the coverage of the ECN (e.g., see (Subik *et al.*, 2010)).

Access segment: According to (Subik *et al.*, 2010; Campana *et al.*, 2014; NICER, 2022), it can be assumed that each team deployed in the disaster area (e.g. fire brigade, police, or civil protection) is equipped with the necessary network infrastructure to enable on-site communication between members of the same team. This network infrastructure forms the access segment or organisation specific segment. The access segment consists of several access networks built with organisation-specific equipment in one or more operational locations. For providing services (e.g., location images, team member vital parameter monitoring, patient documents, or robot scattering) required to support the teams in the disaster field, each access network contains a central point with the necessary hardware equipment (e.g., access point, gateway, router, server). This equipment is often located in a vehicle if the team is mobile. The access networks are connected to the lead team outside the disaster area via an external network (e.g., internet, 3G/LTE/5G or satellite) or the core segment.

Core segment: The core network, if available, is built by wireless routers that are distributed in the affected area immediately after the disaster (Suzuki *et al.*, 2006). Its first task is to interconnect access networks to enable intra- and inter-organisational communication. Its second task is to extend the connection to external networks (e.g., internet, 3G/LTE/5G, or satellite). Therefore, the routers building the core network are equipped with additional interfaces and provide gateway functionalities.

Disaster safe segment: The fourth segment of the ECN is located outside the affected area (usually in the cloud or at the organisations' headquarters that lead the rescue response).

This segment consists of service provider network equipment (e.g., firewalls, load balancers, web and proxy servers) necessary to manage the operations remotely by providing the required communication services.

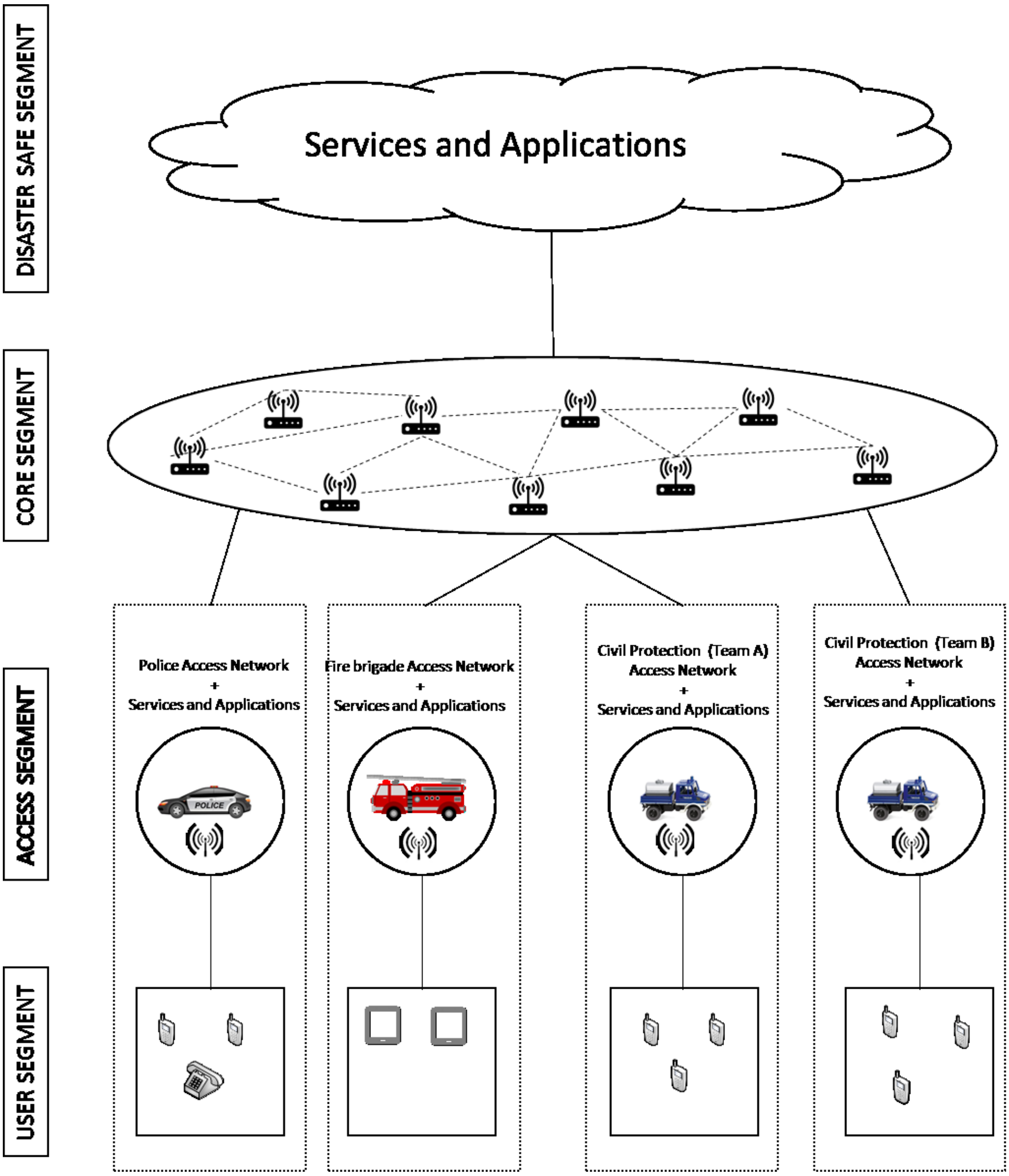

DISASTER SAFE SEGMENT
Services and Applications
CORE SEGMENT
ACCESS SEGMENT
Police Access Network
+
Services and Applications
POLICE
Fire brigade Access Network
+
Services and Applications
Civil Protection (Team A)
Access Network
+
Services and Applications
Civil Protection (Team B)
Access Network
+
Services and Applications
USER SEGMENT

Figure 4.1: Current network architecture in disaster scenario according to the literature review

This network architecture is highly resourcing inefficient and has the following bottlenecks:

1. In the described architecture, the cooperation between different organisations is limited to the information shared over the network. Hardware resources like servers computation cannot be shared. Each organisation has to plan and manage its communication equipment. As an example, the servers used by the police to inform people immediately after the disaster cannot be used many hours later by a humanitarian organisation to collect information about the wounded or used for storing information about blood donation.
2. Because each organisation uses dedicated hardware equipment for its teams, the costs necessary to build the network are high. In addition, the introduction of new network services requires an upgrade of the complete communication equipment. This is often impossible due to the limited budget of many organisations.
3. An organisation with four communication units can only deploy four teams during a disaster because they only have the equipment to support them. They cannot adapt their response to the specific case and create five teams for example.
4. When a team has finished with its work in one particular area and has to move to the next one, the team members have to move the hardware communication equipment they require for their work.
5. Energy efficiency is another issue in the described network architecture. To avoid limitations during their operations, each organisation tends to design its network by considering the worst-case. This leads to the overprovisioning of the provided applications and network services in most cases. As a result, more energy is used than required. Another example of energy inefficiency are duplicated network

functions such as DHCP servers or firewalls when different organisations operate in the same area.

These issues demonstrate the importance of an open network that all organisations can use. Figure 4.2 shows the architecture of the proposed solution. The network is built with commercial off-the-shelf (COTS) outdoor routers resulting in a lower cost. In contrast to the network architecture in Figure 4.1, the proposed solution only has three segments: the user segment, the core segment and the disaster safe segment. The main segment is now built by the core segment. Its function is no longer limited to the transport of packets between different networks and the extension of external networks. Now, it integrates the organisation specific access networks as well as the applications and network services, which were provided by the organisation specific network equipment so far. This is possible through the integration of NFV. The proposed architecture has the following advantages:

1. Physical resources like computational power are now shared between organisations. All organisation end devices are connected directly to the core network though access points. This increases the network connectivity by facilitating the communication between the devices of different organisations and reducing the number of access points in a defined area.
2. Another significant advantage of the proposed network architecture is that the cost necessary to build the network can dramatically be reduced because each organisation no longer must invest in its individual network equipment. Additionally, the network now offers the possibility of innovation through the rapid integration of new services.

3. The network services (e.g., VoIP or web services) needed by each organisation and their teams are scalable and can be adapted to any situation due to the sharing of hardware resources.
4. There is no need to migrate the network equipment when the team members progress and move to the following location. The necessary network services can migrate to follow their movements (VNFs live migration).
5. The last advantage of the proposed architecture is that it creates new opportunities to optimise the energy consumption and, therefore, the network lifetime.

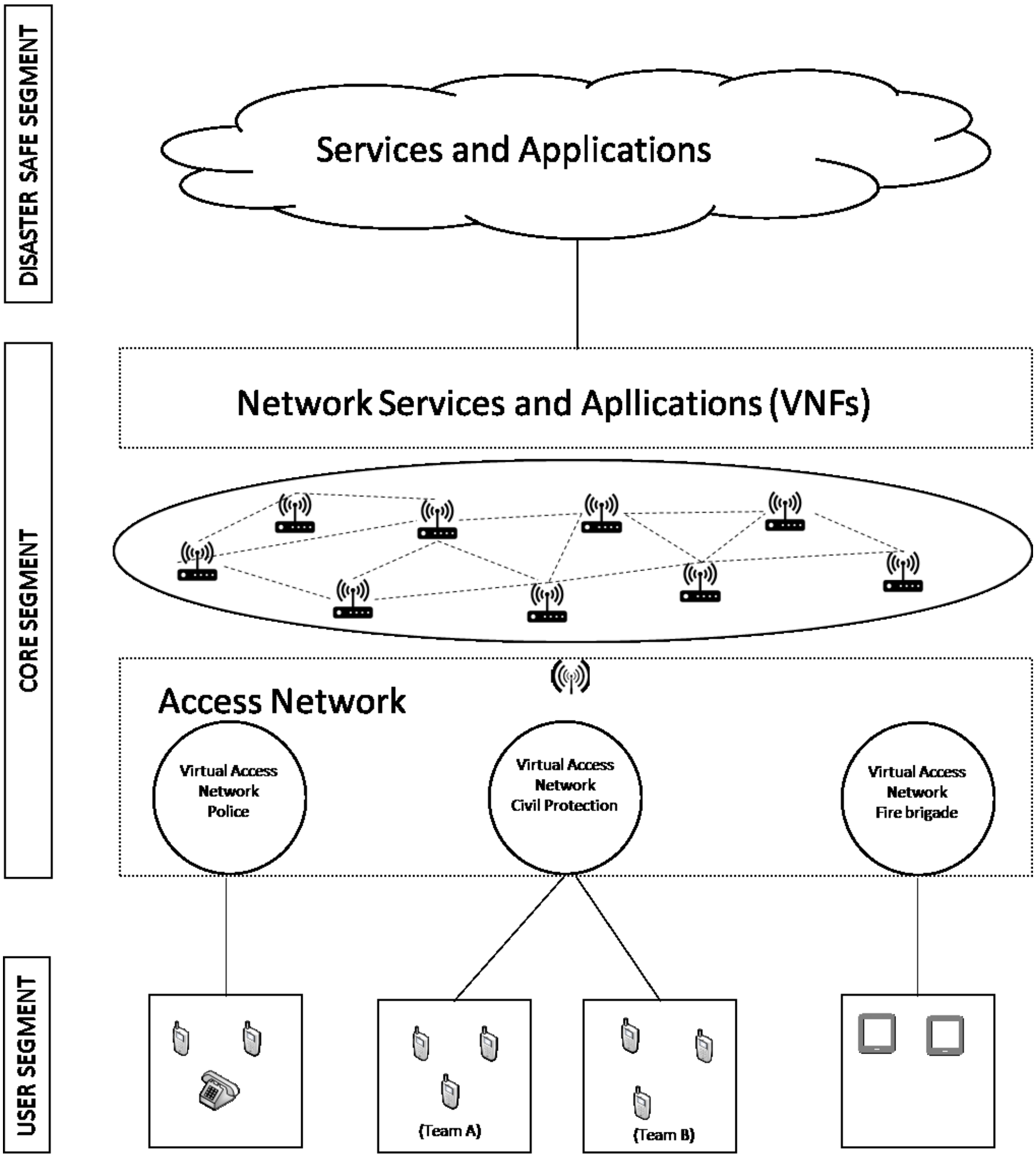

DISASTER SAFE SEGMENT
Services and Applications
CORE SEGMENT
Network Services and Apllications (VNFs)
Access Network
Virtual Access Network Police
Virtual Access Network Civil Protection
Virtual Access Network Fire brigade
USER SEGMENT
(Team A)
(Team B)

Figure 4.2: Proposed network architecture with integrated VNFs

4.2 Architecture Description

The following focuses on the core segment of the proposed network architecture as the main point of difference to the existing solutions. This core segment is shown in Figure 4.3. It consists of a WMN built with battery-powered WLAN routers. These mesh routers are distributed in the field by the helpers immediately after the disaster event. To avoid being shielded by buildings and other obstacles, they are placed a few metres above the surface. Tripods or balloons are used for this purpose. In cities, the routers can also be placed on the roof of tall buildings.

The power consumption of a mesh router is made up of three main components: a basic component, a forwarding component and a processing component (see Figure 4.3).

Basic component: The basic component or basic power consumption has a constant value. This consumption occurs when the mesh router goes into on-mode. It is hardware dependent.

Forwarding component: The forwarding component of power consumption results from the transmission of data packets. Each mesh router has several WLAN interfaces for communication with the neighbouring routers. These WLAN interfaces are called mesh interfaces and function on non-overlapping channels to reduce interference in the network. Mesh interfaces with the same radio channel within the transmission range of each other form a cluster. As an example, Figure 4.3 shows a WMN with two mesh interfaces per router, and 25 clusters. In addition to the mesh interfaces, each router is often equipped with one or more additional interfaces. These additional interfaces enable the connection of user terminals in the network and are called access interfaces. Access interfaces do not necessarily have to be realised with WLAN technology. However, it is recommended to use a widespread technology or a combination of several technologies to enable most end devices to connect. Depending on the application, technologies such as TETRA, LoRa, RFID, WLAN, or Bluetooth can be used. It is also recommended to implement separate virtual access networks for the different user groups to prevent security breaches and restrict access to certain services for selected user groups. An example is a separation between the access network for persons in distress and the access network for helpers. While the people in distress can access the network without authentication and send emergency calls, the members of an emergency organisation have to identify themselves first and can access more services after this process. The last type of interfaces that play a role in the forwarding component of power consumption are gateway interfaces. Gateway interfaces use a different technology (e.g., mobile communication) to connect the core segment to external networks where they still exist.

Processing component: The processing component of power consumption results from the processing of service requests by VNFs. The main innovation of the proposed architecture is the integration with NFV. This allows the implementation of applications and other network services as VNFs. These VNFs run as containers in the mesh routers.

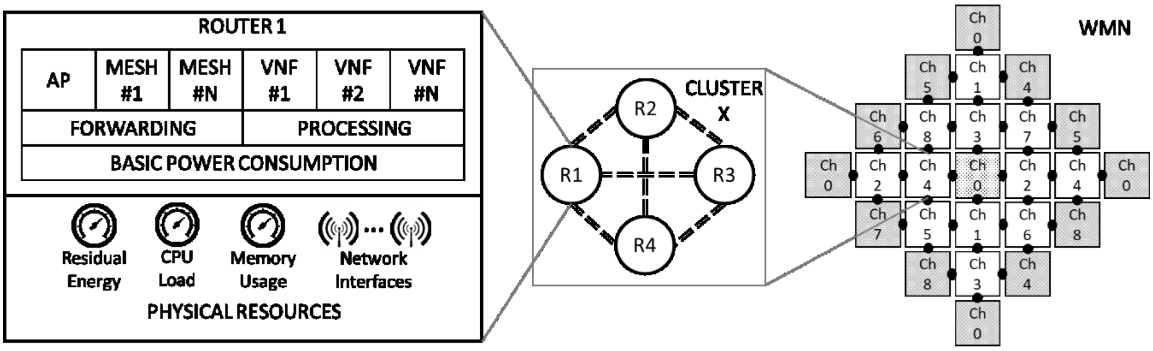


Figure 4.3: Core segment of the proposed network architecture

4.3 Summary and Architecture Challenges

The virtualisation and integration of network functions, which were part of the organisation specific network segment so far, results in significant challenges:

1. The first challenge results from the use of WMN as NFVI. Due to its unique architecture, the limited resources on the mesh routers, and the shared wireless medium, the WMN poses special requirements for NFV integration. It is, therefore, necessary to investigate whether this network architecture is suitable for such integration (see Chaper 5 and 6).
2. The second challenge concerns the placement of VNFs within the network. This placement can be optimised to reduce energy consumption and increase the whole network lifetime (see Chapter 7). Since the location of a VNF has a direct influence on the power consumption of the host server (processing component) and an indirect influence on the power consumption of the switches involved in forwarding the packets to and from its current location (forwarding components), an optimal allocation of the VNFs is the key to optimise the communication network's energy efficiency.
3. The coverage and access to the network are important challenges of the proposed architecture. Since the organisation specific access networks no longer exist, the core network must be extended to guarantee complete coverage of the disaster area. In addition, access to the core segment must be guaranteed by a common technology like WLAN. Additionally wireless technologies such as LoRa or Bluetooth will may be provided.
4. Another challenge consists of the realisation and implementation of virtual networks. Due to the data protection legislation and security issues, it is assumed that some organisations will require logically separated networks for their teams. In such cases, suitable and efficient interfaces are necessary to communicate with other organisations.

5. The last challenge involves administering and orchestrating the provided applications and network services. An orchestrator is required to allocate and manage resources and network services for different organisations. According to the communication challenges in a disaster scenario, this must be done in a distributed manner.

This research focuses on the first and second challenges listed above. To optimise the WMN as an infrastructure for NFV integration, Chapter 5 and Chapter 6 respectively address the problem of channel assignment and the problem of routing in WMN as essential properties for the performance of a mesh network (see Section 2.2). Chapter 7 addresses the problem of the energy-efficient placement of VNFs. The energy-efficiency is achieved in the network through:

- **Minimisation of network energy consumption:** The first optimisation objective is to provide a green communication network to support rescue operations in disaster scenarios. This objective can be achieved by reducing the network's energy consumption when the same services are offered. Besides the hardware-specific electronics and vendor-specific device architecture, a wireless router's power consumption depends on the processed network traffic and the hosted network functions (e.g., DNS or DHCP). To provide a hardware-independent optimisation, this research work assumes that the energy consumption of a wireless router depends only on the latter parameters (forwarded/routed traffic and hosted functionalities).

- **Maximise the network lifetime:** The second optimisation objective results from the limited energy on the mesh router since they are assumed to be battery supplied in disaster scenarios. The energy consumption must be proportionally distributed over the network to maximise the whole network lifetime. If this is not the case, the routers with a higher power consumption leave the network prematurely due to the energy leak. This leads to a loss in the coverage of the WMN. To overcome this issue, the location of a VNF is not only selected to minimise the energy consumption for the provided service but distributed over the network to maximise the whole network lifetime.

5 High Throughput Wireless Mesh Network

This chapter addresses the problem of channel assignment in multi-radio multi-channel WMN. Section 5.1 presents the results of the measurements carried out to complete the comparison between CA strategies in Section 3.2. The aim is to check whether the investigated strategies fulfil the interference compliance and throughput requirements. These questions could not or only partially be answered by the literature review in Section 3.2. Since the answer to these questions is negative, a new channel allocation method is proposed in Section 5.2. The proposed cluster-based strategy addresses issues such as cluster size, number of network interfaces, and the used wireless standard.

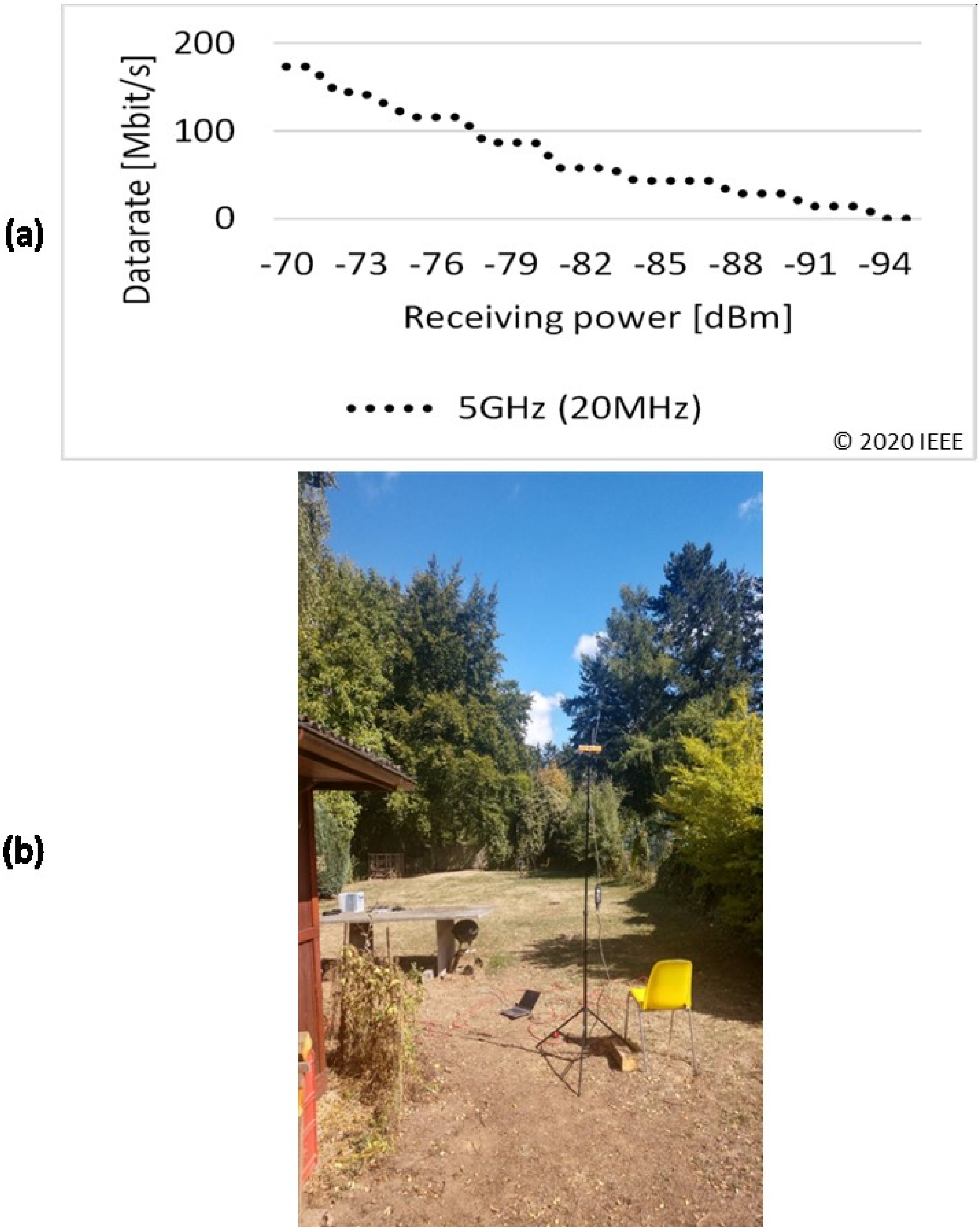
Some parts in this chapter have been published in (Tchinda *et al.*, 2020).

5.1 WLAN Field Measurements

This section presents the results of the throughput measurements to deepen the evaluation of the CA strategies presented in Section 3.2. The first series of measurements aim to determine the transmission range of WLAN. The interference range of WLAN is determined via the second series of measurements, and an interference model is proposed. The third measurement series determines and compares the throughput results in multi-radio multi-channel WMN with the throughput results in single-radio single-channel WMN. This section ends with a summary of the knowledge gained from the measurements. The measurement testbed and the used hardware are described in the following subsection. The measurements were performed only at the 5GHz frequency band. The 2.4GHz frequency band provides four non-overlapping channels in the EU (European Union) and three in the USA and is therefore not suitable for use in multi-channel WMN.

5.1.1 Description of the Measurement Testbed

The measurements were performed in a garden outside the town to avoid interferences with other WLAN devices in the neighbourhood. For the measurement, four fanless mini PCs were used. Each mini PC was equipped with two WLE600VX wireless modules (Compex Systems, 2021). This wireless module uses a Qualcomm-Atheros QCA9882 chipset (Compex Systems, 2021). The chipset implements a 2X2 MIMO and the IEEE802.11a/ac/b/g/n wireless standards. Figure 5.1a) shows the sensitivity of the chipset when using the IEEE802.11n standard in the 5GHz frequency band with a channel bandwidth of 20MHz. According to the datasheet, a theoretical data rate of 173.3Mbit/s is expected for a receiving power of more than -71dBm at 5GHz (Compex Systems, 2021). For the connection between the wireless module and the antennas outside the box, a cable with an attenuation of 0,7dB at 5GHz was used (Delock, 2022). Two antennas were attached to each wireless module with a gain of 4,5dBi at 5GHz. During the measurement, the mini PCs were set to a height of 3m above the floor with the help of a tripod (see Figure 5.1b)). The measurement duration for the TCP stream was 90 seconds.



© 2020 IEEE

Figure 5.1: (a) Sensibility of the WLE600VX WLAN module, IEEE802.11n, 20MHz (Compex Systems, 2021), (b) Mini-PC on tripod during measurements of WLAN transmission and interference range

5.1.2 Transmission range

This subsection determines the transmission range of IEEE802.11n is and compares the results with the theoretical expectations.

Figure 5.2 shows the setup for determining the transmission range. The power at the receiving station P_B can be calculated using the following equation:

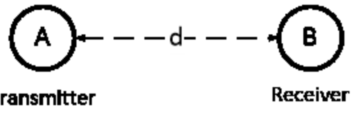
$$P_B = P_A - A_A + G_A - PL + G_B - A_B - Fade\ Margin \tag{5.1}$$

where P_A is the transmitting power, A_A is the attenuation between the transmitter wireless module and the transmitter antenna, G_A is the gain of the transmitter antenna, PL is the path loss during the transport between transmitting and receiving station, G_B is the gain of the receiver antenna, A_B is the attenuation due to the transport between receiver antenna and receiver wireless module, $Fade\ Margin$ is the allowed error during transmission.

This research uses the free space path loss to estimate the attenuation due to the transport through the wireless medium. This estimation can be done due to the absence of obstacles and reflexions in the garden. The free space path loss in dB is given by the equation (Valenzuela, 1996)

$$PL = 20\,log(d) + 20\,log(f) - 147.55 \tag{5.2}$$

d is the distance between transmitting and receiving mesh router in m (see Figure 5.2) and f is the frequency in Hz.



© 2020 IEEE

Figure 5.2: Setup for determining the transmission range (Tchinda *et al.*, 2020)

The standard procedure for determining the transmission range is to measure the data rate change depending on the distance between transmitter and receiver at constant transmitting power. This procedure requires a movable power supply to operate the mini PCs and adequate measurement field length. Since the length of the garden was 100 m and thus below the expected range, an alternative measuring method was used. The sending power of the transmitting router was varied to simulate a distance change (a change in the path loss) between transmitter and receiver (see Equations 5.1 and 5.2).

