2019-12

Requirements for a Distributed NFV Orchestration in a WMN-Based Disaster Network

Frick, G

10.1109/ict-dm47966.2019.9032953
2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)
IEEE

Requirements for a Distributed NFV Orchestration in a WMN-based Disaster Network

Gregor Frick[12], Auberlin Paguem Tchinda[12], Besfort Shala[12], Ulrich Trick[1], Armin Lehmann[1], Bogdan Ghita[2]
[1]Research Group for Telecommunication networks, Frankfurt University of Applied Sciences, Frankfurt/Main, Germany
{ frick, paguem, shala, trick, lehmann }@e-technik.org
[2]Centre for Security, Communications and Network Research, University of Plymouth, Plymouth, United Kingdom
{ gregor.frick, auberlin.paguemtchinda, besfort.shala, bogdan.ghita }@plymouth.ac.uk

***Abstract*—To provide an emergency communication infrastructure for rescue helpers and victims in the event of a disaster, the research project VirtO4WMN proposes to utilise a Wireless Mesh Network (WMN)-based disaster network. The network is constructed from battery-supplied wireless outdoor routers. By integrating the concept of Network Function Virtualisation (NFV), the network and service availability as well as their reliability are improved. For eliminating the single-point-of-failure of a centralised NFV orchestration the functionality of the NFV orchestration shall be distributed among the nodes in the WMN. For providing the best possible solution for a distributed NFV orchestration in a WMN-based disaster network, various requirements the orchestration must meet are defined and presented in this paper. The requirements are directly derived from the requirements of a WMN-based disaster network, which are also defined in this paper.**

Keywords—Disaster Network, Wireless Mesh Network, Network Function Virtualisation, Distributed Orchestration

I. INTRODUCTION

Natural disasters such as earthquakes, tsunamis, hurricanes, and floods as well as man-made disasters such as persistent power failures are often causing significant damage to existing telecommunication infrastructure or even destroy them. Due to the missing communication infrastructure a coordination of rescue teams and volunteers as well as the discovery of victims in need is difficult to impossible. According to [1], an operating communication infrastructure is therefore assumed as crucial regarding the rescuing of victims in need and the management of rescue teams.

The research project VirtO4WMN [2] funded by the German Federal Ministry of Education and Research (BMBF) investigates the possibility of using an enhanced disaster network in the event of a catastrophe. The disaster network is constructed from battery-supplied wireless outdoor routers, which are deployed in the disaster area and together establish a wireless mesh network (WMN). The WMN (see Fig. 1) provides the basis for an IP-based network infrastructure, while the integration of virtualisation will enable a dynamic service provisioning.

The provided services include common network services and functionalities (such as Dynamic Host Configuration Protocol (DHCP)-, Domain Name System (DNS)-Server, firewalls, Network Address Translations (NATs), etc.), communication-related services (such as Multimedia over IP (MoIP), instant message (IM), etc.) and data provisioning services (provided via databases and data storage servers). By using virtualisation techniques for the deployment of the services, their position in the network can be dynamically changed by relocating the services on a desired location through the reallocation of the corresponding virtual resources (i.e. a virtual machine (VM) or container) on another outdoor

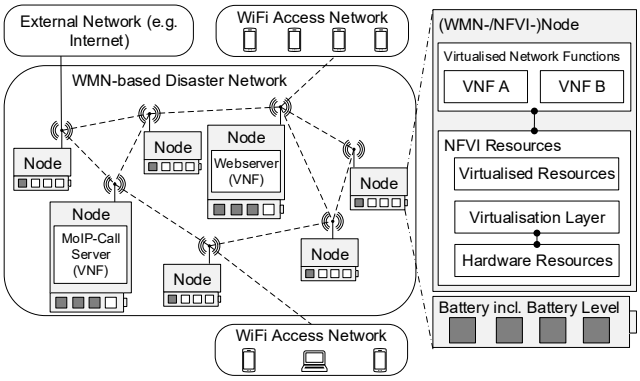

Fig. 1. Conceptual network infrastructure of the WMN-based disaster network

router. Services could, for example, be hosted close to the users, resulting in energy savings through optimised network traffic and improved service availably and user experience through low latencies. In addition to these optimisation aspects, virtualisation can also optimise and improve the overall network availability, reliability, and scalability.

For enabling these optimisation aspects in the WMN-based disaster network, the