Figure 5.3 resumes the results of the power measurement at the receiver. The receiving power was determined at the receiver using the Linux tool `iw` and compared with the theoretical expectation. The theoretical expected values are calculated using the equations 5.1 and 5.2. The $Fade\ Margin$ was set to 0, and the hardware characteristics (antenna gain and cable attenuation) introduced in Subsection 5.1.1 were used. The measurements were performed for the distances 10, 20, and 80m. The measurements were done by channel 36 (5180MHz) at the 5GHz frequency band. The transmission power was varied between 23dBm and 2dBm.

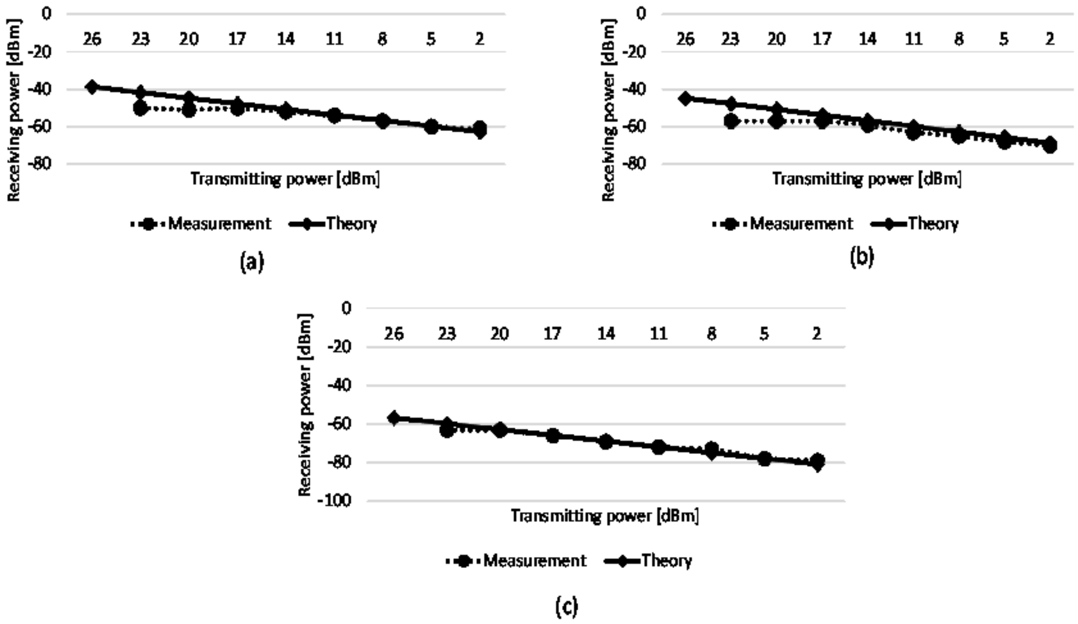
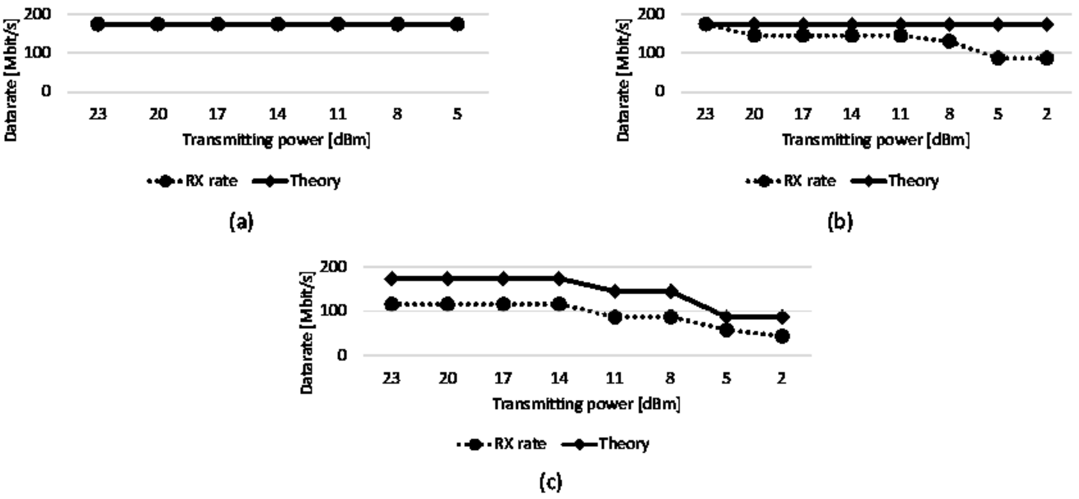


Figure 5.3: Comparison between theory and measured receiving power at channel 36 – 5.18GHz (a) 10m, (b) 20m and (c) 80m (Tchinda *et al.*, 2020)

The measured receiving power is almost identical to the theoretical expectation. A small deviation can be observed with a transmission power higher than 17dBm. A closer look in the datasheet of the wireless module (Compex Systems, 2021) shows a maximal transmission power of 16dBm if the Modulation and Coding Scheme (MCS) 8 is used at 5 GHz. This maximal value increases to 22dBm by the lowest MCS 0 and explains why theory and expected values are nearly identical at 80m.

In a second step, receive bit rates (RX rates) were measured. These values were compared with the expected values from the theory. The theoretical receive bit rates can be determined from the measured receive power. For this purpose, the measured receive powers (see Figure 5.3) are compared with the sensitivity of the wireless module in Figure 5.1a) (e.g. a receive power above -71dBm leads to a theoretical receive bit rate of

173.3Mbit/s). The results of the comparison are shown in Figure 5.4. A discrepancy between the two values can be observed. This means that the used MCS is lower than the value specified by the manufacturer of the wireless module. This discrepancy can be explained either by an error in the chip manufacturer's specifications or by an unsuitable alignment of the antennas, which results in the transmission error rate being higher than expected. This discrepancy increases with distance, as shown in Figure 5.4, making it impossible to predict the RX value based on the wireless module's calculated receive power and sensitivity.



© 2020 IEEE

Figure 5.4: Comparison between the measured RX rate and the expected value according to the measured receiving power at channel 36 – 5.18GHz (a) 10m, (b) 20m, and (c) 80m (Tchinda *et al.*, 2020)

Steps 1 and 2 have shown that it is impossible to determine the transmission range from purely theoretical considerations.

Therefore, it is necessary to estimate the transmission range based on the measured bitrate values. For this purpose, a TCP measurement was performed between the transmitting and receiving routers. The results are presented in Figure 5.5. It is important to note that the measured TCP bitrates are below the measured RX rates in Figure 5.4. This is due to the overhead caused by IEEE802.11 management frames (beacon frames) and the headers of the underlying protocols to TCP. According to the results presented in Figure 5.5, if the transmitting power used by the sender is 17dBm, a TCP bitrate of 130Mbit/s at 10m, 108Mbit/s at 20m. and 102Mbit/s at 80m can be expected.

Based on the measured bitrates at 10m, a prediction about the expected bitrates at 20m can be made. According to equations (5.1) and (5.2) these values are obtained through a translation of 6dBm in the measured throughput. The same process can be applied to the measured values at 80m. As a result, a TCP bitrate of 57,7 Mbit/s can be expected by a distance of 160m using a transmission power of 17dBm. This value corresponds to the measured TCP bitrate for a transmission power of 11 dBm.

It is important to mention that these results are only partially transferable to other WLAN standards or chips from other manufacturers because they are real field measurements. However, they give a good indication of the state-of-the-art development of WLAN (expected data rates when setting up a WMN for disaster) and a good comparison with theory.

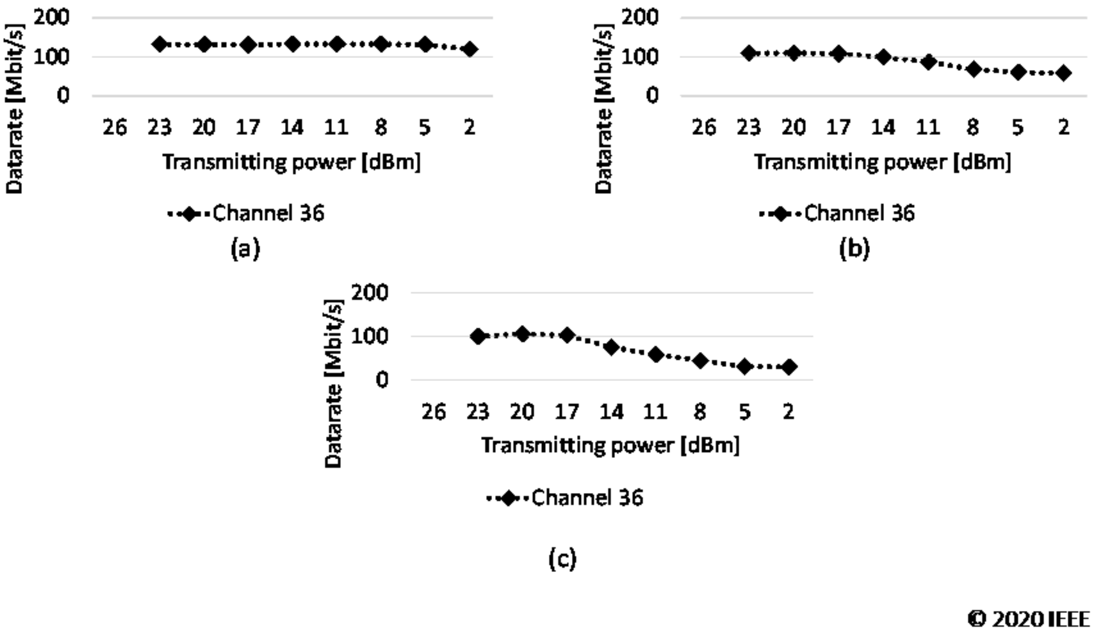
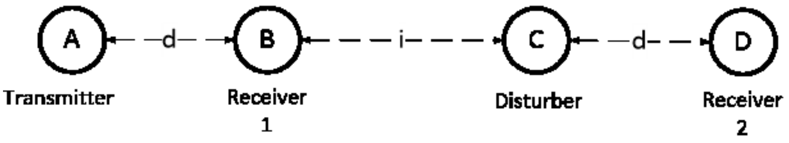


Figure 5.5: Measured TCP bitrate depending on the transmission power at channel 36 – 5.18GHz (a) 10m, (b) 20m and (c) 80m (Tchinda *et al.*, 2020)

5.1.3 Interference Range

Interferences occur when two or more mesh routers in the interference range of each other want to transmit on the same channel simultaneously. Two models are typically used to describe the interference range between mesh routers in the literature. The first one is the protocol model. It considers that two mesh points interfere when they are in the carrier sense range of each other (Wildman and Weber, 2016). According to this model, the inferences caused by a mesh point B in a few meters from a mesh point A and the interferences caused by a mesh point C far away are supposed to be the same as long as node C is inside the carrier sense range of node A. Because the carrier sense range of a node is at least as high as its maximal transmission range, this model leads to a high interference area and, therefore, a significant throughput decrease inside a WMN. The second model is the physical model, which considers that the interferences caused by a disturbing station depend on the difference between the signal strength from the disturbing router and the transmitting router at the receiver. Again if the above-described scenario is considered, the interferences caused by node B will be higher than those caused by node C at node A.

This subsection aims to determine which model most accurately describes the interferences within the WMN. To achieve this goal, the following measurements were performed. Figure 5.6 describes the measurement testbed. The distance between transmitter (A) and receiver 1 (B), respectively, between disturber (C) and receiver 2 (D) was 20m. The transmission power was set to a fixed value of 17 dBm at routers A and B. The transmission power was changed in 3dBm steps on router C and D. This variation of the transmitting power was done to simulate an increase in the interference distance i between B and C. The TCP data stream was measured between A and B. At the same time, another TCP transmission was started between C and D.



© 2020 IEEE

Figure 5.6: Setup for determining the interference range (Tchinda *et al.*, 2020)

Figure 5.7 resumes the measurement results. It presents the measured TCP data rate between A and B depending on the receiving power from C at B. For a receiving power under -77dBm, the measured bitrate is half of the expected bitrate without interferences. That means both routers A and C equally share the wireless medium as expected by the protocol model. For a receiving power between -78 and -87dBm, the measured throughput varied between 50 and the maximal value of 110 Mbit/s. In this segment of the graph, the physical model is used. Below this value, the TCP stream between C and D does not influence the stream between A and B. This result shows that neither the physical nor the protocol model can describe the interference in a WMN properly. The praxis shows two areas, each of which can be explained by one of these models.

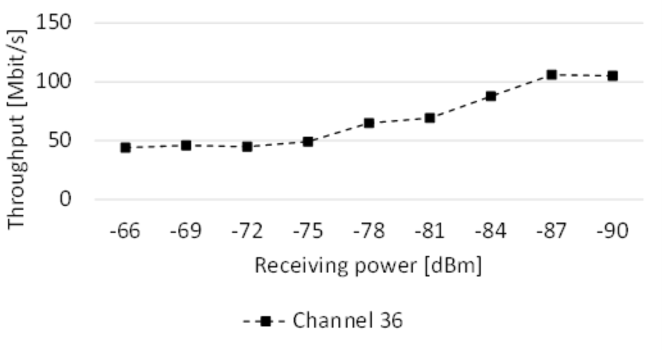


Figure 5.7: Throughput depending on the receiving power of the disturber
(Tchinda *et al.*, 2020)

5.1.4 Multi-Hop Communication

In this subsection, the expected throughput in a multi-radio WMN is measured, and the results are compared with the throughput in a single-radio WMN. The measuring set-up consists of four stations at a distance of 5 m from each other (see Figure 5.8). The transmission power was set to 8dBm. In order to force the TCP stream to use the multi-hops path, the direct links between the routers A-C, A-D and B-D were disabled in both directions using the `iw` tool.

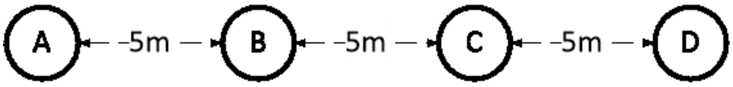


Figure 5.8: Setup for determining the hop dependence of the path throughput
(Tchinda *et al.*, 2020)

Figure 5.9 resumes the measurement results. According to these results, the throughput inside a single radio WMN decreases to 50% when the traffic goes through two hops. This is because routers A and B must transmit simultaneously for the transmission to be uninterrupted. However, because they are within interference range of each other, only one router is allowed to transmit at a time. After three hops, the measured throughput is nearly 30% of the link throughput. Here, too, the decrease in the data rate can be explained by the interference range of WLAN (see Subsection 5.1.3). Routers A, B and C must be able to transmit simultaneously so that the transmission can take place without interruption. In contrast, the TCP throughput remains constant when the traffic goes over several hops in multi-radio multi-channel WMN. The reason for this is that the transmission between router A and B, router B and C and router C and D can occur independently of each other.

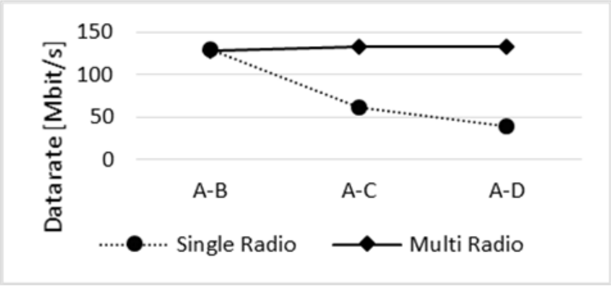


Figure 5.9: TCP throughput depending on the number of hops (Tchinda *et al.*, 2020)

5.1.5 Conclusion

Table 5.1 is the extension of Table 3.2 and presents the evaluation of existing channel allocation procedures in multi-radios WMN. Based on the measurements in this section, the fulfilment of the interference compliance and throughput requirements can now be evaluated.

Interference compliance: This requirement is met only in link-based CA procedures with few interfaces. The cluster-based CA strategies examined all assume that the channels can already be reused after twice the transmission range. This contradicts the results in Subsection 5.1.3, where it was shown that the distance between clusters with the same channel must be higher to have a high data rate during transmission.

Throughput: This requirement is also not fulfilled by the existing cluster-based channel allocation methods. There, the size of the clusters is not addressed. Moreover, multi-hop communication is allowed within clusters. As the results of Subsection 5.1.4 show, a 2-hop communication leads to a halving of the data rate.

Table 5.1: Evaluation of existing CA strategies (extension)

Requirements	**CA strategy**				
	Lb(high)	***Lb(low)***	***CoMTaC***	***CBCA***	***CCA***
Topology preserve	+	-	o	+	o
Interference compliance	-	+	-	-	-
Scalability and complexity	+	-	+	+	+
Throughput	+	+	-	-	-
Wireless standard compliance	-	+	+	+	+

Assessment notation: + satisfied, o partially satisfied, - not satisfied

5.2 Proposed Channel Assignment Strategy

The measurements and the subsequent evaluation of existing CA strategies in Section 5.1 have demonstrated the necessity to develop a new CA strategy that can comply with the interferences in WMN. In this section, a new solution that fulfils the high throughput requirement of WMN in disaster scenarios is proposed. In the following, the optimal size of the cluster (number of routers in a cluster) and optimal number of interfaces are determined so that the proposed channel allocation strategy takes into account the results obtained in Section 5.1.

5.2.1 Clustering and cluster size

In this subsection, the optimal cluster size n_{opt} is determined. This size is defined by the two following optimisation objectives:

- The first optimisation objective consists of the minimisation of interferences or throughput maximisation. According to (Gupta and Kumar, 2000), the throughput inside a WMN, where routers can directly communicate with each other, is given by the equation

  $$\frac{W}{\sqrt{n\ log\ n}} \tag{5.3}$$

  W is the expected link throughput for the Point-to-Point communication between two routers in Mbit/s, and n the number of mesh routers, which build the WMN. This throughput decreases with the value of n. That means the number of router inside the cluster has to be low as possible to maximise the throughput.

- The second optimisation objective is to maintain the connectivity between mesh routers in WMN. The maximal connectivity is achieved when no communication link is lost during the clustering process. This means that all routers within transmission range of each other can continue to communicate via 1 hop after the clustering process. For example, if a communication network is considered where each router is equipped with two wireless interfaces, each neighbour router must be connected over one of these two interfaces after the clustering process.

In addition to these optimisation objectives, two optimisations constraints are also defined.

- First, the routers which build the cluster must be in the transmission range of each other. This constraint is made to avoid the multi-hop transmission inside a cluster. Inside a WMN, where routers communicate in a multi-hop manner using the same channel, the throughput decreases dramatically, as shown by the measurement in Section 5.1.
- Second, a new cluster is built only if two or more cluster members provide a gateway functionality to adjoining clusters. This constrain is defined to avoid the partitioning of the WMN (network resilience (Frick *et al.*, 2019)).

Assume the WMN topology in Figure 5.10a), where each router can communicate with eight neighbouring routers (routers within its transmission range) and is equipped with two wireless interfaces. According to the above-defined optimisation objectives and constraints, the optimal cluster size n_{opt} can be determined using the following steps:

- First, neighbouring routers of router A are separated into two groups and assigned to one of its two interfaces depending on their location within the network. For example, the first group is built by the routers B, C, D and E and is connected via the first interface. The second group consists of the routers F, G, H and I. These routers are connected via the second interface (see Figure 5.10b).
- Second, subgroups are created for each defined group in the first step. These subgroups consist of routers that are within communication range of each other and must contain Router A. The cluster is formed by the subgroup with the highest number of members. This step can lead to the loss of connections between Router A and the neighbouring routers that are not part of the cluster. If the first group of the previous example is considered, the following subgroups can be built: (A, B, C, D) and (A, D, E). The cluster is built by the routers A, B, C and D, because this subgroup maintains the connectivity with the highest number of neighbouring routers. This leads to the loss of the link between A and E (see Figure 5.10c).
- Third, each group member that was not part of the selected subgroup to build the cluster will next be tested (e.g. router E). If a new cluster can be built, this is done according to steps 1 and 2. If it is not the case (e.g. due to the second constrain), the router is attached to the current cluster.

Figure 5.10d shows the end state of the clustering process. The optimal cluster size for the examined topology is 4 ($n_{opt} = 4$). This result is specific to this network topology. Clustering must be performed for each topology to determine the optimal cluster size.

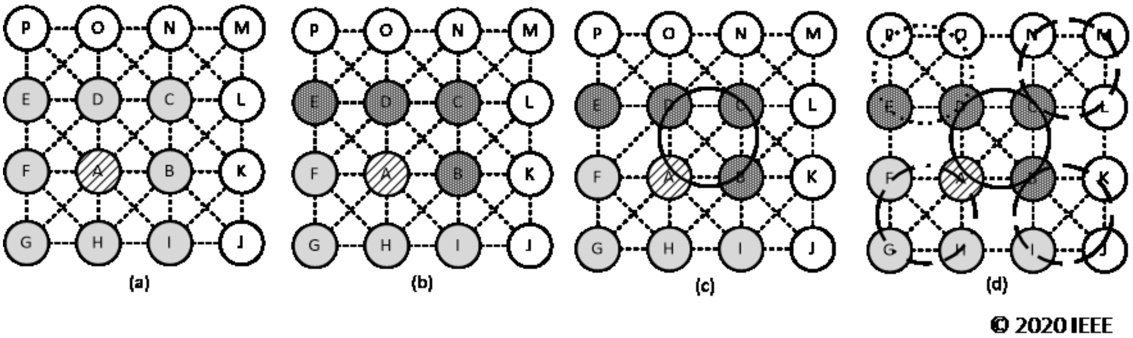


Figure 5.10: WMN clustering (a) routers within the transmission range of A in grey, (b) routers assigned to the first interface of A, (c) cluster built by the routers A, B, C, and D (d) end state (Tchinda *et al.*, 2020)

5.2.2 Number of interfaces and channel assignment

In the previous subsection, an algorithm to determine the optimal cluster size n_{opt} was introduced. It was demonstrated that its value depends on two major factors: the number of interfaces and the number of neighbour routers. In this subsection, the optimal number of interfaces ε_{opt} is determined to perform the channel assignment. This number is defined by the following constraints:

- First, the number of existing non-overlapping channels provided by the IEEE802.11 standard. This number is limited to three channels when the 2.4GHz frequency band is used and 23 in the EU (European Union) respectively 26 in the USA, when the 5GHz frequency band with a bandwidth of 20MHz is used (EUR-Lex, 2005; 2007; IEEE, 2016) (only channels with a allowed transmission power of more than 20 dBm, as the channels with a lower transmission power have a shorter range, as shown in Subsection 5.1.2. They are therefore unsuitable for setting up the WMN in the disaster scenario (see requirement in Section 2)).

- Second, the restriction is given by the channel re-usage. This depends on the interference range. Two clusters should not use the same channel within each other's interference range, as the measurements in Subsection 5.1.3 show.

Assume a network topology where each router is equipped with ε wireless interfaces and has β neighbouring routers (number of routers in its transmission range). According to the measurement results presented in Section 5.1, the transmission range T_{rg} can be written as a fraction of the interference range I_{rg} $(T_{rg} = \frac{I_{rg}}{\alpha})$. The value of the factor α depends on the wished data rate and was estimated through measurements to proximally four respectively eight when a TCP bitrate of 80Mbit/s respectively 110Mbit/s is required between the different cluster members.

Assuming router A is a member of a cluster (see Figure 5.11). All members of the same cluster must be within the transmission range T_{rg} of router A.

If the channel C_0 is used by A for the communication inside the cluster, another cluster should not use this channel within the interference range I_{rg} of A.

Assuming router C is a member of the same cluster. The router C is located at a maximum distance T_{rg} of A. Since C is using the same channel C_0 to communicate with A, another cluster should not use this channel within the interference range I_{rg} of C.

As result the channel C_0 should not be used by another cluster within a range of $I_{rg} + T_{rg}$ from the current location from router A.

Due to symmetry, the area that must be covered by non-overlapping channels is half of the area where channel C_0 may not be reused $\frac{I_{rg}}{2} + \frac{T_{rg}}{2}$ (channel C_0 may not be reused within a range of $I_{rg} + T_{rg}$ because it was used in the middle of the defined area, but if chosen appropriately, the other channels may occur twice in this area).

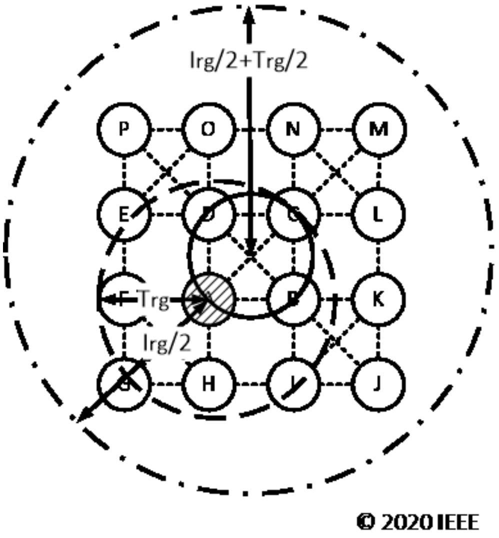


Figure 5.11: Estimation of the required number of non-overlapping channels
(Tchinda *et al.*, 2020)

The number of routers N inside this area (area with non-overlapping channels) can be calculated using the following equation

$$\begin{aligned} N &= area \times \ density \\ &= \pi\left(\frac{I_{rg}}{2}+\frac{T_{rg}}{2}\right)^2 \times \ density \\ &= \pi\left(\frac{I_{rg}}{2}+\frac{T_{rg}}{2}\right)^2 \times \frac{\beta}{\pi {T_{rg}}^2} \\ &= \left(\frac{\alpha}{2}+\frac{1}{2}\right)^2 \beta \end{aligned} \tag{5.4}$$

Where $density = \frac{\beta}{\pi {T_{rg}}^2}$ is the number of routers per unit area (e.g., number of routers within the transmission range β divided by the area of the transmission area).

The total number of wireless interfaces inside this area is given by (the number of routers N (see equation (5.4)) multiplied by the number of interfaces)

$$\varepsilon N = \frac{(\alpha + 1)^2}{4} \varepsilon\beta \tag{5.5}$$

If the number of cluster members is equal to n_{opt}, the number of cluster γ and therefore the number of required non-overlapping channels can be determined with the equation

$$\gamma = \frac{\varepsilon N}{n_{opt}} = \frac{(\alpha + 1)^2}{4} \frac{\varepsilon\beta}{n_{opt}} \tag{5.6}$$

That means if the network topology in figure 5.10 is considered, in which each router is equipped with two radio interfaces ($\varepsilon = 2$) and has eight neighbouring routers ($\beta = 8$), the maximal value of α and therefore the maximal throughput of the network can be calculated for the optimal cluster size $n_{opt} = 4$ (see the demonstration in Subsection 5.2.1). This value is calculated for $\gamma = 26$ (number of non-overlapping channels). The value of α is obtained by reformulating the equation 5.6

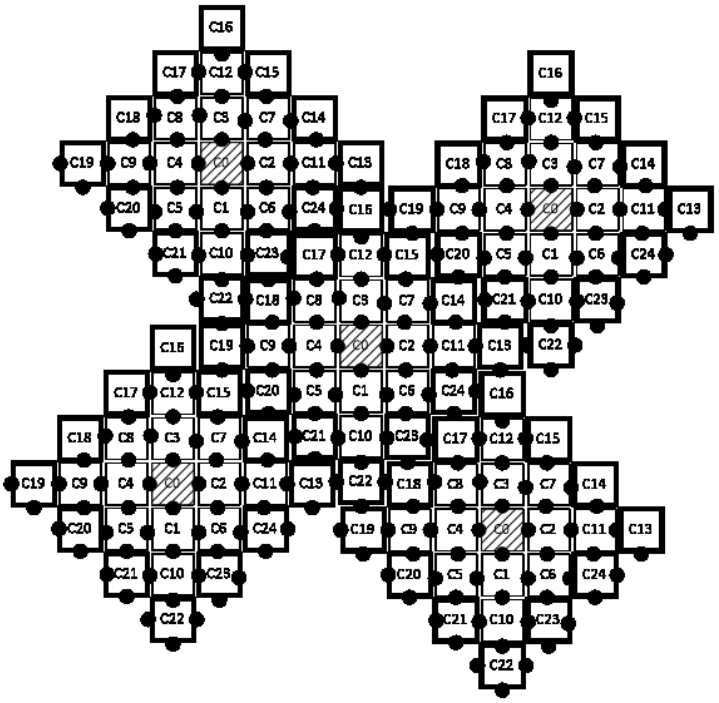
$$\alpha = \sqrt{\frac{4\gamma n_{opt}}{\varepsilon\beta}} - 1 \tag{5.7}$$

and is equal to $\alpha = 4{,}1$.

That means the maximal network throughput is obtained when the transmission range is one-quarter of the interference range. According to the measurements in Section 5.1, this throughput is proximally equal to 80Mbit/s.

On the same way, it can be demonstrated that no throughput improvement (higher value of α) can be reached through additional interfaces. For example, if the same network topology is considered with the difference that each router is equipped with four instead of two interfaces, each interface is now connected to two neighbours and the optimal cluster size $n_{opt} = 3$. In this case $\alpha = 2{,}6$. That means $T_{rg} = I_{rg}\ /2{,}6$. The expected TCP throughput at this distance is estimated to be 26Mbit/s.

Figure 5.12 shows the optimal CA within a grid topology, where each router is equipped with two radio interfaces and can communicate with eight neighbours. The clustering and CA was performed according to the proposed strategy. Figure 5.12 demonstrates that at least 25 non-overlapping channels are required to ensure that the minimal distance between routers using the same channel but members of different clusters is four times the transmission range.



© 2020 IEEE

Figure 5.12: Optimal channel assignment for a grid topology (Tchinda *et al.*, 2020)

5.3 Summary

In this chapter, the limitation of existing CA strategies in disaster scenarios has been demonstrated. This was done based on multiple real-world measurements. It has been shown that none of the existing strategies can meet the requirements defined in Section 2.2. In Section 5.2 a new CA strategy has been proposed to address these requirements. The proposed strategy solves the topology preserve requirement in WMN by implementing a cluster-based scheme in which each router attempts to maintain a connection with all routers within its transmission range. The interference compliance requirement is also solved through optimal usage of the available non-overlapping channels in the IEEE802.11 standard and by taking care of the relationship between transmission and interference range ($T_{rg} = \frac{I_{rg}}{\alpha}$, where α can be higher than two). The throughput requirement is met by avoiding multi-hop communication within the same cluster (1-hop channel switching). The proposed strategy also solves the requirements for scalability and complexity by using locally available information (list of routers within the transmission and interference range) and not generating additional packets or changes to the standard.

The results of the field measurements presented in this chapter have two significant usages. First, they are used to realise the CA in the core segment (WMN) of the proposed network architecture. This CA is a basis for the mathematical modelling of the optimisation problem in Chapter 7. Unlike wired networks, where the links have a fixed capacity, the capacity in wireless networks depends on both the transmission- and interference range. Second, the realised measurements are used to make realistic assumptions for evaluating the proposed algorithms for energy-efficient placement of

VNFs in Chapter 7. The assumed transmission range, interference range and multi-hop communication behaviour are based on the measurements presented in this chapter. That means a data rate of 102Mbit/s at 80m is assumed between transmitter and receiver according to the transmission range measurements in Subsection 5.1.2. Similarly, only routers in the same cluster can interfere using a protocol model after the CA process (see Subsection 5.1.3).

6 Routing in Wireless Mesh Network

This chapter aims to identify the most suitable protocol for routing in NFV optimised WMN. For this purpose, the performance of the routing protocols HWMP, Babel and B.A.T.M.A.N. advanced is compared in Section 6.1. These three protocols turn out to be promising from the literature review in Section 3.3. The three protocols are compared using a virtual test environment developed for this research. The comparison focuses on the performance (network throughput and latency) of the three routing protocols under dynamic processes such as different link qualities, incoming traffic, failure or the addition of a new router. The fulfilment of the dynamic requirement could not be evaluated by a literature review alone because different characteristics (link state or distance vector, proactive, reactive or hybrid) influence it. Section 6.2 proposes a two-layer network solution to address the routing problem in large networks. Section 6.3 summarises the results.

Some parts in this chapter have been published in (Tchinda *et al.*, 2017)

6.1 Performance Comparison of HWMP, Babel and B.A.T.M.A.N. advanced

This thesis uses a virtual environment to evaluate the performance of the routing protocols HWMP, Babel and B.A.T.M.A.N. advanced. The first series of tests investigates the influence of link quality and existing data transmissions on the selection of the communication route. The second series compares the performance of the tested routing protocols in terms of the time required to find a suitable communication route when a router fails or when the mesh is expanded by adding a new router. The last series of tests examines the impact of network size on the performance of the routing protocols.

Table 6.1 summarizes the configurations of the protocols used for the comparison.

Table 6.1: Routing protocols configuration

Routing Protocol	Configuration
HWMP	Configuration modus: reactive PREQ interval: 4s Beacon frame interval: 1s
Babel	Version: babeld-1.8.0-6-g16ae1f9 Hello interval: 4s IHU interval: 12s Update interval: 16s
B.A.T.M.A.N. advanced IV	Version: batman-adv-2017.2 OMG interval: 4s
B.A.T.M.A.N. advanced V	Version: batman-adv-2017.2 OMG interval: 4s

6.1.1 Description and evaluation of the test environment

The used test environment is an extension of ViPMesh (Rethfeldt *et al.*, 2016). ViPMesh is a virtual prototyping framework for evaluating IEEE 802.11s based WMN. It combines the advantages of simulation with those of emulation tools. The implemented virtual environment uses Docker containers to realise the routers, the kernel module mac80211_hwsim to realise the IEEE 802.11 radios (Jouni, 2008) and wmediumd (Wmediumd, 2022) to emulate different transmission ranges between the radio interfaces of the routers.

Figure 6.1 shows the architecture of the test environment. It consists of three core elements: Docker, mac80211_hwsim, and wmediumd.

Docker: Docker uses namespaces to create containers with isolated network stacks and control groups (cgroups) to allocate resources (CPU, memory, disk I/O …) to those (Docker, 2022). The generated containers use the host operating system kernel so that the resources necessary to run an image are small. The usage of containers has the following advantages:

- Many nodes can be created and run simultaneously on the host machine.
- The routing protocols HWMP, Babel and B.A.T.M.A.N. advanced are already implemented for Linux, and the implementations are compatible with multiple network namespaces.
- Multiple and complex applications can be implemented inside Docker containers.

mac80211_hwsim: mac80211_hwsim is a Linux kernel module that can be used to simulate an arbitrary number of IEEE 802.11 interfaces (Jouni, 2008). The simulated drivers work like common hardware drivers and require no changes to the mac80211. mac80211_hwsim is part of the Linux kernel. The simulated radios can be associated with a network namespace or a Docker container. It also provides an additional network interface (hwsim0), which can be used to monitor frames exchanged between virtual interfaces (Jekyll, 2020).

wmediumd: Between the simulated IEEE 802.11 interfaces using mac80211_hwsim, there are no interferences, bandwidth limitation or packet loss. The performance of the host PC determines these parameters. So, the bandwidth can be several Gbit/s without packet loss in the normal state. This problem can be solved using wmediumd. wmediumd uses netlink (Yaron, 2017) to manage the data transfer between virtual wireless interfaces. For example, it can be used to integrate a bandwidth limitation according to the information contained in each frame's MAC-header and simulate packet loss according to a specific setup given by a configuration file or deduce from the position of the current node. The code of wmediumd is available on the GitHub repository (Wmediumd, 2022) and can be modified to integrate new functionalities.

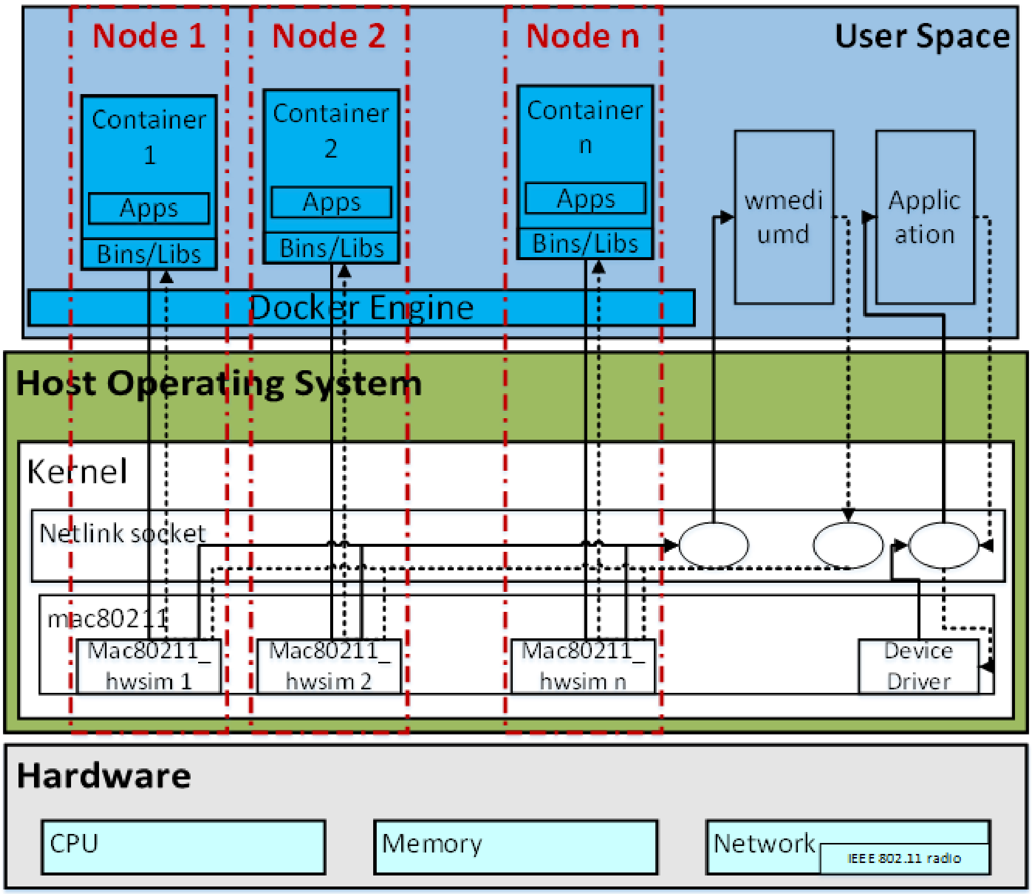


Figure 6.1: Test environment architecture

The following tests were carried out to ensure that the implemented environment works as expected.

Dependence between link quality and bandwidth: The Received Signal Strength Indicator (RSSI) between two network routers R1 and R2 was continuously changed using wmediumd to test the dependency between link quality and link bandwidth. After each change, the maximum throughput between both routers was measured using a UDP and then a TCP data stream that iperf3 generated (Dugan *et al.*, 2022). Both routers were configured to use the ad-hoc modus. The graph in Figure 6.2 summarises the results of this test. As the RSSI value increases, the bandwidth increases gradually and takes on discrete values defined in the IEEE 802.11 b/g standards. In addition, the measured UDP throughput is higher than the TCP throughput. This is due to the protocol overhead of TCP and the interruption caused by acknowledgement packets.

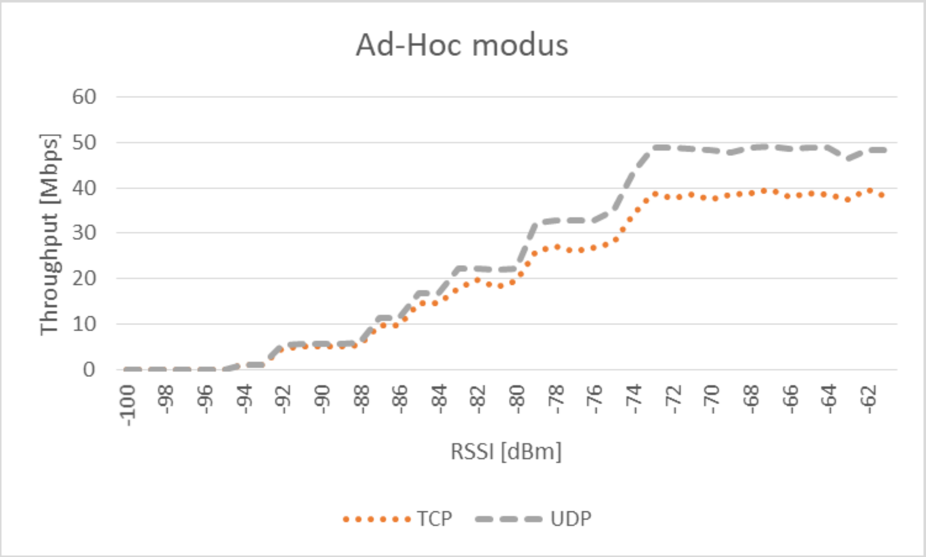


Figure 6.2: Throughput depending on the link quality

Medium sharing and data stream priority: For the second test, the RSSI value is set to -81 dBm between the routers R1 and R2 so that the maximum throughput between both routers is 24 Mbit/s on layer 1. First, a 60s length UDP data stream is started between R1 and R2. After 20s, a second one is started between the same devices. For both data streams, a UDP bandwidth of 24 Mbit/s is required. The measured bandwidths are shown in Figure 6.3. These results can be interpreted as follows:

- From 0 to 20s, the first stream uses the total link capability. Due to the header and control frames, the transmitted UDP data rate is 18 Mbit/s.
- Between 30s and 60s, the first and second streams have to share the resources (medium access). The average data rate is now 9 Mbit/s for each flow. This value corresponds to half of the maximum data rate.
- After 60s, the resources are free for the second stream. The transmitted data rate is 18 Mbit/s again.

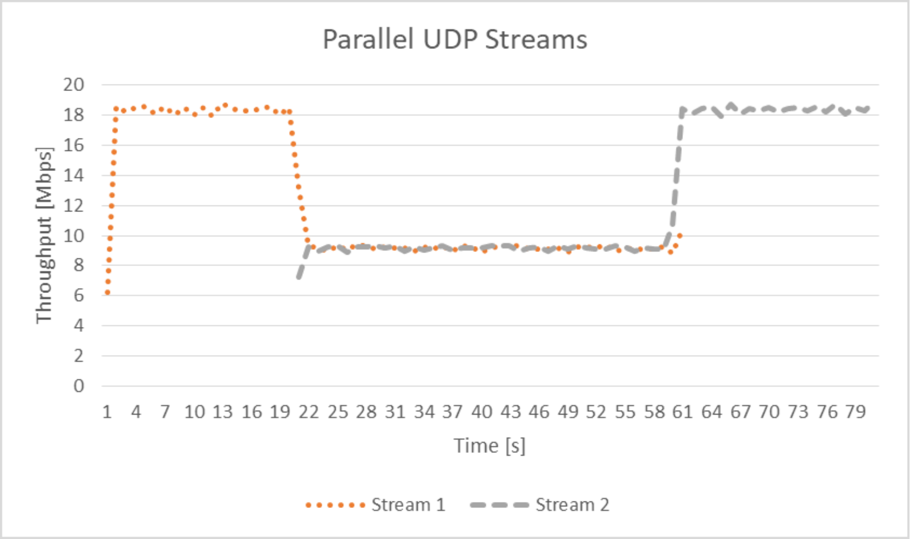


Figure 6.3: Data rate change by simultaneous data transfers

6.1.2 Link and Traffic Dynamic

In this subsection, the WMN routing protocols HWMP, Babel, B.A.T.M.A.N. advanced IV and V are evaluated regarding link and traffic dynamic scenarios. The first scenario consists of the path selection for a data transfer when the maximal throughput of the existing paths is different. The second scenario consists of path selection when the best path is overloaded. Figure 6.4 shows the network topology used to perform these two scenarios. It consists of 10 mesh routers. The RSSI value is set to -90dBm and -81dBm so that the maximum bitrate is 5.5 and 24Mbit/s, respectively.

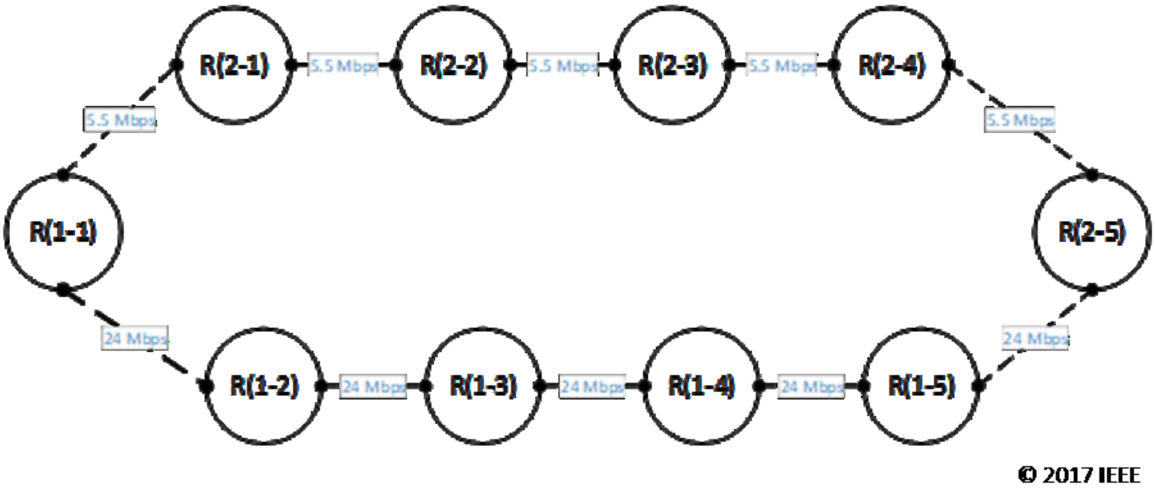


Figure 6.4: Mesh-Topology with 10 mesh routers (Tchinda *et al.*, 2017)

When building a WMN in a disaster area, it can be assumed that the distance between mesh participants is not the same overall. The data transmission between two neighbouring routers is also influenced by different factors, such as the used IEEE 802.11 standard or the disaster environment. Therefore, it is impossible to have the same link conditions between all routers in the WMN. Due to these differences, significant changes are expected in the maximum data rate. The routing protocol must consider the available bandwidth between the source and the destination router to overcome this issue. To test this, the network topology in Figure 6.4 is used. After configuring the routers, a waiting period is inserted to ensure that all routing updates have been carried out (this is important for proactive protocols). The maximum throughput between routers R(1-1) and R(2-5) was measured by simulating a 90s UDP data transmission using iperf3. The process was repeated ten times for each protocol and the next transit router was determined. The results obtained can be interpreted as follows:

- The routing protocol HWMP considers the maximum bandwidth of the available paths. Therefore, the UDP packets are routed via router R(1-2) in all ten tests.
- The routing protocol Babel balances well between the two alternative paths. The next router is selected depending on the path that was learned first. The Hello messages used by Babel to determine the link quality are sent to the broadcast address. In WLAN, messages sent to the broadcast address are transmitted using the lowest possible data rate (1 Mbit/s in this scenario). Because no packet loss is registered at this rate, the protocol cannot differentiate between the path over R(1-2) and the one over R(2-1). Furthermore, the routing protocol Babel implements a mechanism to avoid unnecessary route changes. A route change occurs if the new route has a significantly better metric.
- The Routing mechanism and metric used by B.A.T.M.A.N. advanced IV leads to the same problem like Babel. Unlike Babel, B.A.T.M.A.N. advanced IV lacks a strategy for avoiding frequent route changes. The selected route can change more than once during a 90s transmission.

- The metric of B.A.T.M.A.N advanced V is based on the measured throughput. Therefore, it selects in all cases the router R(1-2) as the next router to reach R(2-5).

Another issue in WMN is the network traffic load. The routing protocol must consider the existing traffic and choose an alternative route if the best route is congested at the time of path establishment. The tests were carried out with the network topology from Figure 6.4 but introduced cross traffic. Firstly, a UDP data transfer was simulated between R(1-3) and R(1-4). The required bitrate for this transfer was set to 24 Mbit/s so that the link between these two routers was overloaded (the maximum bitrate was set to 24 Mbit/s on layer 1 using wmediumd). Secondly, a second UDP flow was simulated between R(1-1) and R(2-5), 30s after the first one was started. It was expected that the new flow would be routed over R(2-1) as long as the first stream between R(1-3) and R(1-4) is running. The experiment was repeated ten times. The obtained results can be summarised as follows: using HWMP and B.A.T.M.A.N advanced V, the data stream is routed over R(1-2) by all ten tests like in the previous scenario. This indicates that the existing data stream between R(1-3) and R(1-4) does not affect the new communication. By Babel the path over R(1-2) is selected 6 times and over R(2-1) 4 times. The same result is obtained with B.A.T.M.A.N advanced IV. Here, the chosen path can change more than once during the transmission. This means that none of the protocols examined can take into account the existing communication between R(1-3) and R(1-4) when choosing the communication path.

6.1.3 Router Dynamic

Unlike common ad hoc networks where mobility plays an important role, dynamic processes are not the focus in a WMN. However, they are an essential part of the use cases in disaster situations. In this subsection, the ability of the routing protocols HWMP, Babel, B.A.T.M.A.N. advanced IV and V to react to the loss or the integration of new devices will be tested and evaluated.

A common scenario in a disaster situation is the loss of an existing mesh router due to events such as aftershocks. As the devices of the disaster network are battery-supplied, a lack of energy can also lead to the loss of a router. To react to this loss, all data flows via the lost router must be redirected within a short period. In this this test series, the time required for discovering an alternative path will be analysed. The network topology in Figure 6.4 was used for this purpose, and an ICMP data transfer was simulated between the routers R(1-1) and R(2-5). The interval between ICMP Requests was 10ms. After 30s, the router R(1-3) was shut down, and the time difference between the last ICMP packet sent via R(1-2) (old path) and the first packet sent via R(2-1) (new one) was measured with Wireshark. The result is shown in Figure 6.5. The protocol HWMP is the fastest and needs 0.2s to find an alternative path. This is due to the PERR frames generated by the neighbouring routers of R(1-3) after it leaves the mesh. The protocols B.A.T.M.A.N. advanced IV and V need 4.5s in average. This is due to the interval of 4s between the OGMs. The worst result is delivered by Babel (21.6s) and is based on the low frequency of routing updates (16s).

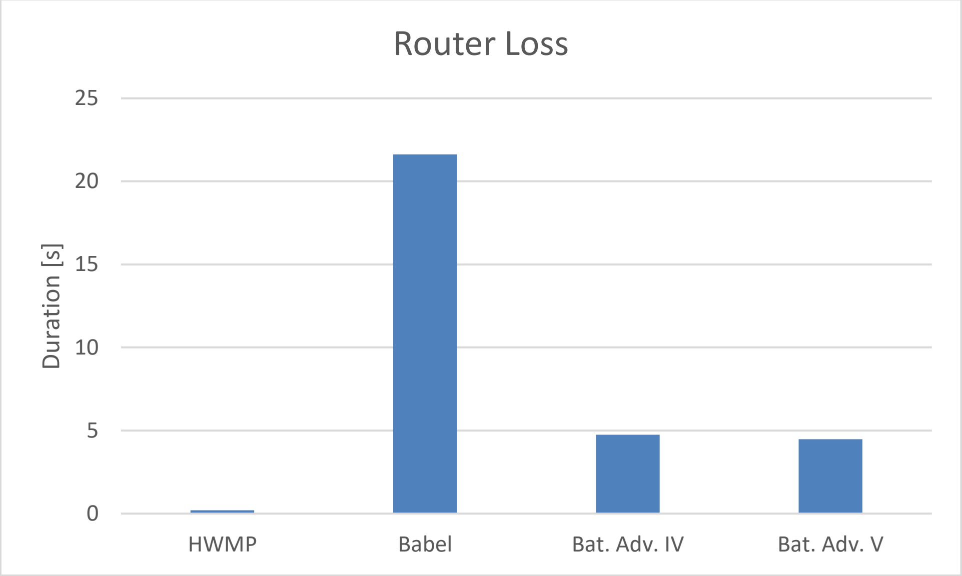


Figure 6.5: ICMP stream interruption duration after the router R(1-3) has left the mesh

An existing mesh can be extended by including new routers. This test series investigates the delay needed by the router R(1-1) to reach the router R(2-5) after it was started and becomes available. The test was performed using the `ping` tool. The duration between the first frame sent by R(2-5) after it joins the mesh and the first ICMP response it received, was measured. The results are shown in Figure 6.6. HWMP also presents the best result in this scenario with an average duration of 0,2s. For the protocols B.A.T.M.A.N. advanced IV and V, this procedure requires 6s and 3s, respectively. Babel takes the most time (18s) to establish a communication between R(1-1) and R(2-5). The high delay measured when using Babel can be explained through the duration necessary for the association between R(2-5) and its neighbouring routers and the low frequency of routing updates.

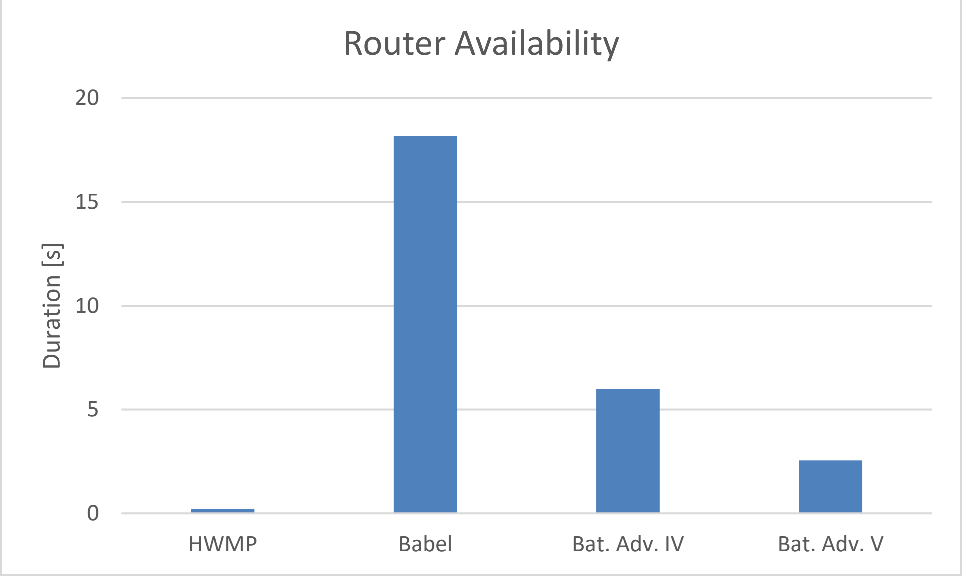


Figure 6.6: Necessary duration to reach a new router after that it connects to the mesh

One main objective of integrating a new router inside an existing mesh is to improve the network performance. In this scenario, the mesh consists of the network topology in Figure 6.4, except for router R(1-3), which initially does not participate in the mesh. A UDP data stream was emulated between R(1-1) and R(2-5). After 30 s, the router R(1-3) joins the mesh, and the experiment measured the delay until the routing protocols discovered a better route via R(1-3). Figure 6.7 shows the results obtained by the test. The results can be interpreted as follows:

- The routing protocol HWMP requires 5s to redirect the UDP stream. This value can be explained through the duration necessary for R(1-3) to discover its neighbouring routers and the interval of the periodic PREQ sent by R(1-1).
- The data stream is not redirected by Babel (0 in the graph). Due to the metric implemented by Babel, the protocol cannot make a difference between the paths over R(1-2) and R(2-1). The data stream is already transmitted over R(2-1) when R(1-3) connects to the mesh. Due to the implemented mechanism to avoid

unnecessary route changes in Babel, this path is used for the complete duration of the transmission.

- The result obtained by B.A.T.M.A.N. advanced IV should be the same as by Babel. However, because the protocol does not implement a mechanism to avoid multiple route changes, the selected path can change more than once after the integration. The selected route changes after 44s on average.
- A complete integration, including the UDP stream's redirection, is possible using B.A.T.M.A.N. advanced V. After the new router joins the mesh, the update procedure is started. This process requires approximately 5s.

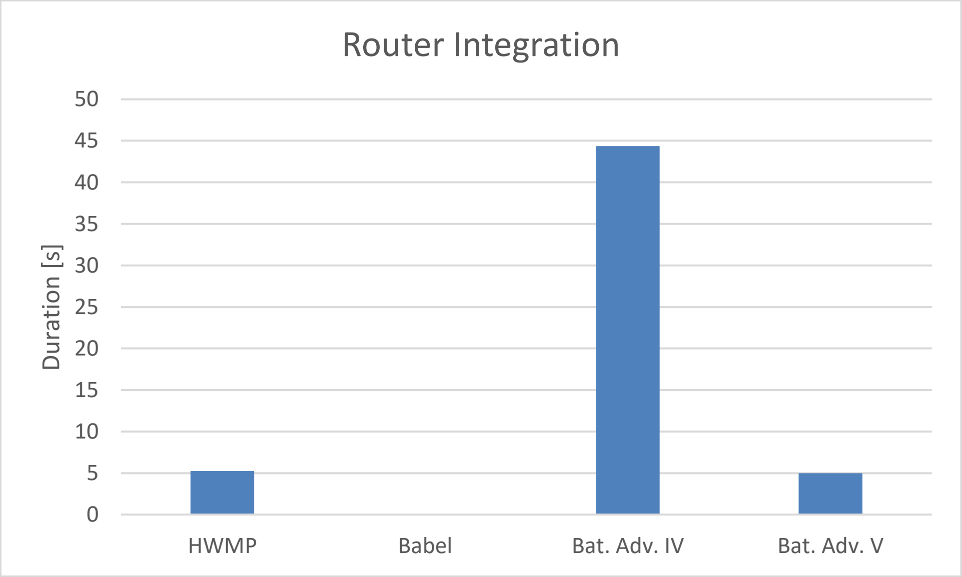


Figure 6.7: Necessary duration for the complete router integration

6.1.4 Network size

This subsection evaluates the performance of the routing protocols HWMP, Babel, B.A.T.M.A.N. advanced IV and V in large networks. Figure 6.8 shows the used network topology. It consists of an n×m grid. The RSSI is set to the same value for all links so that the maximum bandwidth between neighbouring nodes is 24 Mbit/s on layer 1.

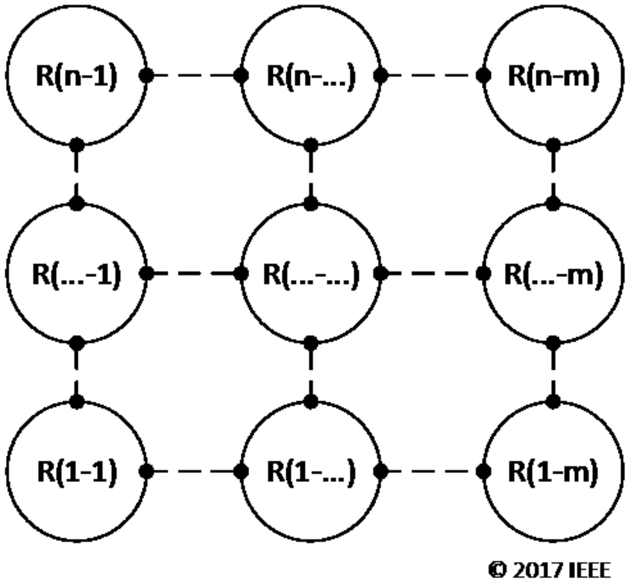


Figure 6.8: Mesh grid (Tchinda *et al.*, 2017)

For the first test, the TCP throughput between the routers R(1-1) and R(n-n) was measured with iperf3. Figure 6.9 shows the obtained results. A strong dependency between the network size and the measured throughput can be observed. There are two reasons for the observed dependence. First, communication via multihop paths leads to a degradation of throughput. As described in (Marchang *et al.*, 2013), the authors conclude that path throughput is approximately proportional to the inverse of the number of hops. Second, the significant number of packets generated by the routing protocol leads to a further deterioration of the path throughput. This second reason explains the differences obtained by the tested protocols. The best result is obtained by the routing protocol HWMP, which generates the smallest number of routing packets. However, if the data traffic within the mesh network increases, the specified performance of the HWMP protocol decreases because each router sends a periodic PREQ for each active data transmission. All mesh participants forward this PREQ. The obtained results show that the routing protocols B.A.T.M.A.N. advanced IV and V should not be used inside a network with more than 36 routers, since the measured throughput is about 1/3 of the throughput in the same network with HWMP. The test fails for large networks by both protocols. The measured bandwidth also decreases by Babel. This is due to the growing number of updates needed to be transmitted when the network size increases.

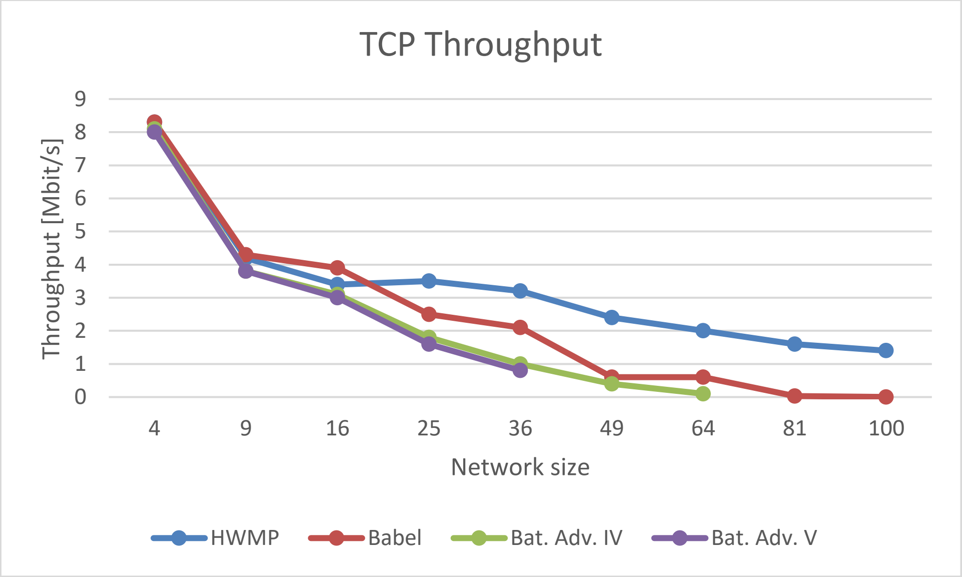


Figure 6.9: TCP throughput depending on the network size

In the second test series, the delay observed by the redirection of the network traffic is measured. This test aims to determine the effect of multiple failures regarding the computation of the communication route. The network topology used previously is maintained. An ICMP data transfer runs between R(1-1) and R(n-n). After a waiting time of 30s, the major part of the routers was disconnected so that only one path was available between both routers. This means the number of damages on the communication path increases with the network size. The time necessary for the router R(1-1) to find an alternative path was documented. The test was repeated ten times. Figure 6.10 shows the results. The best result is obtained by HWMP, with a recovery time under 2 s for a network size below 25 routers. This is due to the generated error messages after a router loss. No dependence could be detected between the path length (increasing with the network size) and the delay necessary for a path recovery for B.A.T.M.A.N. advanced V. By B.A.T.M.A.N. advanced IV, a considerable variation is detected, and the path recovery could not be observed in large networks. The recovery time is above 10s for the Babel protocol and increases with the network size.

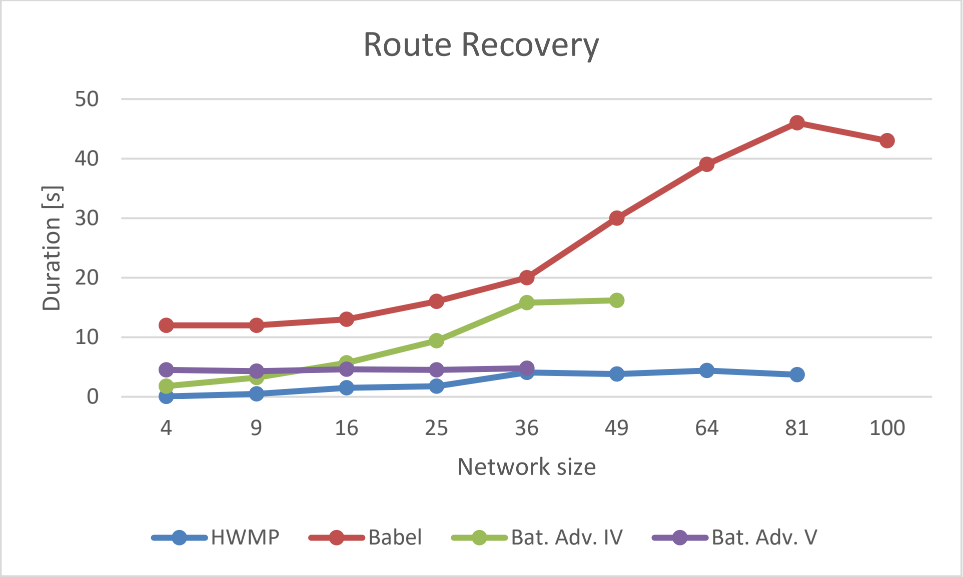
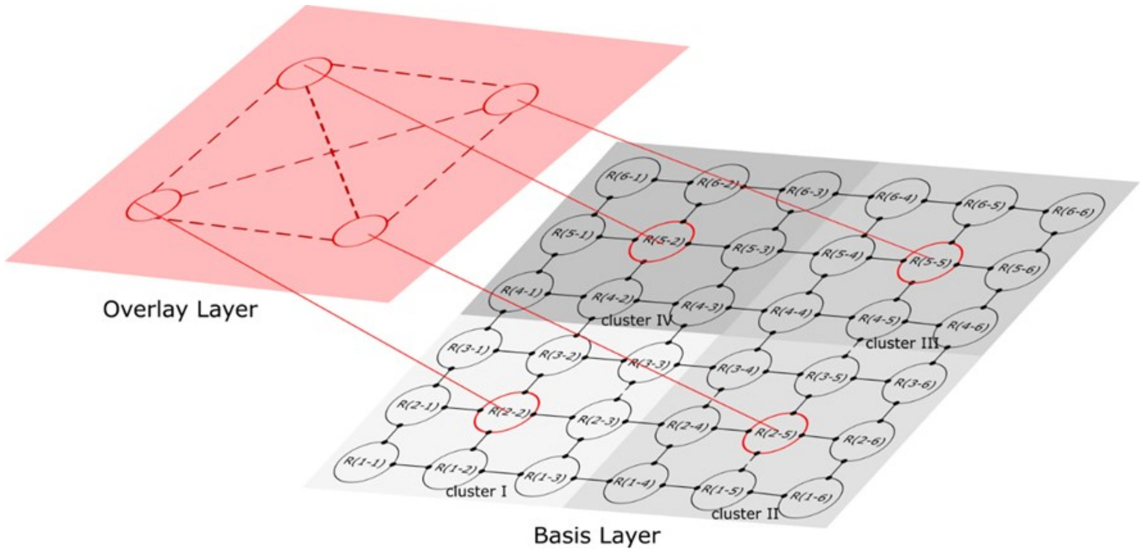


Figure 6.10: Duration of route recovery depending on the network size

6.2 Proposed Routing Solution

In Section 6.1, the performance of the routing protocols HWMP, Babel, B.A.T.M.A.N. advanced IV, and V was tested in several disaster relevant scenarios. According to the obtained results, HWMP shows the best performance regarding the dynamic requirement of routing protocol. However, the protocol cannot be used to build a large network like necessary for the communication after a disaster. This is due to the significant number of routing protocol packets generated in such a network. One solution can be to use a multiple cluster network like proposed in (Kaushal *et al.*, 2012). However, such a network has two major inconvenient: first, the hierarchical architecture is not desirable in disaster network due to the single point of failure and the need for a network administrator for the network configuration and second, the routers which are configured as Cluster Head (CH) require huge computing and network capacity because all the network traffic has to transit them.

This research work proposes a new network architecture to overcome the scalability and the load-balancing issue of the WMN routing protocol for disasters. The proposed architecture is shown in Figure 6.11 and consists of two layers (basis layer and overlay layer). The basis layer is built with wireless routers which run a layer 2 routing protocol (e.g., HWMP). On top of this, an overlay layer is implemented. It provides IP routing functionalities (e.g., using the Babel protocol). From the point of view of an IP router running on the overlay layer of the proposed architecture, the network is fully meshed. Nodes in this layer do not have to deal with link quality changes or hardware router loss. Each cluster builds a subnetwork. The benefits of the proposed network architecture will be discussed more in detail in the following subsections. Its advantages are presented by addressing two specific communication cases (Intra- and inter-cluster communication). In the last subsection, suggestions are made for realising the proposed architecture.



© 2017 IEEE

Figure 6.11: Optimised network architecture to solve routing issues in disaster scenarios (Tchinda *et al.*, 2017)

6.2.1 Intracluster communication

If a client connected to the router R(1-1) wants to communicate with another client connected to R(3-3) inside the same cluster/subnetwork, the communication is established using a layer 2 routing protocol. The first router can attach a cluster-id to each broadcasted frame, so that mesh nodes outside the cluster do not forward the generated frames. The proposed architecture is scalable because the generated broadcast frames are no longer forwarded by all mesh participants but only by routers inside the cluster. Each WMN node can save energy through the smaller number of transmitted routing packets, and the overall network throughput increases.

6.2.2 Intercluster communication

If a client connected to R(1-1) wants to communicate with a client connected to R(6-6), which is not part of its cluster/subnetwork, it first sends the packets to its gateway represented by R(2-2), which uses the proactive layer 3 routing protocol to forward the packets to the next IP router R(5-5). This can be considered as a one-hop communication in layer 3. The router R(2-2) creates a connection with the router R(6-6) on the MAC basis using the layer 2 protocol. The broadcast messages generated by routers hosting layer 3 routing functionalities like R(2-2) use the default cluster-id. Its broadcast messages are relayed by all mesh participants independent of their cluster. This means the layer 2 routing protocol (e.g., HWMP), which is implemented in the underlying layer of the proposed architecture, is responsible for the path establishment between R(2-2) and R(5-5). As shown in the previous Sections 6.1 the established path (e.g., using HWMP) takes care of the link throughput and can provide a quick answer to network changes like router loss. Furthermore, due to the resulting aggregation of the intercluster data stream (only one path is used for the communication between two clusters), the number of hardware routers used to transmit data packets is reduced, and new optimisation opportunities are created. One example can be to reduce the duration of the sleeping mode by routers, which participate in intercluster communication to improve the network throughput and increase the sleeping duration by other routers to save power. Another advantage of the proposed network architecture for intercluster communications is implementing multi-path communications. R(2-2) can send data packets to R(5-5) using two-hop paths in addition to the direct one. This can be used to increase the network throughput or reduce packet loss.

6.2.3 Proposed implementation

According to the results presented in this chapter, the choice of HWMP as layer 2 routing protocol working on the first layer of the proposed network architecture and Babel as layer 3 routing protocol working on the second layer can be a suitable solution. Furthermore, due to the full meshed nature of the overlay IP network, periodic Hello and IHU messages are no longer required. Additionally, the usage of technology like Network Function Virtualization (NFV) to implement routing functionalities on the second layer of the proposed network architecture can improve the network performance and increase the network life. For example, a Babel router, which represents the cluster head, can be implemented as a virtual network function. Its position in the cluster could be changed (live migration) depending on the router that generates the most important intercluster traffic or the remaining router energy. The migration of the cluster heads leads to a change in the selected routes for the intercluster communication and, therefore, a better distribution of the network load/power consumption. An NFV orchestrator has to be used to manage the network's dynamic configuration and build new clusters inside the WMN. The NFV orchestrator also allows a fast recovery when a mesh node running a Babel router shuts down unexpectedly.

6.3 Summary

This chapter tested the performance of the routing protocols HWMP, Babel, B.A.T.M.A.N. advanced IV, and V for disaster scenarios. This performance evaluation was conducted in a virtual environment implemented for this research work. The analysis shows that the protocols HWMP and B.A.T.M.A.N. advanced V consider the path data rate by their routing operations. However, none of the examined protocols considers the influence of existing data transfers and implements load balancing to improve the network capability. Concerning the protocol performance after dynamic processes like router loss, the routing protocol HWMP has shown the best results. Regarding the scalability of the routing protocols studied, the increase in overhead is unsuitable for a large network like necessary for the communication after some disaster events. This is due to the significant number of routing protocol packets generated in such a network. Section 6.2 proposes a two-layer solution to address the routing issue in large networks. The proposed solution reduces the routing protocol overhead by introducing clusters/subnetworks so that packets can now be addressed to a specific network segment. Furthermore, the proposed solution fulfils the service aware routing requirement introduced in Section 2.2 by allowing service specific optimisation on the overlay layer through load balancing of the intercluster communication or an adequate selection of the location for router hosting the virtual cluster head (e.g., router with the highest intercluster traffic).

The results of this chapter allow the following assumptions to be made for the rest of the thesis: first, the traffic generated by the routing protocol is negligible compared to the network data rate, even in large networks (see Section 6.2), and is therefore not considered in the optimisation in Chapter 7. Second, since the response time of the routing protocol in dynamic processes (e.g., 0.2s to find an alternative path after a router loss) is small compared to the time interval between two optimisations of the VNFs location in the network (e.g., 10min for the simulations in Chapter 7), it is assumed that all communication routes in the network are up to date during the optimisation. Third, in the simulations in Chapter 7, the communication routes are calculated based on the results in

Section 6.1. That means the route with the highest data rate is assumed for data transmission. This is also the case if there is existing data traffic over this route.

7 Energy-Efficient Placement of Virtual Network Functions

Reducing energy consumption in the Information and Communications Technology (ICT) sector is a growing challenge. In 2011, the energy consumption of this sector was estimated to be around 3% of the worldwide electricity consumption (Fagas *et al.*, 2017). To address this challenge, the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) demands a radical change in core networking technologies, devices, and network architectures (Matsubara *et al.*, 2013). In addition to this general effort of the research community, the optimisation of the energy consumption required and presented in this research work is principally motivated by the limited battery capacity of wireless routers used to build the ECN in a disaster scenario. This chapter has four significant contributions. Firstly, it provides a power consumption measurement for different VNFs used in disaster scenarios in Section 7.1. Secondly, the measured power consumptions are used to develop a power consumption model for the mesh network in the same section. Thirdly, four algorithms (an enumeration, random migration, multi-objectives evolutionary, and heuristic algorithm) are proposed to solve the VNFs placement problem in Section 7.2. Lastly, simulations are done to evaluate the proposed placement algorithms in Section 7.3. The evaluation compares the increase in the network lifetime, the difficulty level (number of tested network configurations), and the ability to deal with the existing constraints in WMN like the maximum medium usage in wireless communication. Section 7.4 concludes this chapter.

Part of this chapter has been submitted for publication in a journal and is under the review process.

7.1 Network Model

In Section 2.3, the requirements for the model were defined. Based on these, it was demonstrated that previous works formulations of the optimisation problem could not be applied to the specific scenario of a WMN in disaster in Section 3.4. This is due to unique characteristics such as the battery supply of the hardware, the shared wireless communication medium, the high dynamics of the WMN in comparison to wired network (e.g., link quality changes, mesh router loss), or the distribution of service requests, which have not been taken into account by the previous works. In this section, a mathematical model is developed that meets these requirements. For this purpose, the energy consumption of a mesh router is modelled in the first step.

7.1.1 VNF Energy Consumption Measurements

The authors in (Yang et al., 2017) and (Kaur et al., 2019) deal with the energy-efficient placement of VNFs in data centres and use a linear model for this. There, the energy consumption of a server depends linearly on the current CPU load and a constant base energy consumption. The CPU load in turn depends on the VNFs currently running on the server and the traffic they have to handle. For the energy consumption due to the forwarding of the data packets, a switch is assumed in (Farkiani et al., 2019) whose energy consumption depends on the number of active ports. In addition, there is a constant base energy consumption when the switch is on. In (Zhichao Xu et al., 2018), the authors instead assume that the energy consumption due to forwarding increases linearly with the traffic.

Whether a server-like model is applicable to small devices such as mesh routers has not been investigated yet. Moreover, in the proposed NFV optimised WMN, a mesh router combines server (hosting of VNFs) and forwarding (access point and routing) functionalities. To validate the model, the energy consumption of the following VNFs was measured: access point (AP), openvswitch (OVS), DHCP, DNS, web and call server. Figure 7.1 shows the measurement setup. The setup consists of a mini-PC configured as a mesh router, an ammeter for measuring the current and a constant voltage generator that generates a constant voltage of 12V. The Mini-PC is equipped with an Intel Pentium N4200 processor. The internal memory capacity is 8 GB, and an additional SSD card with a capacity of 260 GB has been installed. The Mini-PC is equipped with two WLAN modules from Compex (WLE600VX). This WLAN module uses the Qualcomm Atheros QCA9882 chipset and is capable of 2x2 MIMO in both 2.4 GHz and 5 GHz frequency ranges. The operating system Ubuntu Server 18.04 was installed on the Mini-PC.

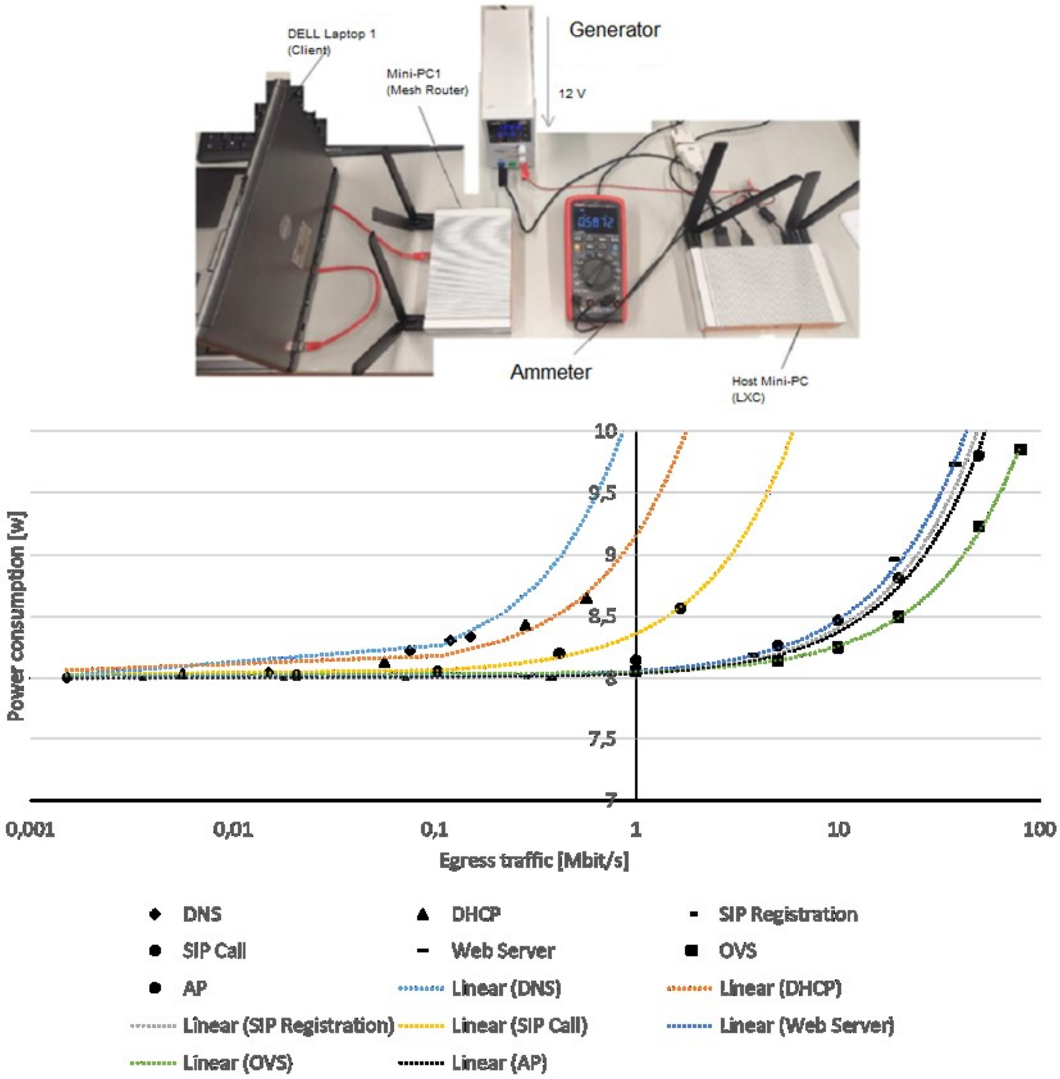


Figure 7.1: Measurement of the power consumption for different VNFs depending on the egress traffic

In the first series of measurements, the power consumption of the mesh router in idle mode was determined. This power consumption is the minimum power consumption of a router and corresponds to the energy required to keep the router in ON state. The current was measured for 12min after the start-up process was completed to determine its value. A value of 7.3W was measured.

The second series of measurements determined the power consumption for forwarding functions like AP and routing. By activating the WLAN interfaces, an increase in power consumption from 7.3 to 7.5W was measured for one interface and to 7.7W for two interfaces. This increase was independent of the configuration of the WLAN interface as a mesh or access point. Then the power consumption was measured as a function of the data rate of the traffic forwarded by AP or the OVS router. The powers were measured for the bit rates 1, 5, 10, 20, 50 and 80Mbit/s for 2 min each. Figure 7.1 shows the measured values. The measured power consumption shows a linear increase with the data rate for both OVS and AP functions. The coefficient of increase is 0.023Ws/Mbit and 0.034Ws/Mbit for OVS and AP, respectively. The energy consumption per Mbit/s is higher for the AP because it has to switch between transmit and receive mode. This is not the case with the OVS when two interfaces are used, and the data is only transmitted in one direction like in the tested scenario.

In the third series of measurements, the power consumption due to the processing of incoming service requests was determined. The measurements were realised for the following VNFs: DNS, DHCP, web, and call server. These VNFs were provided within Linux Containers (LXC). For each VNF, the power consumption was measured depending on the number of requests to be processed. For the call server, a distinction was made between registration and session setup. The size of the accessed web page on the webserver was 20Mbit. In this test, it was not possible to measure the power consumption of the VNFs independently of a forwarding function. For example, the power consumption of the web server was measured in combination with the AP needed to access the server. Since the highest power consumption is caused by sending and not by receiving data packets, Figure 7.1 shows the measured power consumption depending on the egress traffic in Mbit/s. The data traffic that is generated in response to a request (egress traffic) was determined with the help of the analysis tool wireshark. Each VNF had to handle 1, 10, 50, 80 and 100 requests/s. Generally, it can be observed that the power consumption increases linearly with the data traffic for each examined VNF. Furthermore, as expected, this increase is higher than with the AP because it could only be measured in combination with the AP. The smallest increase (0.041Ws/Mbit) was measured for user registration and the highest increase (2.320Ws/Mbit) for DNS.

7.1.2 Mathematical Formulation of the Optimisation Problem

In this research work, the WMN infrastructure is represented by a graph G, where the set of nodes (mesh routers) is annotated by $V(G)$ and the connections between them by $\mathrm{C}(G)$, respectively. Since there is no link with a fixed capacity within a WMN as in wired networks, $C(G)$ represents the set of clusters (mesh routers that are within range of each other and use the same channel for communication (see Chapter 5)). According to the measurements in the previous subsection, the power consumption of a mesh router at a specific time t, can be defined as follows: $P_v = P_{basic}(v) + P_{forwarding}(v) + P_{processing}(v)$. The basic power consumption $P_{basic}(v)$ has a constant value. $P_{forwarding}(v)$ and $P_{processing}(v)$ are linear functions from the current traffic that they process. This assumption can be made for a specific time slot Δt in which the state of the network can be considered constant. In this time slot, changes in the network infrastructure and the behavior of the users do not exist, and the energy efficiency can be reached through the minimisation of the total power consumption

$$min(Energy\ consumption) = min(\sum_{v \in V(G)} P_v\,\Delta t) \tag{7.1}$$

The second goal of the optimisation is to maximise the lifetime of the network. This can be reached through the minimisation of the residual energy variance by battery-powered nodes.

$$min(variance) \ = min(\sum_{v \in V(G)} (\bar{R} - R_v)^2) \tag{7.2}$$

$\bar{R}$ is the expected average residual energy at the end of the upcoming time interval Δt and R_v is the expected residual energy of router v. Both values depend on the chosen allocation for VNFs.

Besides these two optimisation objectives, the following constraints can be defined:

$$\sum_{j \in V(VNF)} \delta_v^j c(j) \leq c_{v,max} \tag{7.3}$$

$$m_C = sum\, diag(A_C.T_C) \leq 1 \tag{7.4}$$

$$\sum_{v \in V(G)} \delta_v^j = 1 \tag{7.5}$$

Equation (7.3) shows that the maximum capacity $c_{v,max}$ of the resources on a router must not be exceeded. $c(j)$ represents the resources required by the VNF j. δ_v^j is a binary number that is equal to 1 when the VNF j is running on the router v and 0 otherwise. $V(VNF)$ is the set of all VNFs. Equation (7.4) shows that the wireless medium usage m_C in a cluster C must not be overloaded. Here A_C is the inverse of the adjacency matrix where each column represents for a node the quality of connection with others cluster member in Mbit/s and is equal to 0 for node itself. T_C is the transmission matrix of the cluster. Each column in T_C represents for a node the traffic sends to other cluster members and is equal to zero for the node itself. Equation (7.5) shows that each VNF can only have one location in the network.

Figure 7.2 shows an example of a WMN consisting of seven routers $V(\mathrm{G}) = \{V1, V2, V3, V4, V5, V6, V7\}$ and two clusters $C(G) = \{C1, C2\}$. Packets can be transmitted between the routers with a maximum data rate of 80Mbit/s or 100Mbit/s depending on their distance. Assume that each router provides an access point function through which the end devices can connect. Assume that these end devices generate data traffic of 1 Mbit/s in the direction of a web server located on router V1. In response to these requests, the web server generates data traffic of 10 Mbit/s in the direction of the routers. This data traffic is forwarded via the shortest path in the network (see Figure 7.2). The medium usage of cluster $C1$ or cluster $C2$ can be calculated as follows:

$$m_{C1} = sum\ diag\left(\begin{pmatrix} 0 & \frac{1}{100} & \frac{1}{80} & \frac{1}{100} \\ \frac{1}{100} & 0 & \frac{1}{100} & \frac{1}{80} \\ \frac{1}{80} & \frac{1}{100} & 0 & \frac{1}{100} \\ \frac{1}{100} & \frac{1}{80} & \frac{1}{100} & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 4 & 1 \\ 10 & 0 & 0 & 0 \\ 40 & 0 & 0 & 0 \\ 10 & 0 & 0 & 0 \end{pmatrix}\right) = 0{,}77$$

$$m_{C2} = sum\ diag\left(\begin{pmatrix} 0 & \frac{1}{100} & \frac{1}{80} & \frac{1}{100} \\ \frac{1}{100} & 0 & \frac{1}{100} & \frac{1}{80} \\ \frac{1}{80} & \frac{1}{100} & 0 & \frac{1}{100} \\ \frac{1}{100} & \frac{1}{80} & \frac{1}{100} & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 1 & 1 \\ 10 & 0 & 0 & 0 \\ 10 & 0 & 0 & 0 \\ 10 & 0 & 0 & 0 \end{pmatrix}\right) = 0{,}3575$$

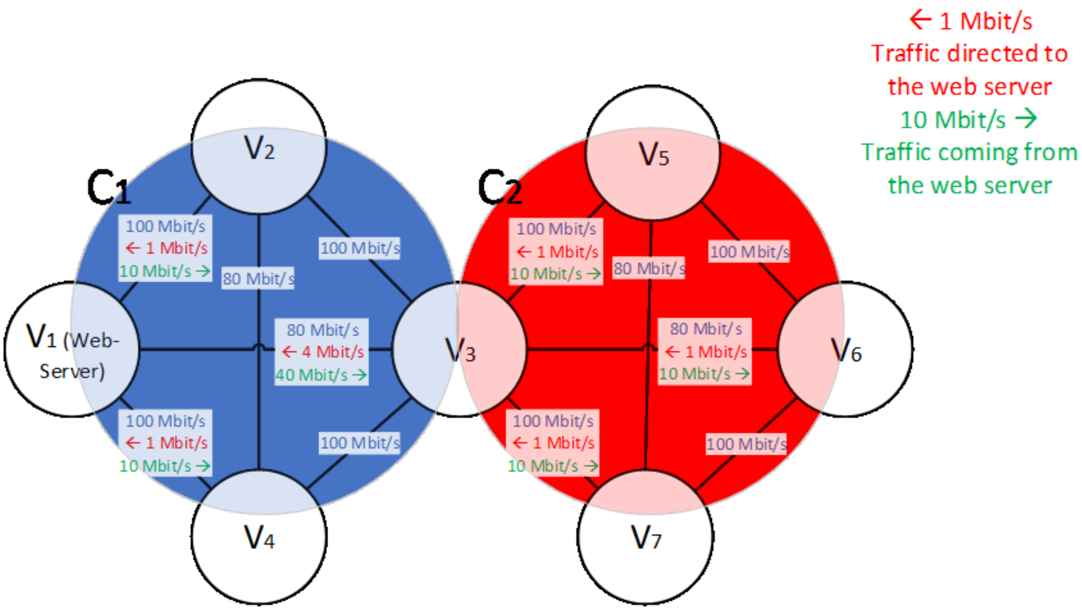


Figure 7.2: Example: Calculation of medium usage in a WMN with two clusters

7.2 Placement Algorithms

This section proposes four algorithms to address the placement of VNFs in WMN based on the mathematical formulation of the optimisation problem in Section 7.1.

7.2.1 Enumeration (BF)

Similar to a brute force search, all potential network configurations are sampled. For each network configuration, the objective functions (7.1) and (7.2) must be calculated, and the satisfaction of the constraints in equations (7.3) to (7.5) must be checked. Since this is a multi-objective optimisation problem, the correct solution consists of a list of pareto optimal network configurations (Deb *et al.*, 2002). These are all feasible configurations where a reduction in energy consumption can only be achieved by a worse distribution of the residual energy. The main disadvantage of this method is the high number of possible network configurations. This number increases exponentially with the number of VNFs s^n (where s is the number of mesh routers and n is the number of VNFs to be placed), because for each chosen location for a VNF, all possible positions for the other VNFs have to be checked depending on each other. As an example, in a network consisting of 100 routers, and where 8 VNFs have to be placed, there are 100^8 possible configurations. The enumeration method is therefore not applicable for large networks with a high number of VNFs. This algorithm will be referred to as "Brute Force (BF)" in the rest of the chapter.

7.2.2 Random Migration

The random migration of VNFs in the network is a procedure that, in many aspects, can be seen as the opposite of an exact procedure such as enumeration. While all possible network configurations are tested in the enumeration procedure, in random migration, the next location of each VNF is determined at random. The advantages of such a placement algorithm become more apparent with the example of a webserver that has to be placed in a WMN and has to handle equally distributed requests from the entire network. Due to the random migration of the webserver, the energy consumption due to the processing of the requests is evenly distributed across the network. Similarly, the energy consumption due to traffic forwarding is also distributed evenly across the network. As a result, in this scenario, the expected gain from the costly optimisation using the enumeration method is similar to the gain from the random migration of the webserver. This method is easily applicable in large networks with many VNFs because it does not require any calculation. Although the expected gain of the random migration in the previously described scenario is supposed to be similar to the gain by an elaborate optimisation using the enumeration method, the outcome is no longer trivial in case of unequal distributions of requests, time-dependent distribution of requests (e.g., due to the movement of helpers), or unequal distribution of residual energy. Furthermore, random migration does not check the fulfilment of constraints such as the available resources on hosting mesh routers.

7.2.3 Multi-Objectives Evolutionary Algorithm (MOEA)

The MOEAs offer a compromise between the elaborate enumeration method and the "possibly" inaccurate random migration of VNFs. These algorithms are inspired by processes in biology such as mutations, crossovers and selections. They are metaheuristics and can be applied to a whole range of problems. A widely used genetic algorithm is the so-called Nondominated Sorting Genetic Algorithm II (NSGA-II) (Deb *et al.*, 2002). To apply the NSGA-II algorithm, the population size and the number of generations must be specified. The working principle of the NSGA-II algorithm can be explained most simply with an example.

Suppose a webserver needs to be placed in a WMN that consists of 100 routers (see Figure 7.3 a)). The NSGA-II algorithm is used with a population size of 10 and a number of generations of 5. For the first generation, 10 out of 100 possible network configurations are chosen at random. Since the algorithm is elitist (not only the current generation but also the parent generation is needed to select the next generation), the algorithm can only start with selecting the second generation. The second generation is generated by applying the usual operators (mutation and crossover) to the first generation. Now that the first and second generations are known, the NSGA-II can be used to find the parents of the third generation. The objective functions in equations (7.1) and (7.2) are calculated for the first and second generations. The obtained results are sorted into several non-dominant fronts (first, second, ...) (see Figure 7.3 b)). Ten positions are selected as parents for the third generation. The selection starts with the first non-dominant front. Crowding distance is used for priority within the same front (Deb *et al.*, 2002). The third generation is obtained by mutations and crosses from the parents. The parents for the fourth generation are the result of selecting the third generation and its parents. This process is repeated until the desired number of generations is reached (in this case 5). A major advantage of NSGA-II is that the number of network configurations tested can be freely chosen by specifying the population size and the number of generations.

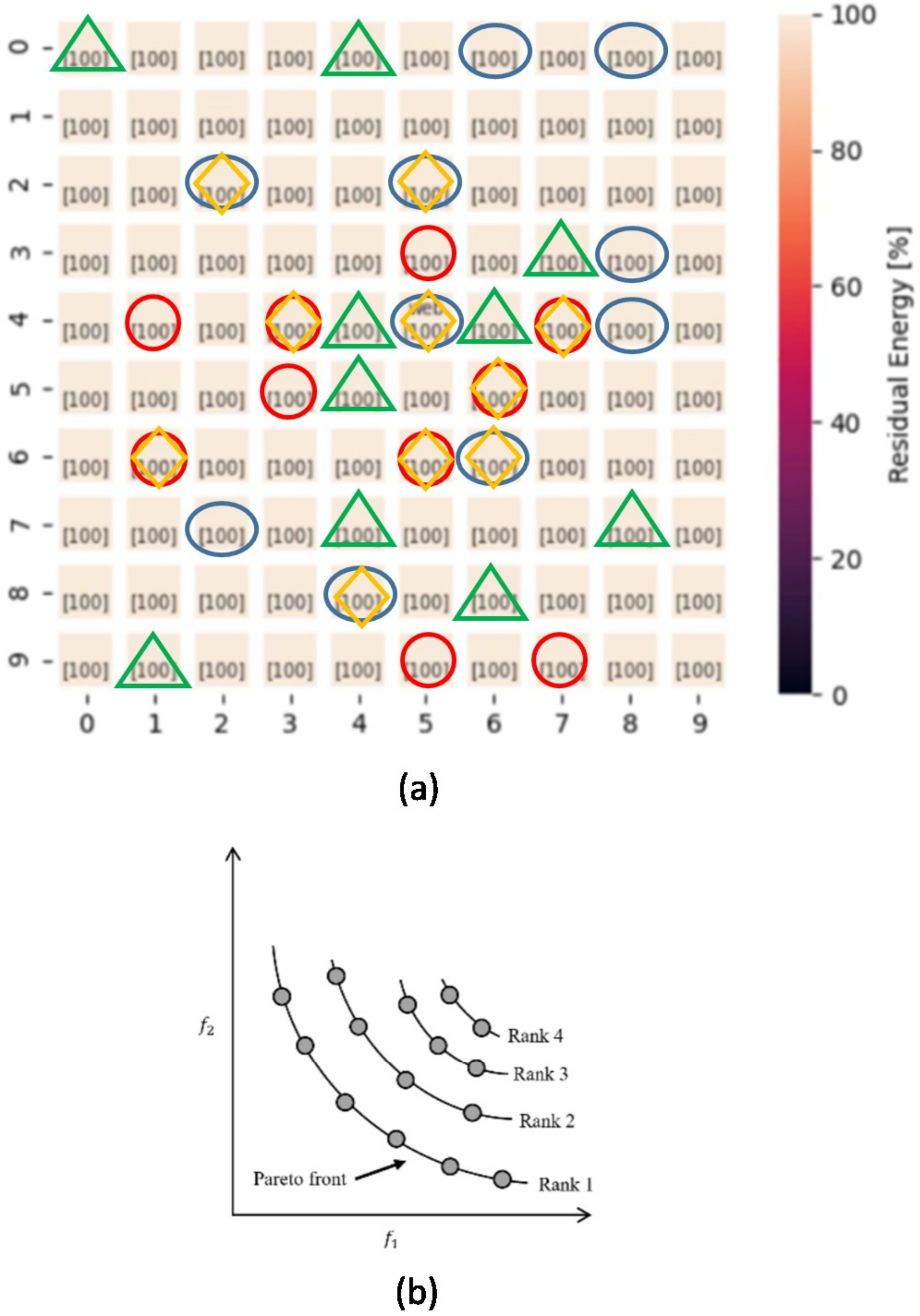


Figure 7.3: Illustration of the function of the NSGA-II algorithm (a) First (blue), second (red) and third (green) –generation and parents of the third generation (yellow); (b) First, second, third and fourth non-dominant front (Verma *et al.*, 2021)

7.2.4 Proposed Heuristic Algorithm

Besides metaheuristic algorithms such as NSGA-II, which can be applied to solve a whole class of problems, heuristic algorithms are developed to solve a specific problem. The last algorithm (Optimised Brute Force (OBF)) presented in this chapter belongs to this group. It was specifically designed to solve the problem of energy-efficient placement of VNFs in WMN. In order to find a suitable network configuration with little effort (few numbers of tested configurations), the optimisation problem in Section 7.1 is modified as follows:

Step 1: The objective functions in equations (7.1) and (7.2) are converted into constraints. The first objective of the optimisation is to minimise the energy consumption in equation (7.1). Since this is a linear equation, it is equivalent to minimising the energy consumption when placing the individual VNFs. Instead of minimising this energy consumption, allowable energy consumption is now defined for each VNF. This means that the minimisation of energy consumption over the entire network is now ensured by not exceeding the allowed energy consumption when placing the individual VNFs. The allowed energy consumption during the placement of a VNF is variable and depends on three main parameters. Among them is the number of requests it has to handle. The higher the number of requests, the higher the energy consumption for processing them. The second parameter is the type of VNF. The energy consumption of a webserver is different from that of a DHCP server. The third parameter that plays a role is the topology of the network (size and connectivity). The larger and more poorly connected a network, the more likely a packet will have to be forwarded before reaching the destination router. This thesis defines the permissible energy consumption for a VNF as follows.

$$E_{allowed} = OEC + \sum_{i} (I_i + E_i) \times L \times RoutCost \qquad (7.6)$$

Here, OEC is the energy consumption due to the processing of requests at the VNF and at the access points. It depends on the VNF type and the number of incoming requests (see parameter 1 and 2 above). However, it is independent of the network topology. L denotes the average path length (number of hops) in the network (see parameter 3). I_i respectively E_i is the ingress respectively egress data traffic to the VNF with the mesh router i as access respectively output router and $RoutCost$ is the energy consumption incurred by a router due to forwarding per data unit. Equation (7.6) allows to define a range around the optimal solution in which the energy consumption is acceptable. For example, assume a webserver needs to be placed in a WMN where all requests come from a single access point. The optimal solution would be to allocate the webserver on the router where the traffic is generated. The acceptable range for the webserver consists of all routers whose distance to this router is less than the average path length in the network. All other positions in the network belong to the existing solutions, which leads to too high energy consumption.

The second objective of the optimisation is to maximise the network's lifetime. As introduced in Section 7.1, this can be achieved by minimising the variance of the residual energies (see equation (7.2)). This objective function is now to be replaced by a limitation. For this purpose, a tolerable deviation from the average residual energy is defined. That means, during the optimisation, it is avoided that the residual energy of a router falls below a defined percentage of the average residual energy. This ensures indirectly that the variance of the residual energies remains low.

Step 2: The locations for the VNFs and, consequently, the tested network configurations are selected randomly. The probability P_i of a mesh router i being selected as a location for a VNF depends on the following parameters:

- Traffic to the VNF and traffic from neighbouring routers to the VNF (in the current implementation, both data traffic are weighted with 50 %). Routers with high data traffic or routers whose neighbours have high data traffic are preferred.
- The residual energy on the router. Routers with high residual energy are preferred. Their power consumption increases by choosing them more frequently as a location for the VNFs. As a result, their residual energy decreases, and so does the variance (see equation (7.2)).
- The congestion of the clusters over which the router communicates.

The probability of a router being chosen as a host for a VNF is therefore defined by the following equation (7.7). Where M is the average cluster usage: $M = \frac{1}{p}\sum_{C=1}^{p} m_C$ (m_C is the medium usage of the cluster C (see equation 7.4)). $m_{C1(i)}$ respectively $m_{C2(i)}$ is the medium usage of the cluster, which is reachable via interface 1 respectively 2, and I respectively E is the average ingress respectively egress traffic to the VNF.

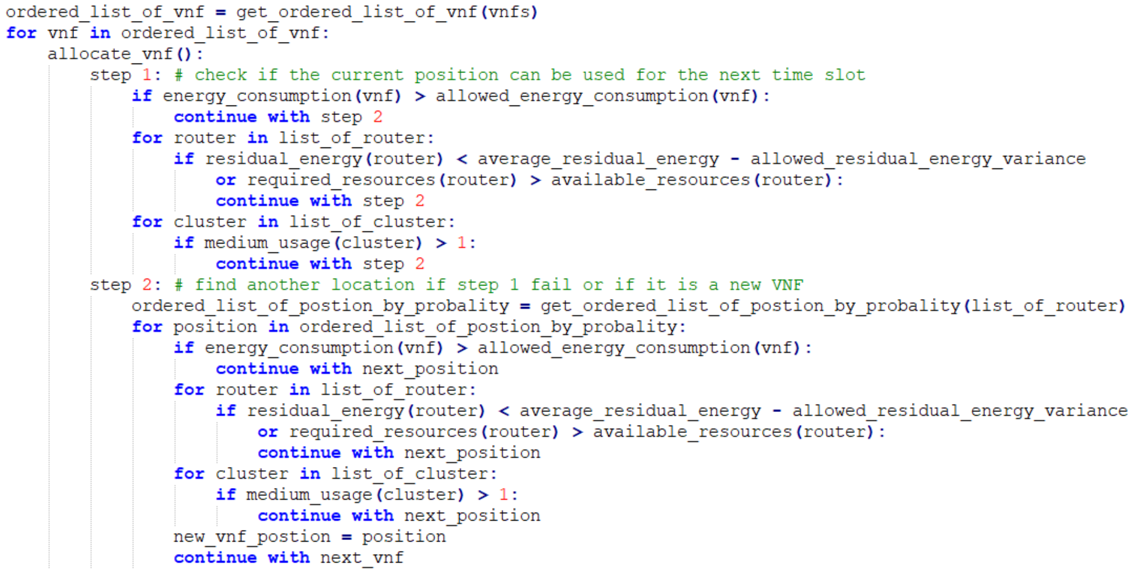
$$P_i = \left(1 + \frac{\frac{1}{2}(I_i + E_i) + \frac{1}{2} \times \frac{1}{m}\sum_{j=1}^{m}(I_j + E_j)}{I + E}\right) \times \left(\frac{R_i}{R}\right) \times \left(\frac{1 - m_{C1(i)}}{M}\right)\left(\frac{1 - m_{C2(i)}}{M}\right) \tag{7.7}$$

The optimisation is terminated when a solution is found that satisfies all the restrictions in step 1 and the constraints (7.3) to (7.5) in Section 7.1.

Using this algorithm, the VNFs are placed in the network independently of each other. They are first sorted according to their prioritisations. An example of prioritisation could be the expected amount of data processed by each VNF (VNFs with high traffic are placed first in the network). Another possibility would be to prioritise the VNFs according to the organisations or user groups to which they belong (services for helpers are placed first and those for affected people last). As a third possibility, a combination of both would also be considered. This combination was used for the simulations in Section 7.3.

For each VNF in the sorted list of VNFs, it is first checked whether the current location of the VNF can continue to be used. This is the case if the expected energy consumption at the current location is below the allowed value, the residual energy at no router falls below the allowed variance of the average residual energy due to the newly placed VNF, the current router has enough physical resources available such as CPU or memory and the expected medium usage is not overloaded at any cluster. If one of these conditions is not fulfilled (i.e., the previous position can no longer be used), or if it is a new service, the second step is to search for another location for the VNF. For this, the next possible position for the VNF is chosen randomly. The probability of each router being chosen is calculated using equation (7.7). The draw is repeated until a location is found where all conditions are fulfilled or until all locations in the network are tested (see Figure 7.4).

An important advantage of this algorithm is that the location of each VNF is tested for a maximum of the number s of routers that build the WMN. This results in a maximum number $n \times s$ of tested network configurations. Another advantage is that the optimisation can be stopped without all VNFs being placed. This is, for example, advantageous when the network is working at its limit. Only as many services are made available as the network allows. VNFs with a low priority are not placed in WMN if the resources are insufficient. The third advantage is that VNFs with a high priority are placed in the network in order of priority and do not have to wait until the end of the optimisation. In the further course of the work, this algorithm will be referred to as "Optimised Brute Force (OBF)".



```
ordered_list_of_vnf = get_ordered_list_of_vnf(vnfs)
for vnf in ordered_list_of_vnf:
    allocate_vnf():
        step 1: # check if the current position can be used for the next time slot
            if energy_consumption(vnf) > allowed_energy_consumption(vnf):
                continue with step 2
            for router in list_of_router:
                if residual_energy(router) < average_residual_energy - allowed_residual_energy_variance
                    or required_resources(router) > available_resources(router):
                    continue with step 2
            for cluster in list_of_cluster:
                if medium_usage(cluster) > 1:
                    continue with step 2
        step 2: # find another location if step 1 fail or if it is a new VNF
            ordered_list_of_postion_by_probality = get_ordered_list_of_postion_by_probality(list_of_router)
            for position in ordered_list_of_postion_by_probality:
                if energy_consumption(vnf) > allowed_energy_consumption(vnf):
                    continue with next_position
                for router in list_of_router:
                    if residual_energy(router) < average_residual_energy - allowed_residual_energy_variance
                        or required_resources(router) > available_resources(router):
                        continue with next_position
                for cluster in list_of_cluster:
                    if medium_usage(cluster) > 1:
                        continue with next_position
                new_vnf_postion = position
                continue with next_vnf
```

Figure 7.4: Pseudocode of the proposed heuristic algorithm

7.3 Evaluation

This section evaluates the algorithms for energy-efficient placement of VNFs in WMN presented in Section 7.2. For this purpose, different simulations are carried out. The simulations are done with the help of self-developed software in Python. The simulation of the energy consumption of a router is based on laboratory measurements in Section 7.1. The implementation of the MOEA solution uses the NSGA-II algorithm from the Platypus framework (Hadka, 2015). The MOEA algorithm is differentiated between MOEA50 and MOEA100. For MOEA50 and MOEA100, the population size and the number of generations are chosen so that the number of network configurations tested equals $\frac{n \times s}{2}$ and $n \times s$, respectively.

7.3.1 Maximum number of VNFs

The first simulation series is used to determine the maximum number of VNFs that can be placed in a WMN depending on the network size. To achieve this goal, it will first be determined how much time it takes to calculate a network configuration. This time depends not only on the network size but also on the current location of the VNF and the number of routers that are currently acting as entry or exit points for data traffic with the VNF.

Figure 7.5 shows the measured times as a function of network size for a single VNF. The assumption for the simulation is that each router serves as an entry or exit point for the data traffic. The values shown are the average of the measurements from all possible locations for the VNF.

Based on the measured times, it can be calculated how long it would take to determine the optimal network configuration. This results from multiplying the measured time for testing a configuration by the number of tested configurations. As an example, in a WMN with 100 routers and 8 VNFs, the enumeration respectively MOEA100 tests 100^8 Respectively 8×100 configurations. According to the measurement, testing a configuration in a WMN with 100 routers takes 0.0267s on average (simulation on a laptop without graphics card optimisation). This results in an expected computation time of 2.67×10^{14}s (approx. 8,466,514 years) respectively 21.36s if the enumeration method respectively the MOEA100 algorithm is used.

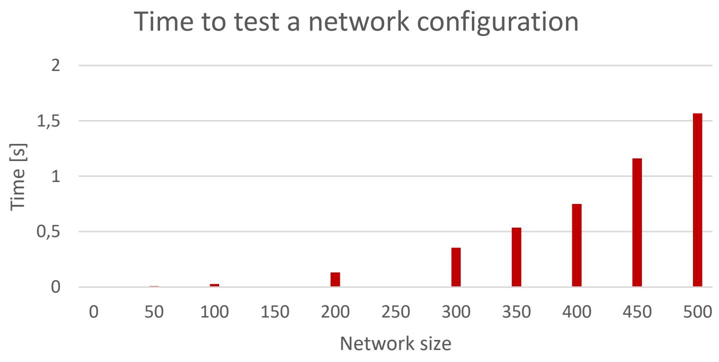


Figure 7.5: Time to test a network configuration

Figure 7.6 presents the expected computing time depending on the number of VNFs for different network sizes (50, 100, 200, and 400 routers) and the four algorithms proposed in Section 7.2. The horizontal line is the update interval from the network (e.g., 10min for the current simulation. During this time interval the state of the network is assumed to be static (no router loss, no link quality changes, …)). It corresponds to the maximum allowed computing time. A logarithmic scaling was used for a better presentation of the results. The following conclusions can be drawn from the diagrams:

- The exponential increase in the degree of difficulty (number of network configurations to be tested) leads to problems even in small networks, when using the enumeration method (BF) (e.g., in a network with 50 routers, the optimal network configuration for the placement of maximum 2 VNFs can be determined with this algorithm).
- The linear increase in the degree of difficulty of MOEA50, MOEA100, and the proposed heuristic algorithm (OBF) allows these algorithms to be used in large networks (e.g., in a network with 100 respectively 200 routers, the optimal network configuration for the placement of more than 100 VNFs, respectively 23 VNFs can be determined with MOE100 or with the heuristic algorithm).

However, it is found that even these algorithms are of limited use in networks with more than 200 routers (e.g., in a network with 400 routers, the optimal network configuration for the placement of a maximum of 2 VNFs can be determined with MOE100 or with the heuristic algorithm).

Now that it has been established that the proposed alternatives to the enumeration method can be calculated under the desired time limit, the next step is to determine the quality of the calculated network configurations.

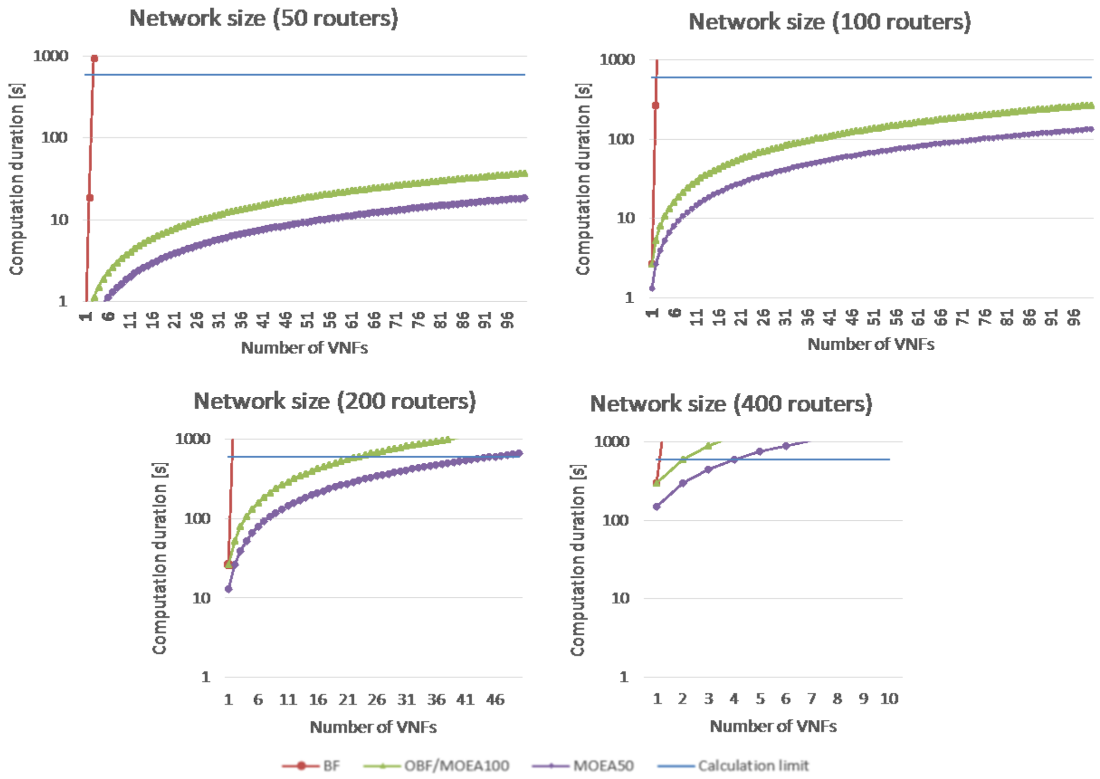


Figure 7.6: Influence of the number of VNFs on the estimated computer duration for network size

7.3.2 Influence of the Data Traffic

For the simulations, a WMN consisting of 100 routers is assumed. These routers are each equipped with two physical mesh interfaces to communicate with the neighbouring routers. A maximum transmission rate of 100Mbit/s is assumed between neighbouring routers in a row or column. Along a diagonal, the maximum transmission rate is 80Mbit/s.

In order to investigate the influence of data traffic on the performance of the algorithms for the energy-efficient placement of VNF, the optimal position for a webserver is identified over time. It is assumed that the webserver has to process 3,000 requests within 10 minutes, which are equally distributed over the entire network. The size of the requested website is 1, 7, and 20Mbit. This results in continuous data traffic of 5, 35, and 100Mit/s with the webserver. Figure 7.7 shows the results of the simulation. The gain (compare to the WMN without optimisation of the VNF placement) in network lifetime through optimisation depends strongly on the web page's size and thus on the traffic. For a small site (1Mbit), the gain is less than 2.2%. This gain increases and reaches 42.2% for a web page of size 20Mbit.

Furthermore, the simulation results do not show much difference between algorithms regarding lifetime gain. However, the difference between algorithms is found when looking at the cumulative number of tested configurations needed. This number is the same for enumeration and MOEA100 because a single VNF must be placed in the network. The number of tested configurations is 100 for each time interval for these algorithms and is independent of the traffic with the webserver. The slight decrease in the number of tested configurations with the increase in traffic seen in Figure 7.7 b) is due to the decrease in network lifetime with the increase in traffic (more energy is consumed for forwarding data). MOEA50 tests 50 positions per time interval. Therefore, the cumulative number of tested configurations is half of the number in MOEA100 and the enumeration method (BF). It is also observed that the actual required number of tested configurations in the proposed heuristic solution (OBF) is well below the maximum value of 100 per time interval (similar to MOEA100). As expected, this number increases with the increase in traffic because the high energy consumption at the current location more often leads to the need to determine a new position. With the random method, no network configuration needs to be tested. However, it is found that the probability of catching an unfavourable location during migration increases with the data traffic. For example, the random allocation leads to overloaded medium usage about 12% of the time when the web page's size is 20Mbit.

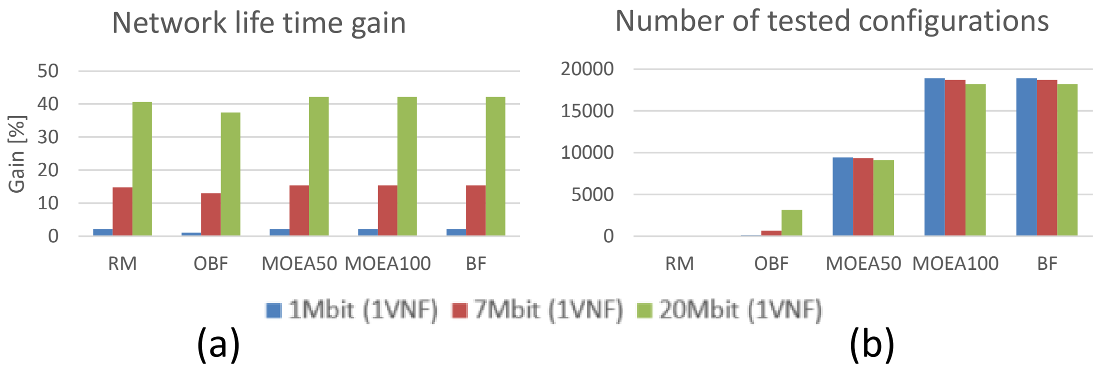
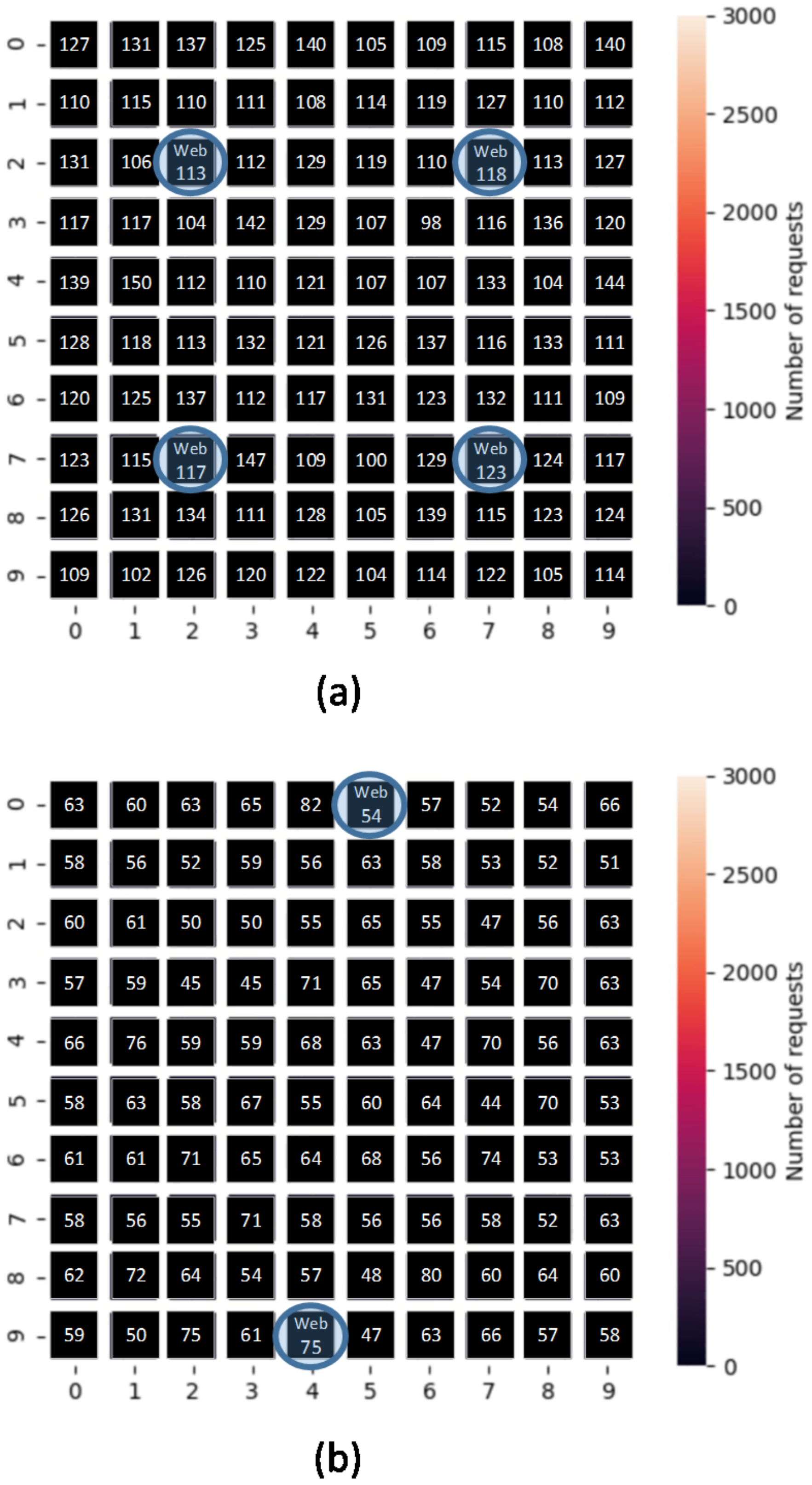


Figure 7.7: Influence of the data traffic on the performance of the proposed algorithms

7.3.3 Influence of the Number of VNFs

To investigate the influence of the number of VNFs on the performance of the algorithms, the placement of 4 respectively 2 VNFs in WMN is simulated (see Figure 7.8). To make the results more comparable with the placement of a single VNF in Subsection 7.3.3, the simulation assumes that the simulated VNFs are webservers, and each webserver has to process 3,000 requests within 10 minutes. These requests are equally distributed over the entire network (see Figure 7.8). The size of the requested web page is 7 respectively 20Mbit. If 4 respectively, 2 VNFs have to be placed in the network.



	0	1	2	3	4	5	6	7	8	9
0	127	131	137	125	140	105	109	115	108	140
1	110	115	110	111	108	114	119	127	110	112
2	131	106	Web 113	112	129	119	110	Web 118	113	127
3	117	117	104	142	129	107	98	116	136	120
4	139	150	112	110	121	107	107	133	104	144
5	128	118	113	132	121	126	137	116	133	111
6	120	125	137	112	117	131	123	132	111	109
7	123	115	Web 117	147	109	100	129	Web 123	124	117
8	126	131	134	111	128	105	139	115	123	124
9	109	102	126	120	122	104	114	122	105	114

(a)

	0	1	2	3	4	5	6	7	8	9
0	63	60	63	65	82	Web 54	57	52	54	66
1	58	56	52	59	56	63	58	53	52	51
2	60	61	50	50	55	65	55	47	56	63
3	57	59	45	45	71	65	47	54	70	63
4	66	76	59	59	68	63	47	70	56	63
5	58	63	58	67	55	60	64	44	70	53
6	61	61	71	65	64	68	56	74	53	53
7	58	56	55	71	58	56	56	58	52	63
8	62	72	64	54	57	48	80	60	64	60
9	59	50	75	61	Web 75	47	63	66	57	58

(b)

Figure 7.8: Influence of the Number of VNFs: User distribution and selected locations for the VNFs

Figure 7.9 a) shows the gain in network lifetime compared to service provision without migration of the VNFs. In the simulation of the standard case (without migration), the VNFs to be placed are distributed over the network as optimally as possible (Each VNF was placed in a network quadrant or network half (see Figure 7.8)). From the graph in Figure 7.9 a), it can be seen that the gain from migrating the VNFs decreases with the number of VNFs when the VNFs are optimally distributed across the network. This result can be explained by the better distribution of energy consumption across the network compared to the case with a single VNF. It is also observed in Figure 7.6 a) that the gain due to optimisation remains relatively high (about 13% when the size of the accessed web page is 7Mbit respectively 36% when the size of the accessed web page is 20Mbit). Finally, it can be observed from this graph that there is not much difference between the algorithms in terms of lifetime gain. In Figure 7.9 b), as expected, the number of tested network configurations increases linearly with the number of VNFs when MOEA50 or MOEA100 are applied. For example, the cumulative number of tested configurations increases by 383% respectively by 192% when the number of VNFs increases from 1 to 4 respectively 2. The measured increase in the number of tested configurations is less than 400% and 200% because it is a cumulative value. The total lifetime of the network becomes shorter with additional VNFs because more energy is consumed. For the proposed heuristic solution, the number of tested network configurations also increases with the number of VNFs. However, this number remains far below the maximum theoretical value 71,600 respectively 35,000 tested in MOEA100. For the random migration, the probability of an invalid network configuration increases with the number of VNFs. For example, approximately 49% of all configurations result in medium congestion in a WMN with two webservers and a web page size of 20Mbit. In a WMN with a single VNF, this number is around 12%.

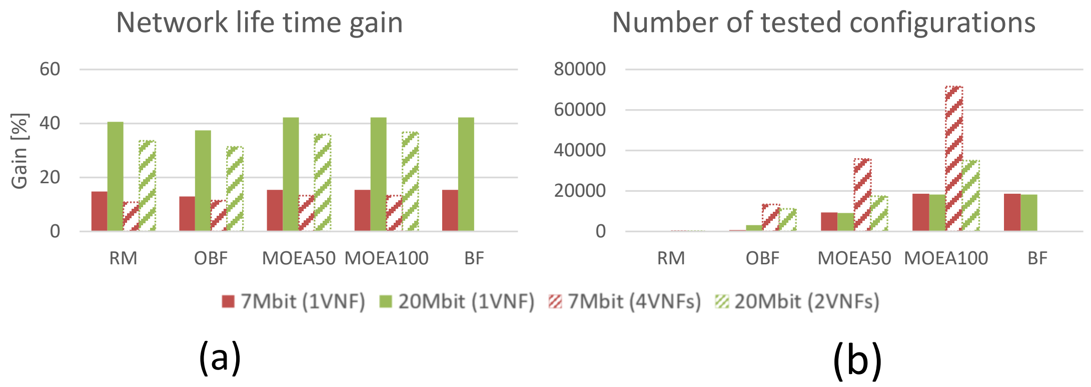


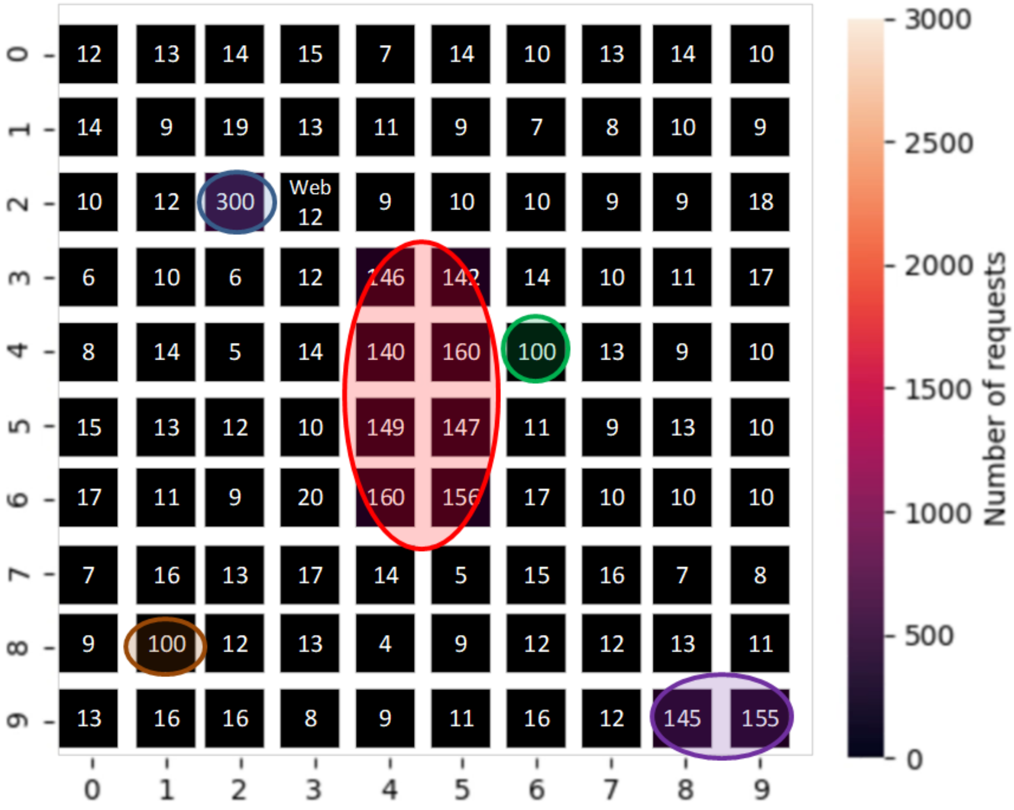
Figure 7.9: Influence of the number of VNFs on the performance of the proposed algorithms

7.3.4 Influence of the Distribution of Requests: Single VNF

Until now, the simulations have assumed that the requests to the VNF are equally distributed across the entire network. In practice, in the event of a disaster, there are densely populated and less densely populated areas, as well as severely affected and less severely affected areas. Due to these differences, there are also differences in the distribution of requests for a specific VNF. In this test series, the aim is to investigate how the unequal distribution of requests affects the performance of the algorithms. For this purpose, it is assumed that the 3,000 requests that have to be processed by the webserver in 10 minutes are distributed over five areas as follows (see Figure 7.10):

- City centre (8 routers): 1,200 requests;
- High-rise housing estate (1 router): 300 requests;
- Helper center (2 routers): 300 requests;

- Hospital (1 router): 100 requests;
- Railway station (1 router): 100 requests.



	0	1	2	3	4	5	6	7	8	9
0	12	13	14	15	7	14	10	13	14	10
1	14	9	19	13	11	9	7	8	10	9
2	10	12	300	Web 12	9	10	10	9	9	18
3	6	10	6	12	146	142	14	10	11	17
4	8	14	5	14	140	160	100	13	9	10
5	15	13	12	10	149	147	11	9	13	10
6	17	11	9	20	160	156	17	10	10	10
7	7	16	13	17	14	5	15	16	7	8
8	9	100	12	13	4	9	12	12	13	11
9	13	16	16	8	9	11	16	12	145	155

Figure 7.10: Helper distribution – Single VNF: City center (red), High-rise housing estate (blue), Helper center (purple), Hospital (brown), Railway station (green), and Rest of the city

The remaining requests are equally distributed over the rest of the area. The simulation is performed for a 7Mbit and a 20Mbit big website. Figure 7.11 a) shows the relative gain in lifetime compared to the service provision without optimisation. In general, the gain with optimisation in a WMN with unequally distributed requests (LD) is smaller than with equally distributed requests (ED). This is because the location of the webserver was optimally selected during the simulation. The webserver is therefore close to both the city center and the high-rise housing estate (see Figure 7.10). These two areas generate 1,500 requests. Because of this good location, less energy is consumed in the forwarding of packets. Figure 7.11 b) shows the cumulative number of tested network configurations. For MOEA50 and MOEA100, this number is independent of the distribution of the requests. The visible difference in the graph can be explained by the difference in the network's lifetime. A network with unequally distributed requests lives shorter because there is a non-optimisable energy consumption on the routers with more traffic due to the access point functionality. The number of tested network configurations becomes smaller in a WMN with unequally distributed requests when the proposed heuristic algorithm is used. This is because this algorithm uses the traffic as a parameter for selecting the location for the VNF. Finally, the probability of an invalid configuration with random migration increases from 12% to 17%.

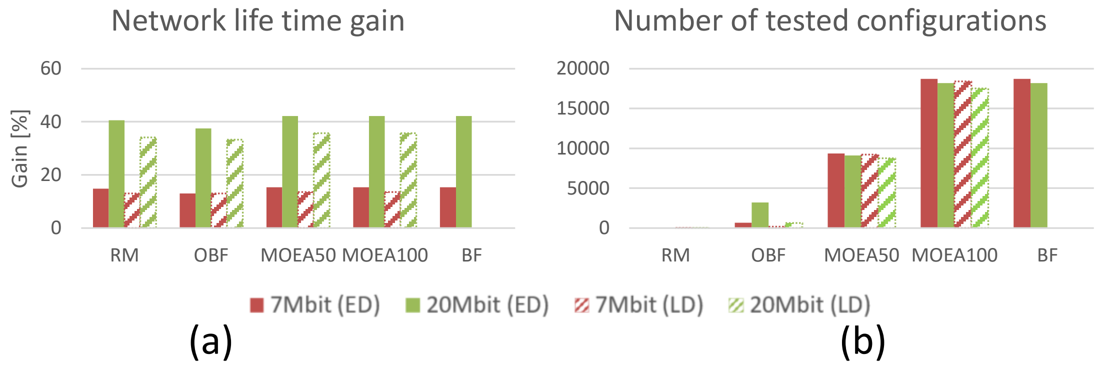


Figure 7.11: Influence of the distribution of requests on the performance of the proposed algorithms – Single VNF

7.3.5 Influence of the Distribution of Requests: Multiple VNFs

In Subsection 7.3.4, the influence of an unequal distribution of requests on the performance of the algorithms for the energy-efficient placement of VNFs in the WMN was investigated. The aim was to find the optimal location for a web server that processes requests from the entire network. In some cases, the number of requests for a particular service may be so high that a single VNF cannot handle them. This may be the case, for example, if there is no router with enough resources (e.g., CPU or memory) to host the VNF or if the traffic cannot be forwarded until the destination. In this case, additional VNFs are created, and the traffic is distributed between them. For example, suppose the webserver in the previous scenario now has to process 30,000 requests in 10 minutes instead of 3,000. This results in traffic of 350Mbit/s with the webserver when the requested page size is 7Mbit. The maximum transmission speed is 100Mbit/s in an empty cluster in the network. Therefore, this service cannot be provided by a single VNF. A possible solution to this problem would be to provide the service through 8 VNFs, each responsible for one area of the network as follows (see Figure 7.12):

- City centre (8 routers): 12,000 requests → 2 webservers for the northern and southern part;
- High-rise housing estate (1 router): 3000 requests → 1 webserver;
- Helper centre (2 routers): 3000 requests → 1 webserver;
- Hospital (1 router): 1000 requests → 1 webserver;
- Railway station (1 router): 1000 requests → 1 webserver.

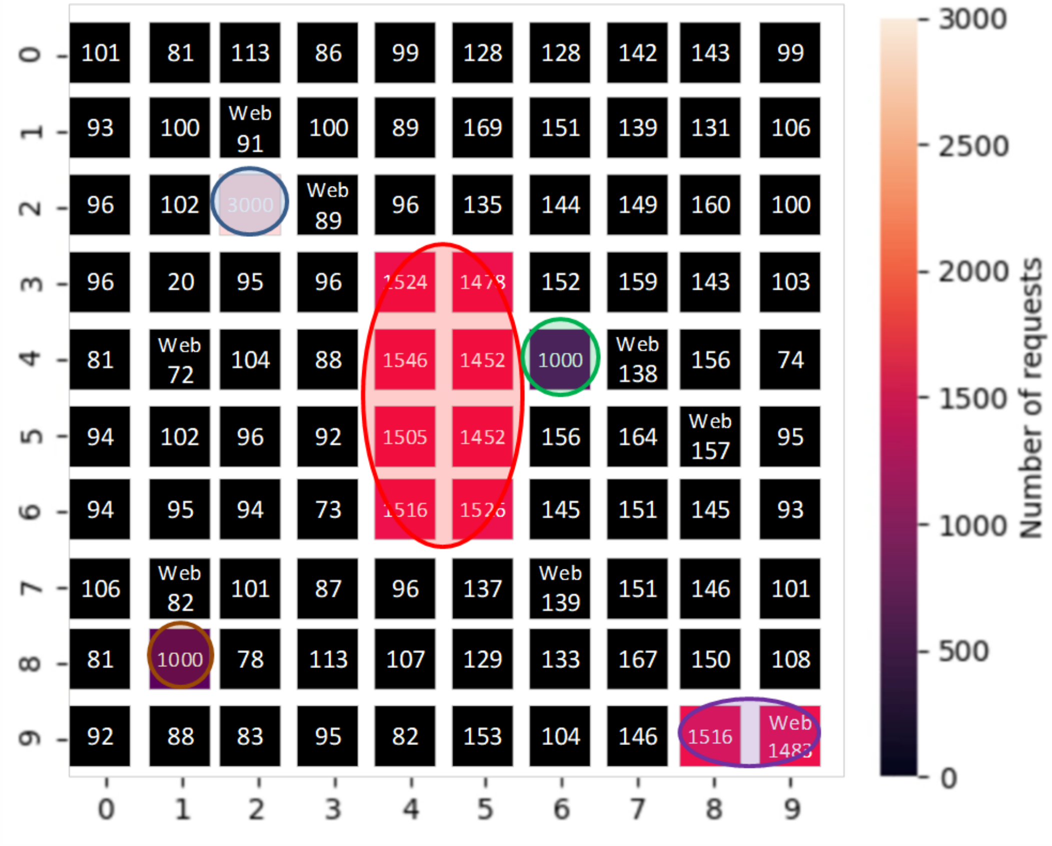


Figure 7.12: Helper distribution – Multiple VNFs: City center (red), High-rise housing estate (blue), Helper center (purple), Hospital (brown), Railway station (green), and Rest of the city

10,000 requests are generated in 10min, processed by two further webservers on the remaining area. One webserver is responsible for the eastern part of the network and one for the western part. Figure 7.13 a) shows the gain in network lifetime compared to the simulation without optimising the VNF locations. The locations of the VNFs were chosen as optimally as possible in the simulation without VNF migration to maximise the network lifetime. This means that they were placed as close as possible to the areas they are responsible for. Figure 7.13 a) shows that a gain of about 9% could be achieved by optimising with the proposed heuristic algorithm despite this optimal positioning. This gain is smaller for the MOEA solution but increases with the number of network configurations tested, from 6.5% for MOEA50 to 7.2% for MOEA100. The worst result is achieved with the random migration of VNFs. There the gain is only 2.2%. When randomly migrating VNFs in a network with unequally distributed requests, the energy consumption due to traffic forwarding increases if the VNFs are not placed near the locations with the most traffic.

Similarly, the high percentage of invalid network configurations is unsurprising. When random migration is used, about 96% of the configurations are invalid because they have clusters with overloaded medium usage. For the MOEA algorithm, the probability of having an invalid configuration at the end of the optimisation decreases with the number of configurations tested. As an example, it drops from 30.6% for MOEA50 to 19.6% for MOEA100. In this scenario, the heuristic algorithm alone provided valid network configurations at the end of each optimisation. Furthermore, the graph in Figure 7.13 b) shows that the actual number of tested configurations for the proposed heuristic solution (OBF) is 5.2% from the theoretical maximum value.

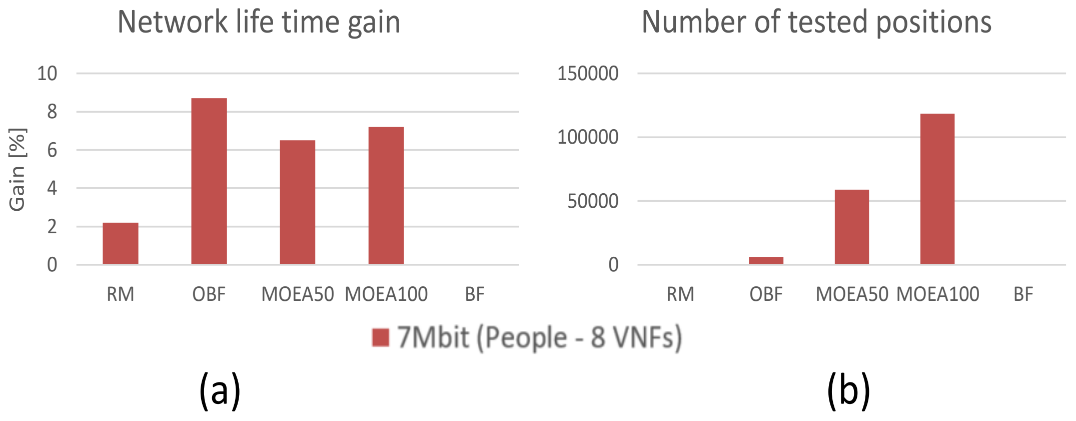


Figure 7.13: Influence of the distribution of requests on the performance of the proposed algorithms – Multiple VNFs

7.4 Summary

The goal of this chapter was to realise the placement of VNFs in a WMN in a more energy-efficient way. In Section 7.1, a model was developed by formulating the optimisation problem mathematically. The WMN was defined as a graph consisting of several subgraphs (clusters). This way, the two objective functions for the optimisation (minimisation of energy consumption and maximisation of network lifetime) and the constraints could be defined. In Section 7.2, four algorithms were proposed to solve the optimisation problem. The first algorithm is based on the enumeration method. The second algorithm implements a random migration of the VNFs after each time interval. The third algorithm is a multi-objective genetic algorithm (NSGA-II) applied in the literature to solve similar problems. Finally, a heuristic algorithm was developed specifically for this problem. The performance of these four algorithms was investigated in Section 7.3. Among other things, the influence of the number of VNFs, the influence of traffic and the influence of the distribution of service requests were investigated. While the results of the simulations for the enumeration method and the random migration of the VNFs show no surprises, the proposed heuristic algorithm performs significantly better than the MOEA algorithm for the same number of tested network configurations. This result can be explained as follows: If it is assumed that $f_1(\vec{x})$ is the first objective function that gives the total energy consumption depending on the current location of the VNFs $\vec{x}$ and $f_2(\vec{x})$ is the second objective function that gives the variance of the residual energy depending on the current location of the VNFs $\vec{x}$ in the network, the proposed heuristic solution can be considered as a mathematical function ($\vec{x} \rightarrow f_1, f_2$) which tries to select the VNFs positions $\vec{x}$ (e.g., based on the traffic or based on the residual energy) so that the resulting energy consumption f_1 and the resulting variance of the residual energy f_2 are above the allowed values. While the MOEA algorithm can be considered as a mathematical function (f_1, f_2 → $\vec{x}$) which based on the evaluation of the objectives functions f_1 and f_2, tries to guess the best possible placement for the VNFs $\vec{x}$. The problem is that parameters such as the residual energy of each router, the data traffic with the VNF, or the current load of the clusters are not considered. This complicates the process of finding a suitable network configuration.

8 Conclusion and Future Work

Section 8.1 of this chapter summarises the main findings of this thesis. Section 8.2 shows the limitations of the research conducted. Section 8.3 concludes this chapter by making suggestions for further optimising the ECN and presenting ideas for future work.

8.1 Achievements of the Research

This research aimed to realise an energy-efficient communication network to support rescue operations after disaster events. For this, the first step was to define the requirements for the ECN (see Chapter 2). These requirements can be divided into infrastructure and service requirements. Infrastructure requirements include the quick and easy deployment of the communication network, the complete coverage of the disaster area, the network access for most end devices, the QoS support for the provided services, the limited budget to build the network, and the fail-safety of the network infrastructure. The focus of the fail-safety requirement was on optimising energy consumption. This focus results from the observation that most of the devices that build the network in the event of a disaster are battery-powered. Optimising energy consumption is therefore an essential element in avoiding equipment failure due to insufficient residual energy. Service requirements refer to the network services and applications needed to communicate and support teams at the disaster site. These requirements include, among others, the scalability and fail-safe nature of the services provided, as well as the cost-effective and rapid integration of new services.

Chapter 3 was dedicated to projects and publications with the goal of building a disaster communication network. Both mesh- (SPIDER, NICER and SKYMESH) and non-mesh-based architectures (WISECOM, E-SPONDER and TetraMoD) were examined and compared with each other. This comparison was realised based on the requirements defined in chapter 2.

Since previous work could not fulfil the requirements of the ECN, a new network architecture was proposed in Chapter 4 to meet unaddressed or partially addressed requirements such as the failure safety of the network infrastructure or the scalability of the services provided. The proposed network architecture is an open network that multiple organisations can use simultaneously. It consists of a user, a core and, in some cases, a disaster safe segment located outside the disaster area. The core segment is a WMN consisting of wireless routers distributed in the field immediately after the disaster. The main novelty of this architecture is the integration with NFV. This integration enables the implementation of network services and applications as VNFs.

Since this work is the first to deal with the integration of NFV in a WMN, the optimisation of the WMN as NFVI was a core part of the realised research. Chapter 3, therefore, addressed the issue of limited data rate in WMN by investigating and comparing the existing CA strategies in multi-radio multi-channel WMN. The comparison was based on the following requirements: topology preserve, interference compliance, scalability and complexity, throughput, and wireless standard compliance. As the interference compliance and throughput requirements could not be evaluated by a literature review alone, measurements were carried out to determine the transmission and interference range of WLAN and the data rate in multi-hop communication. The results of these measurements are presented in Chapter 5. The outcome is that none of the existing link- and cluster-based CA strategies fulfil the above-mentioned requirements. Therefore, this thesis has proposed a cluster-based solution that meets these requirements by addressing issues such as the optimal cluster size or the optimal number of WLAN interfaces (see Chapter 5).

Another issue addressed by this work was the routing of packets in an NFV optimised WMN. Besides the allocation of channels, the routing protocol used is an important property that influences the performance of a WMN and thus its use as an NFVI. An important contribution of this thesis was the comparison of the routing protocols HWMP, Babel, B.A.T.M.A.N. advanced, ZRP, DSR, AODV, DSDV and OLSR for their use in WMN for disaster situations in Chapter 3. This comparison could be deepened in Chapter 6 by the emulation results on the example of the routing protocols HWMP, Babel, and B.A.T.M.A.N. advanced. The emulation was realised in a virtual environment, which was developed and tested within the scope of this thesis. As a result of the comparison, the protocol HWMP emerges as the winner because it fulfils the highest number of requirements. An important shortcoming of this protocol is that it cannot be used in large networks due to its overhead. Chapter 6, therefore, proposes a two-layer routing architecture, which in its first layer consists of clusters, using the routing protocol HWMP to determine the optimal communication path between cluster members. The IP-based overlay is used for communication between members of different clusters. It can be implemented with a Layer 3 routing protocol such as Babel or OVS to realise multi-layer switching. In addition, the architecture proposes to implement the IP routers on the overlay as VNFs so that their positions in the network can be optimised according to the router residual energy or the current network traffic.

The integration of NFVs in a WMN for disasters brings benefits and challenges. One of these challenges is the placement of VNFs. Since the location of a network function is no longer bound to physical hardware, it can be optimised to increase the energy efficiency of the network. Chapter 3, therefore, examined the publications that have dealt with the energy-efficient placement of VNFs in communication networks by comparing the models developed there with the requirements such as the limited energy supply of WLAN routers or the shared communication medium in WMN. As a result, it turned out that none of the previous formulations of the optimisation problem fit with the case of a WMN for disaster scenarios. Chapter 7 formulates the energy-efficient placement problem of VNFs in WMN mathematically as a multi-objective optimisation problem. In the same chapter, four algorithms were proposed to solve the problem so formulated. The performance of the four algorithms was tested in different disaster relevant scenarios. The heuristic algorithm developed in this thesis emerged from this performance comparison as the winner.

8.2 Limitations of the Research

The aim of this research work to develop an energy-efficient communication network for disaster situations could be fulfilled, as the summary in Subsection 8.1 shows. The proposed solution is modular. The concepts developed, such as the channel assignment procedure, can still be used when the technology is updated (e.g. IEEE802.11ax) or applied to non-WLAN based WMNs, such as the proposed algorithms for determining the optimal location for the VNFs. In this subsection, a few limitations of the proposed solution are listed:

1. The optimisation of energy consumption that has been realised in this work is limited to the optimisation of the placement of VNFs in WMN. To propose a complete solution, the optimisation must consider other aspects such as the energy-efficient routing of packets, the use of energy-efficient medium access methods, or energy-efficient hardware.
2. The optimisation of the WMN as an NFVI has focused on two important properties: the allocation of channels and the routing of packets. Besides these properties, there are other properties such as network coding or the use of directional antennas that influence the performance of a WMN. These properties are objects of current research and could not be considered within the scope of this work.
3. The investigation of routing protocols in Chapter 3 was limited to the most commonly used routing protocols. There are more than 100 different routing protocols for MANET in the literature (Junhai *et al.*, 2009; Ahmeda and Esseid, 2010; Dodke *et al.*, 2016; Lavanya *et al.*, 2017). Many of these protocols have only been defined in one paper, and no implementation exists for them. They have therefore been classified as not relevant for this research.
4. The comparison of algorithms for the energy-efficient placement of VNFs in WMN was tested based on self-defined scenarios. A better comparison would be possible with data from previous disaster events. Unfortunately, this data could not be found to the desired extent.
5. The monitoring of resources and its influence on energy consumption was only indirectly considered in the model because its contribution to the total energy consumption was assessed as negligible.

8.3 Suggestions and Future Work

Optimising the communication network through NFV integration has the potential to revolutionise the way services and applications are delivered in disasters by addressing existing challenges such as scalability, resilience or the cost-effective and rapid integration of new services. Further research needs to be conducted before this future vision becomes a reality. This subsection gives a list of suggestions for future work:

1. One of the main challenges of the proposed architecture is the management and orchestration of the NFVI and the VNFs. An orchestrator is needed for this task. This orchestrator must be decentralised to avoid the issue of a single point of failure. Appropriate communication mechanisms and areas of competence must be defined between its instances.
2. Another challenge and research question is the realisation of fail-safe services. This was simply assumed in the context of this work. Further research is needed to address this. One way to realise fail-safe services is through regular monitoring of the function of the provided services by the orchestrator. It can configure the backup functions in case of a failure quickly.
3. Another research question is securing communication resources such as data rates for certain user groups or applications. The data rate measurements and the resulting optimisation of the channel allocation process in Chapter 5 provide the basis for this. This can be realised, for example, through network slicing.
4. The fourth research question that needs to be addressed before deploying the proposed solution is the network's security. Since different organisations and affected people now use the network, it needs to be protected against external and

internal attacks. Appropriate authentication procedures must therefore protect access to the network, and concepts must be developed to prevent attacks such as denial of service.

References

Agarwal, S., Malandrino, F., Chiasserini, C. F. and De, S. (2019) 'VNF Placement and Resource Allocation for the Support of Vertical Services in 5G Networks', *IEEE/ACM Transactions on Networking*, 27(1), pp. 433–446. doi: 10.1109/TNET.2018.2890631.

Aguayo, D., Bicket, J. and Morris, R. (2005) 'SrcRR: A high throughput routing protocol for 802.11 mesh networks (DRAFT)'.

Ahmeda, S. S. and Esseid, E. A. (2010) 'Review of routing metrics and protocols for wireless mesh network', in *2010 Second Pacific-Asia Conference on Circuits, Communications and System*. IEEE, pp. 27–30. doi: 10.1109/PACCS.2010.5626819.

Akyildiz, I. F. and Xudong Wang (2005) 'A survey on wireless mesh networks', *IEEE Communications Magazine*, 43(9), pp. S23–S30. doi: 10.1109/MCOM.2005.1509968.

Alamsyah, Setijadi, E., Ketut Eddy Purnama, I. and Hery Pumomo, M. (2018) 'Performance Comparative of AODV, AOMDV and DSDV Routing Protocols in MANET Using NS2', in *2018 International Seminar on Application for Technology of Information and Communication*. IEEE, pp. 286–289. doi: 10.1109/ISEMANTIC.2018.8549794.

Ali, K., Nguyen, H. X., Quoc-Tuan Vien and Shah, P. (2015) 'Disaster management communication networks: Challenges and architecture design', in *2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*. IEEE, pp. 537–542. doi: 10.1109/PERCOMW.2015.7134094.

Alim Al Islam, A. B. M., Islam, M. J., Nurain, N. and Raghunathan, V. (2016) 'Channel Assignment Techniques for Multi-Radio Wireless Mesh Networks: A Survey', *IEEE Communications Surveys & Tutorials*, 18(2), pp. 988–1017. doi: 10.1109/COMST.2015.2510164.

Athota, K. and Negi, A. (2015) 'A topology preserving cluster-based channel assignment for wireless mesh networks', *Int. J. Commun. Syst.*, 28, pp. 1862–1883.

Baraković, S. and Baraković, J. (2010) 'Comparative performance evaluation of Mobile Ad Hoc routing protocols', in *The 33rd International Convention MIPRO*, pp. 518–523.

Bari, S. M. S., Anwar, F. and Masud, M. H. (2012) 'Performance study of hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s WLAN mesh networks', in *2012 International Conference on Computer and Communication Engineering (ICCCE)*. IEEE, pp. 712–716. doi: 10.1109/ICCCE.2012.6271309.

Barik, R. K., Lenka, R. K., Rao, K. R. and Ghose, D. (2016) 'Performance analysis of virtual machines and containers in cloud computing', in *2016 International Conference on Computing, Communication and Automation (ICCCA)*. IEEE, pp. 1204–1210. doi: 10.1109/CCAA.2016.7813925.

Belda, R., de Fez, I., Fraile, F., Murcia, V., Arce, P. and Guerri, J. C. (2008) 'Multimedia System for Emergency Services over TETRA-DVBT Networks', in *2008 34th Euromicro*

Conference Software Engineering and Advanced Applications. IEEE, pp. 142–149. doi: 10.1109/SEAA.2008.71.

Berioli, M., Courville, N. and Werner, M. (2007) ‘Emergency Communications over Satellite: the WISECOM Approach’, in *2007 16th IST Mobile and Wireless Communications Summit*. IEEE, pp. 1–5. doi: 10.1109/ISTMWC.2007.4299271.

de Boer, J. (1990) ‘Definition and classification of disasters: Introduction of a disaster severity scale’, *The Journal of Emergency Medicine*, 8(5), pp. 591–595. doi: https://doi.org/10.1016/0736-4679(90)90456-6.

Bradonjié, M. and Kong, J. S. (2007) ‘Wireless Ad Hoc Networks with Tunable Topology’, *Forty-Fifth Annual Allerton Conference, Allerton House, UIUC, Illinois, USA*.

Campana, T., Casoni, M., Marousis, A., Maliatsos, K. and Karagiannis, A. (2014) ‘E-SPONDER system: A new communication infrastructure for future emergency networks’, in *2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, pp. 136–143. doi: 10.1109/WiMOB.2014.6962162.

Centenaro, M., Vangelista, L., Zanella, A. and Zorzi, M. (2016) ‘Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios’, *IEEE Wireless Communications*, 23(5), pp. 60–67. doi: 10.1109/MWC.2016.7721743.

Chauhan, A. and Sharma, V. (2016) ‘Review of performance analysis of different routing protocols in MANETs’, in *2016 International Conference on Computing, Communication and Automation (ICCCA)*. IEEE, pp. 541–545. doi: 10.1109/CCAA.2016.7813779.

Chayapathi, R., Hassan, S. A. and Shah, P. (2016) ‘Network Functions Virtualization (NFV) with a Touch of SDN’, in.

Choi, N., Patel, M. and Venkatesan, S. (2006) ‘A Full Duplex Multi-channel MAC Protocol for Multi-hop Cognitive Radio Networks’, in *2006 1st International Conference on Cognitive Radio Oriented Wireless Networks and Communications*. IEEE, pp. 1–5. doi: 10.1109/CROWNCOM.2006.363465.

Chroboczek, J. (2011) ‘The Babel Routing Protocol’, *RFC*, 8966, pp. 1–54.

Clausen, T. H. and Jacquet, P. (2003) ‘Optimized Link State Routing Protocol (OLSR)’, *RFC*, 3626, pp. 1–75.

Compex Systems (2021) ‘WLE600VX: Dual Band 5GHz 2x2 MIMO 802.11ac Mini PCIe WiFi Module: Designed for Dual Band Wireless Access Points’.

Deb, K., Pratap, A., Agarwal, S. and Meyarivan, T. (2002) ‘A fast and elitist multiobjective genetic algorithm: NSGA-II’, *IEEE Transactions on Evolutionary Computation*, 6(2), pp. 182–197. doi: 10.1109/4235.996017.

Delock (2022) ‘WLAN cable: Delock RP-SMA Buchse zum Einbau > MHF/U.FL kompatibler Stecker 200 mm 1.37’.

Dijkstra, E. W. (1959) ‘A note on two problems in connexion with graphs’, *Numerische Mathematik*, 1(1), pp. 269–271. doi: 10.1007/BF01386390.

Docker (2022) *Empowering App Development for Developers | Docker*. Available at: https://www.docker.com/ (Accessed: 9 March 2022).

Dodke, S., Mane, P. B. and Vanjale, M. S. (2016) 'A survey on energy efficient routing protocol for MANET', in *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*. IEEE, pp. 160–164. doi: 10.1109/ICATCCT.2016.7911984.

Draves, R., Padhye, J. and Zill, B. (2004) 'The architecture of the link quality source routing protocol'.

Dugan, J., Elliott, S., Mah, B. A., Poskanzer, J. and Prabhu, K. (2022) *iPerf - The TCP, UDP and SCTP network bandwidth measurement tool*. Available at: https://iperf.fr/ (Accessed: 9 March 2022).

ETSI GS NFV 002 (2013) *Network Functions Virtualization (NFV); Architectural Framework v1.1.1*. Available at: http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf.

ETSI ISG NFV (2012) *Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action. Issue 1.*

EUR-Lex (2005) *EUR-Lex - 32005D0513 - EN - EUR-Lex*. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32005D0513 (Accessed: 30 March 2022).

EUR-Lex (2007) *EUR-Lex - 32007D0090 - EN - EUR-Lex*. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007D0090 (Accessed: 30 March 2022).

Fagas, G., Gammaitoni, L., Gallagher, J. P. and Paul, D. J. (2017) 'ICT - Energy Concepts for Energy Efficiency and Sustainability', in.

Fazli, E. H., Werner, M., Courville, N., Berioli, M. and Boussemart, V. (2008) 'Integrated GSM/WiFi Backhauling over Satellite: Flexible Solution for Emergency Communications', in *VTC Spring 2008 - IEEE Vehicular Technology Conference*. IEEE, pp. 2962–2966. doi: 10.1109/VETECS.2008.312.

Freifunk (2022) *freifunk.net - Freifunk steht für freie Kommunikation in digitalen Datennetzen*. Available at: https://freifunk.net/en/ (Accessed: 23 February 2022).

Frick, G., Tchinda, A. P., Shala, B., Trick, U., Lehmann, A. and Ghita, B. (2019) 'Requirements for a Distributed NFV Orchestration in a WMN-Based Disaster Network', in *2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*. IEEE, pp. 1–6. doi: 10.1109/ICT-DM47966.2019.9032953.

Garcia, J.-E., Kallel, A., Kyamakya, K., Jobmann, K., Cano, J.-C. and Manzoni, P. (2003) 'A novel DSR-based energy-efficient routing algorithm for mobile ad-hoc networks', in *2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No.03CH37484)*. IEEE, pp. 2849-2854 Vol.5. doi: 10.1109/VETECF.2003.1286127.

Gupta, P. and Kumar, P. R. (2000) 'The capacity of wireless networks', *IEEE*

Transactions on Information Theory, 46(2), pp. 388–404. doi: 10.1109/18.825799.

Gwalani, S., Belding-Royer, E. M. and Perkins, C. E. (2003) ‘AODV-PA: AODV with path accumulation’, in *IEEE International Conference on Communications, 2003. ICC ’03*. IEEE, pp. 527–531. doi: 10.1109/ICC.2003.1204232.

Haas, Z. J. and Pearlman, M. R. (1998) ‘The zone routing protocol (zrp) for ad hoc networks" intemet draft’, in.

Hadka, D. (2015) *Platypus - Multiobjective Optimization in Python — Platypus documentation*. Available at: https://platypus.readthedocs.io/en/latest/ (Accessed: 20 March 2022).

Halpern, J. M. and Pignataro, C. (2015) ‘Service Function Chaining (SFC) Architecture’, *RFC*, 7665, pp. 1–32.

Huang, J.-S. and Lien, Y.-N. (2012) ‘Challenges of emergency communication network for disaster response’, in *2012 IEEE International Conference on Communication Systems (ICCS)*. IEEE, pp. 528–532. doi: 10.1109/ICCS.2012.6406204.

IEEE (2002) ‘IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)’, *IEEE Std 802.15.1-2002*, pp. 1–473. doi: 10.1109/IEEESTD.2002.93621.

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

International Telecommunication Union (ITU) (2013) ‘Technical Report on Telecommunications and Disaster Mitigation’, Version 1. Available at: Technical Report on Telecommunications and Disaster Mitigation.

Jahir, Y., Atiquzzaman, M., Refai, H., Paranjothi, A. and LoPresti, P. G. (2019) ‘Routing protocols and architecture for disaster area network: A survey’, *Ad Hoc Networks*, 82, pp. 1–14. doi: https://doi.org/10.1016/j.adhoc.2018.08.005.

Jekyll (2020) *Mac80211_hwsim to generate virtual wireless NIC*. Available at: https://linuxtut.com/en/221ca606ffb0a656dfe2/ (Accessed: 28 March 2022).

Jia, J. and Zhang, Q. (2007) ‘Hardware-Constrained Multi-Channel Cognitive MAC’, in *IEEE GLOBECOM 2007-2007 IEEE Global Telecommunications Conference*. IEEE, pp. 4653–4658. doi: 10.1109/GLOCOM.2007.883.

Jiang, M. (1999) ‘Cluster based routing protocol (CBRP)’, in.

Jin-Man Kim and Jong-Wook Jang (2006) ‘AODV based Energy Efficient Routing Protocol for Maximum Lifetime in MANET’, in *Advanced Int’l Conference on Telecommunications and Int’l Conference on Internet and Web Applications and Services (AICT-ICIW’06)*. IEEE, pp. 77–77. doi: 10.1109/AICT-ICIW.2006.49.

Johnson, D. B., Maltz, D. A. and Broch, J. (2001) ‘DSR: the dynamic source routing protocol for multihop wireless ad hoc networks', in.

Jouni, M. (2008) *mac80211_hwsim - software simulator of 802.11 radio(s) for mac80211 — The Linux Kernel documentation*. Available at: https://www.kernel.org/doc/html/latest/networking/mac80211_hwsim/mac80211_hwsim.html (Accessed: 8 March 2022).

Junhai, L., Danxia, Y., Liu, X. and Mingyu, F. (2009) 'A survey of multicast routing protocols for mobile Ad-Hoc networks', *IEEE Communications Surveys & Tutorials*, 11(1), pp. 78–91. doi: 10.1109/SURV.2009.090107.

Kaur, K., Garg, S., Kaddoum, G., Gagnon, F. and Jayakody, D. N. K. (2019) 'EnLoB: Energy and Load Balancing-Driven Container Placement Strategy for Data Centers', in *2019 IEEE Globecom Workshops (GC Wkshps)*. IEEE, pp. 1–6. doi: 10.1109/GCWkshps45667.2019.9024592.

Kaushal, D., Niteshkumar, A. G., Prasann, K. B. and Agarwal, V. (2012) 'Hierarchical Cluster Based Routing for Wireless Mesh Networks Using Group Head', in *2012 International Conference on Computing Sciences*. IEEE, pp. 163–167. doi: 10.1109/ICCS.2012.38.

Ko, B.-J., Misra, V., Padhye, J. and Rubenstein, D. (2007) 'Distributed Channel Assignment in Multi-Radio 802.11 Mesh Networks', in *2007 IEEE Wireless Communications and Networking Conference*. IEEE, pp. 3978–3983. doi: 10.1109/WCNC.2007.727.

Kunz, T. (2008) 'Energy-Efficient Variations of OLSR', in *2008 International Wireless Communications and Mobile Computing Conference*. IEEE, pp. 517–522. doi: 10.1109/IWCMC.2008.90.

Kyasanur, P. and Vaidya, N. H. (2006) 'Routing and link-layer protocols for multi-channel multi-interface ad hoc wireless networks', *ACM SIGMOBILE Mobile Computing and Communications Review*, 10(1), pp. 31–43. doi: 10.1145/1119759.1119762.

Lavanya, P., Reddy, V. S. K. and Prasad, A. M. (2017) 'Research and survey on multicast routing protocols for MANETs', in *2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. IEEE, pp. 1–4. doi: 10.1109/ICECCT.2017.8117929.

Lehmann, A., Tchinda, A. P. and Trick, U. (2016) 'Optimization of Wireless Disaster Network through Network Virtualization', in *INC*.

Li, C., Hu, R., Sawaf, A. H. El and Li, Z. (2019) 'A Framework for Constructing Service Function Chaining Systems Based on Segment Routing', in.

Lin, C.-Y., Shu-Hsien Lu and Tseng, Y.-C. (2011) 'A channel management protocol for multi-channel, single-radio 802.11-based wireless mesh networks', in *2011 IEEE 16th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, pp. 26–30. doi: 10.1109/CAMAD.2011.5941111.

Liu, Z. and Wu, W. (2010) 'A Dynamic Multi-radio Multi-channel MAC Protocol for Wireless Sensor Networks', in *2010 Second International Conference on Communication Software and Networks*. IEEE, pp. 105–109. doi: 10.1109/ICCSN.2010.19.

Makram, S. A. and Gunes, M. (2008) 'Distributed channel assignment for multi-radio wireless mesh networks', in *2008 IEEE Symposium on Computers and Communications*. IEEE, pp. 272–277. doi: 10.1109/ISCC.2008.4625737.

Mamechaoui, S., Didi, F. and Pujolle, G. (2013) 'A Survey on Energy Efficiency for Wireless Mesh Network', *International journal of Computer Networks & Communications*, 5(2), pp. 105–124. doi: 10.5121/ijcnc.2013.5209.

Marchang, J., Ghita, B. and Lancaster, D. (2013) 'Hop-Based dynamic fair scheduler for wireless Ad-Hoc networks', in *2013 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, pp. 1–6. doi: 10.1109/ANTS.2013.6802873.

Marina, M. K. and Das, S. R. (no date) 'On-demand multipath distance vector routing in ad hoc networks', in *Proceedings Ninth International Conference on Network Protocols. ICNP 2001*. IEEE Comput. Soc, pp. 14–23. doi: 10.1109/ICNP.2001.992756.

Matsubara, D., Egawa, T., Nishinaga, N., Kafle, V. P., Shin, M.-K. and Galis, A. (2013) 'Toward future networks: A viewpoint from ITU-T', *IEEE Communications Magazine*, 51(3), pp. 112–118. doi: 10.1109/MCOM.2013.6476874.

Mijumbi, R., Serrat, J., Gorricho, J.-L., Bouten, N., De Turck, F. and Boutaba, R. (2016) 'Network Function Virtualization: State-of-the-Art and Research Challenges', *IEEE Communications Surveys & Tutorials*, 18(1), pp. 236–262. doi: 10.1109/COMST.2015.2477041.

Molisch, A. F. (2011) *Wireless Communications*. 2nd edn. Wiley Publishing.

Morshed, M. M., Ko, F. I. S., Lim, D., Rahman, M. H., Rahman Mazumder, M. R. and Ghosh, J. (2010) 'Performance evaluation of DSDV and AODV routing protocols in Mobile Ad-hoc Networks', in *4th International Conference on New Trends in Information Science and Service Science*, pp. 399–403.

Nan, H., Hyon, T.-I. and Yoo, S.-J. (2007) 'Distributed Coordinated Spectrum Sharing MAC Protocol for Cognitive Radio', in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*. IEEE, pp. 240–249. doi: 10.1109/DYSPAN.2007.39.

Naveed, A., Kanhere, S. S. and Jha, S. K. (2007) 'Topology Control and Channel Assignment in Multi-Radio Multi-Channel Wireless Mesh Networks', in *2007 IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems*. IEEE, pp. 1–9. doi: 10.1109/MOBHOC.2007.4428629.

Nelson, C. B., Steckler, B. D. and Stamberger, J. A. (2011) 'The Evolution of Hastily Formed Networks for Disaster Response: Technologies, Case Studies, and Future Trends', in *2011 IEEE Global Humanitarian Technology Conference*. IEEE, pp. 467–475. doi: 10.1109/GHTC.2011.98.

Nemeth, B., Molner, N., Martinperez, J., Bernardos, C. J., De la Oliva, A. and Sonkoly, B. (2021) 'Delay and reliability-constrained VNF placement on mobile and volatile 5G infrastructure', *IEEE Transactions on Mobile Computing*, pp. 1–1. doi: 10.1109/TMC.2021.3055426.

NFV White Paper (2012) *Network Functions Virtualisation: An Introduction, Benefits,* *Enablers, Challenges & Call for Action. Issue 1.*

Nguyen, T. A. B., Englert, F., Farr, S., Gottron, C., Bohnstedt, D. and Steinmetz, R. (2015) ‘Hybrid communication architecture for emergency response — An implementation in firefighter’s use case’, in *2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*. IEEE, pp. 524–529. doi: 10.1109/PERCOMW.2015.7134092.

NICER (2022) *Networked Infrastructureless Cooperation for Emergency Response*. Available at: https://www.nicer.tu-darmstadt.de/en/nicer/overview/ (Accessed: 16 February 2022).

Okada, H., Oka, H. and Mase, K. (2012) ‘Network construction management for emergency communication system SKYMESH in large scale disaster’, in *2012 IEEE Globecom Workshops*. IEEE, pp. 875–880. doi: 10.1109/GLOCOMW.2012.6477691.

Open-Mesh (2022a) *BATMAN V - batman-adv - Open Mesh*. Available at: https://www.open-mesh.org/projects/batman-adv/wiki/BATMAN_V (Accessed: 17 March 2022).

Open-Mesh (2022b) *Doc-overview - batman-adv - Open Mesh*. Available at: https://www.open-mesh.org/projects/batman-adv/wiki/Doc-overview (Accessed: 15 March 2022).

Owczarek, P. and Zwierzykowski, P. (2013) ‘ROUTING PROTOCOLS IN WIRELESS MESH NETWORKS -A COMPARISON AND CLASSIFICATION’, in, pp. 85–95. doi: 10.13140/RG.2.1.3321.2646.

Paguem Tchinda, A., Lehmann, A. and Trick, U. (2016) ‘Untersuchung von Wireless Mesh Network-Routing-Protokollen für den Einsatz in Netzen für Katastrophengebiete’, *Berlin: VDE Verlag GmbH*, (ITG-Fachtagung (2016), Osnabrück).

Perkins, C. E., Belding-Royer, E. M. and Das, S. R. (2003) ‘Ad hoc On-Demand Distance Vector (AODV) Routing’, *RFC*, 3561, pp. 1–37.

Perkins, C. E. and Bhagwat, P. (1994) ‘Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers’, *Proceedings of the conference on Communications architectures, protocols and applications*.

Portmann, M. and Pirzada, A. A. (2008) ‘Wireless Mesh Networks for Public Safety and Crisis Management Applications’, *IEEE Internet Computing*, 12(1), pp. 18–25. doi: 10.1109/MIC.2008.25.

Quinn, P., Elzur, U. and Pignataro, C. (2018) ‘Network Service Header (NSH)’, *RFC*, 8300, pp. 1–40.

Raniwala, A. and Chiueh, T. (2005) ‘Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network’, *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, 3, pp. 2223–2234 vol. 3.

Reina, D. G., Toral, S. L., Barrero, F., Bessis, N. and Asimakopoulou, E. (2011) ‘Evaluation of Ad Hoc Networks in Disaster Scenarios’, in *2011 Third International Conference on Intelligent Networking and Collaborative Systems*. IEEE, pp. 759–764.

doi: 10.1109/INCoS.2011.86.

Rethfeldt, M., Raddatz, H., Beichler, B., Konieczek, B., Timmermann, D., Haubelt, C. and Danielis, P. (2016) 'ViPMesh: A virtual prototyping framework for IEEE 802.11s wireless mesh networks', in *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, pp. 1–7. doi: 10.1109/WiMOB.2016.7763263.

RND (2021) *Hochwasser: Bundeswehr beendet Einsatz nach Flutkatastrophe – noch 86 Soldaten vor Ort*. Available at: https://www.rnd.de/politik/hochwasser-bundeswehr-beendet-einsatz-nach-flutkatastrophe-noch-86-soldaten-vor-ort-YG5AW7IPD4K3PYYMO5ASQHIYKU.html (Accessed: 14 March 2022).

Sbeiti, M., Goddemeier, N., Behnke, D. and Wietfeld, C. (2016) 'PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks', *IEEE Transactions on Wireless Communications*, 15(3), pp. 1950–1964. doi: 10.1109/TWC.2015.2497257.

Sbeiti, M., Pojda, J. and Wietfeld, C. (2012) 'Performance evaluation of PASER - An efficient secure route discovery approach for wireless mesh networks', in *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*. IEEE, pp. 745–751. doi: 10.1109/PIMRC.2012.6362883.

Selvi, K. T. (2014) 'The secured OLSR protocol for MANET', in *International Conference on Information Communication and Embedded Systems (ICICES2014)*. IEEE, pp. 1–6. doi: 10.1109/ICICES.2014.7033969.

Seo, K.-H., Park, J. W., Oh, S., Hahm, J. and Suh, J. (2017) 'Requirement analysis of simulator-based integration for disaster response robots', in *2017 17th International Conference on Control, Automation and Systems (ICCAS)*. IEEE, pp. 1295–1299. doi: 10.23919/ICCAS.2017.8204406.

Singh, M., Lee, S. G., Kit, T. W. and Huy, L. J. (2011) 'Cluster-based routing scheme for Wireless Mesh Networks', in *13th International Conference on Advanced Communication Technology (ICACT2011)*, pp. 335–338.

Skalli, H., Ghosh, S., Das, S. and Lenzini, L. (2007) 'Channel Assignment Strategies for Multiradio Wireless Mesh Networks: Issues and Solutions', *IEEE Communications Magazine*, 45(11), pp. 86–95. doi: 10.1109/MCOM.2007.4378326.

So, J. and Vaidya, N. H. (2004) 'Multi-Channel Mac for Ad Hoc Networks: Handling Multi-Channel Hidden Terminals Using a Single Transceiver', in *Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. New York, NY, USA: Association for Computing Machinery (MobiHoc '04), pp. 222–233. doi: 10.1145/989459.989487.

Soualah, O., Mechtri, M., Ghribi, C. and Zeghlache, D. (2017) 'Energy Efficient Algorithm for VNF Placement and Chaining', in *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*. IEEE, pp. 579–588. doi: 10.1109/CCGRID.2017.84.

Souza Couto, R., Secci, S., Mitre Campista, M. and Maciel Kosmalski Costa, L. (2014) 'Network design requirements for disaster resilience in IaaS clouds', *IEEE Communications Magazine*, 52(10), pp. 52–58. doi: 10.1109/MCOM.2014.6917402.

Stojmenovic, I. and Xu Lin (no date) ‘Power-aware localized routing in wireless networks’, in *Proceedings 14th International Parallel and Distributed Processing Symposium. IPDPS 2000*. IEEE Comput. Soc, pp. 371–376. doi: 10.1109/IPDPS.2000.846008.

Subik, S., Rohde, S., Weber, T. and Wietfeld, C. (2010) ‘SPIDER: Enabling interoperable information sharing between public institutions for efficient disaster recovery and response’, in *2010 IEEE International Conference on Technologies for Homeland Security (HST)*. IEEE, pp. 190–196. doi: 10.1109/THS.2010.5655061.

Suzuki, H., Kaneko, Y., Mase, K., Yamazaki, S. and Makino, H. (2006) ‘An Ad Hoc Network in the Sky, SKYMESH, for Large-Scale Disaster Recovery’, in *IEEE Vehicular Technology Conference*. IEEE, pp. 1–5. doi: 10.1109/VTCF.2006.496.

Tajiki, M. M., Salsano, S., Chiaraviglio, L., Shojafar, M. and Akbari, B. (2019) ‘Joint Energy Efficient and QoS-Aware Path Allocation and VNF Placement for Service Function Chaining’, *IEEE Transactions on Network and Service Management*, 16(1), pp. 374–388. doi: 10.1109/TNSM.2018.2873225.

Talooki, V., Marques, H., Rodriguez, J., Agua, H., Blanco, N. and Campos, L. (2010) ‘An Energy Efficient Flat Routing Protocol for Wireless Ad Hoc Networks’, in *2010 Proceedings of 19th International Conference on Computer Communications and Networks*. IEEE, pp. 1–6. doi: 10.1109/ICCCN.2010.5560058.

Tamilarasi, M., Chandramathi, S. and Palanivelu, T. G. (2008) ‘Overhead reduction and energy management in DSR for MANETs’, in *2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE ’08)*. IEEE, pp. 762–766. doi: 10.1109/COMSWA.2008.4554513.

Tchinda, A. P., Frick, G., Trick, U., Lehmann, A. and Ghita, B. (2020) ‘High Throughput WMN for the Communication in Disaster Scenario’, in *2020 World Conference on Computing and Communication Technologies (WCCCT)*. IEEE, pp. 53–63. doi: 10.1109/WCCCT49810.2020.9170007.

Tchinda, A. P., Frick, G., Trick, U., Lehmann, A., Tchinda, A. P. and Ghita, B. (2017) ‘Performance analysis of WMN routing protocols for disaster networks’, in *2017 IEEE Symposium on Communications and Vehicular Technology (SCVT)*. IEEE, pp. 1–6. doi: 10.1109/SCVT.2017.8240309.

UN/ISDR (2004) *On-Line Conference: Priority Areas to Implement Disaster Risk Reduction*. Available at: https://www.unisdr.org/2004/wcdr-dialogue/terminology.htm (Accessed: 30 March 2022).

Valenzuela, R. A. (1996) ‘Antennas and propagation for wireless communications’, in *Proceedings of Vehicular Technology Conference - VTC*. IEEE, pp. 1–5. doi: 10.1109/VETEC.1996.503396.

Verma, S., Pant, M. and Snasel, V. (2021) ‘A Comprehensive Review on NSGA-II for Multi-Objective Combinatorial Optimization Problems’, *IEEE Access*, 9, pp. 57757–57791. doi: 10.1109/ACCESS.2021.3070634. https://creativecommons.org/licenses/by/4.0/

Viriyasitavat, W., Xu, L. Da and Viriyasitavat, W. (2014) ‘Compliance Checking for

Requirement-Oriented Service Workflow Interoperations', *IEEE Transactions on Industrial Informatics*, 10(2), pp. 1469–1477. doi: 10.1109/TII.2014.2301132.

Wildman, J. and Weber, S. (2016) 'On protocol and physical interference models in Poisson wireless networks'. Available at: http://arxiv.org/abs/1609.05314.

Wmediumd (2022) 'Bcopeland Wireless Medium Simulator (wmediumd)'. Available at: https://github.com/bcopeland/wmediumd.

Wolff, A. H. (2013) *Entwurf und Leistungsbewertung von Ad-hoc-Kommunikationsnetzen für den Katastrophenschutz*. Available at: http://dx.doi.org/10.17877/DE290R-5731.

Wolff, A., Sbeiti, M. and Wietfeld, C. (2012) 'Performance evaluation of process-oriented wireless relay deployment in emergency scenarios', in *2012 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, pp. 000651–000654. doi: 10.1109/ISCC.2012.6249371.

Xu Li, Wu Zi-wen and Zheng Bao-yu (no date) 'TPBDSR: a new DSR-based energy saving routing in MANET', in *2003 International Conference on Computer Networks and Mobile Computing, 2003. ICCNMC 2003.* IEEE Comput. Soc, pp. 470–473. doi: 10.1109/ICCNMC.2003.1243093.

Xu, Z., Zhang, X., Yu, S. and Zhang, J. (2018) 'Energy-Efficient Virtual Network Function Placement in Telecom Networks', in *2018 IEEE International Conference on Communications (ICC)*. IEEE, pp. 1–7. doi: 10.1109/ICC.2018.8422879.

Yang, K., Zhang, H. and Hong, P. (2016) 'Energy-Aware Service Function Placement for Service Function Chaining in Data Centers', in *2016 IEEE Global Communications Conference (GLOBECOM)*. IEEE, pp. 1–6. doi: 10.1109/GLOCOM.2016.7841805.

Yarali, A., Ahsant, B. and Rahman, S. (2009) 'Wireless Mesh Networking: A Key Solution for Emergency &#x00026; Rural Applications', in *2009 Second International Conference on Advances in Mesh Networks*. IEEE, pp. 143–149. doi: 10.1109/MESH.2009.33.

Yaron, S. (2017) *networking:generic_netlink_howto [Wiki]*. Available at: https://wiki.linuxfoundation.org/networking/generic_netlink_howto (Accessed: 9 March 2022).

Yi, J., Cizeron, E., Hamma, S. and Parrein, B. (2008) 'Simulation and Performance Analysis of MP-OLSR for Mobile Ad Hoc Networks', in *2008 IEEE Wireless Communications and Networking Conference*. IEEE, pp. 2235–2240. doi: 10.1109/WCNC.2008.395.

Appendix A – Abbreviations

3G	3rd Generation Mobile Network
4G	4th Generation Mobile Network
5G	5th Generation Mobile Network

A

AODV	Ad hoc On-Demand Distance Vector Routing
AOMDV	On-demand Multipath Distance Vector
AP	Access Point

B

B.A.T.M.A.N. advanced	Better Approach to Mobile Ad hoc Networking advanced
BF	Brute Force
BMBF	German Federal Ministry of Education and Research

C

COTS	Commercial Off-The-Shelf
CA	Collision Avoidance
CA	Channel Assignment
CBCA	Cluster-Based Channel Assignment
CCA	

CH	Cluster Head
CoMTaC	Cluster-based Multipath Topology control and Channel assignment scheme
CPU	Central Processing Unit
CSMA	Carrier Sense Multiple Access

D

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSDV	Destination-Sequenced Distance-Vector
DSR	Dynamic Source Routing
DVB-T	Digital Video Broadcasting – Terrestrial
DYMO	Dynamic MANET On-demand

E

ETSI	European Telecommunications Standards Institute
ECN	Emergency Communication Network
EE-TCA	Energy Efficient Tree search-based Chain placement Algorithm
ETSI	European Telecommunications Standards Institute
ETX	Expected Transmission Count
EU	European Union

F

FR	First Responders
FRUs	First Responder Units

G

H

HWMP	Hybrid Wireless Mesh Protocol

I

IAA	Interference Avoidance Algorithm
IARP	Intra-zone Routing Protocol
ICMP	Internet Control Message Protocol
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IERP	Inter-zone Routing Protocol
IHU	I-Heard-You
ILP	Integer Linear Programming
IoT	Internet of Things
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISG	Industry Specification Group

IT	Information Technology
ITU	International Telecommunication Union

J

K

L

LoRa	Long Range Wide Area Network
LQSR	Link Quality Source Routing
LTE	Long Term Evolution
LXC	Linux Container
LXD	Linux Container Daemon

M

MAC	Media Access Control
MANET	Mobile Ad hoc Network
MANO	NFV Management and Orchestration
MAP	Mesh Access Point
MCS	Modulation and Coding Scheme
MCTS	Monte Carlo Tree Search

MEC	Mobile Edge Computing
MEOC	Mobile Emergency Operations Center
MIMO	Multiple Input Multiple Output
MOEA	Multi-Objectives Evolutionary Algorithm
MOOP	Multi-Objective Optimisation Problem
MP	Mesh Point
MPP	Mesh Portal Point

N

NFV	Network Function Virtualisation
NFVI	Network Functions Virtualisation Infrastructure
NFVO	NFV Orchestrator
NICER	Networked Infrastructureless Cooperation for Emergency Response
NP	Non-deterministic Polynomial-time
NSGA-II	Nondominated Sorting Genetic Algorithm II

O

OBF	Optimised Brute Force
OGM	Originator Message
OLSR	Optimized Link State Routing
OS	Operating System

OSS/BSS	Operational and Billing Support System
OVS	Open vSwitch

P

PRML	Protection and Rescue Markup Language
P2P	Peer-to-Peer
PASER	Position AwareSecure and EfficientRoute Discovery Protocol
PREP	Path Reply
PREQ	Path Request

Q

QoS	Quality of Service

R

RANN	Root Announcement
RD	Relation Degree
RFC	Requests for Comments
RFID	Radio-Frequency Identification
RM	Random Migration
RSSI	Received Signal Strength Indicator
RX	Receive

S

SDN	Software Defined Network
SFC	Service Function Chain
SN	Special Node
SNR	Signal to Noise Ratio
SPAN	Smartphone Ad hoc Network
SPIDER	Security System for Public Institutions in Disastrous Emergency scenaRios
SSD	Solid-State-Drive

T

TETRA	Terrestrial Trunked Radio
TCP	Transmission Control Protocol
THW	Federal Agency for Technical Relief
TLV	Type-Length-Value
TQ	Transmission Quality

U

UDP	User Datagram Protocol
USB	Universal Serial Bus

V

VANET	Vehicular Ad hoc Network
VIM	Virtualised Infrastructure Manager

VM	Virtual Machine
VNF	Virtual Network Function
VNFM	VNF Manager
VoIP	Voice over Internet Protocol

W

WANET	Wireless Ad hoc Network
WiMax	Worldwide Interoperability for Microwave Access
WISECOM	Wireless Infrastructure over Satellite for Emergency Communications
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network

X

XML	Extensible Markup Language

Y

Z

ZRP	Zone Routing Protocol

Appendix B – Own Publications

The following list includes publications related to the area of this research, to which the author of this thesis has contributed during the course of research.

- Paguem Tchinda, A., Lehmann, A. and Trick, U. (2016) ‘Untersuchung von Wireless Mesh Network-Routing-Protokollen für den Einsatz in Netzen für Katastrophengebiete’, Mobilkommunikation: Technologien und Anwendungen, ITG-Fachtagung , Osnabrück, Germany.
  VDE: https://www.vde-verlag.de/proceedings-de/454220013.html
- Lehmann, A., Paguem Tchinda, A. and Trick, U. (2016) ‘Optimization of Wireless Disaster Network through Network Virtualization’, in INC, Frankfurt, Germany.
  CSCAN: https://www.cscan.org/?page=openaccess&eid=18&id=310
- Paguem Tchinda, A., Frick, G., Trick, U., Lehmann, A. and Ghita, B. (2017) ‘Performance analysis of WMN routing protocols for disaster networks’, in 2017 IEEE Symposium on Communications and Vehicular Technology (SCVT). IEEE, pp. 1–6, Leuven, Belgium.
  DOI: https://doi.org/10.1109/SCVT.2017.8240309
  IEEE Xplore: https://ieeexplore.ieee.org/document/8240309
- Frick, G., Paguem Tchinda, A., Trick, U., Lehmann, A., Frick, G., Tchinda, A. P. and Ghita, B. (2018) ‘Distributed NFV Orchestration in a WMN-Based Disaster Network’, in 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN). IEEE, pp. 168–173, Prague, Czech Republic.

DOI: https://doi.org/10.1109/ICUFN.2018.8436705

IEEE Xplore: https://ieeexplore.ieee.org/document/8436705

- Frick, G., Paguem Tchinda, A., Shala, B., Trick, U., Lehmann, A. and Ghita, B. (2019a) ‘Requirements for a Distributed NFV Orchestration in a WMN-Based Disaster Network’, in 2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM). IEEE, pp. 1–6, Paris, France.

  DOI: https://doi.org/10.1109/ICT-DM47966.2019.9032953

  IEEE Xplore: https://ieeexplore.ieee.org/document/9032953

- Frick, G., Paguem Tchinda, A., Trick, U., Lehmann, A. and Ghita, B. (2019b) ‘NFV Resource Advertisement and Discovery Protocol for a Distributed NFV Orchestration in a WMN-based Disaster Network’, in 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). IEEE, pp. 1–6.

  DOI: https://doi.org/10.23919/SOFTCOM.2019.8903694

  IEEE Xplore: https://ieeexplore.ieee.org/document/8903694

- Paguem Tchinda, A., Frick, G., Trick, U., Lehmann, A. and Ghita, B. (2020) ‘High Throughput WMN for the Communication in Disaster Scenario’, in 2020 World Conference on Computing and Communication Technologies (WCCCT). IEEE, pp. 53–63, Warsaw, Poland.

  DOI: https://doi.org/10.1109/WCCCT49810.2020.9170007

  IEEE Xplore: https://ieeexplore.ieee.org/document/9170007

- Frick, G., Paguem Tchinda, A., Trick, U., Lehmann, A. and Ghita, B. (2020) ‘Possible Challenges and Appropriate Measures for a Resilient WMN-Based

Disaster Network', in 2020 World Conference on Computing and Communication Technologies (WCCCT). IEEE, pp. 70–78, Warsaw, Poland.

DOI: https://doi.org/10.1109/WCCCT49810.2020.9170008

IEEE Xplore: https://ieeexplore.ieee.org/document/9170008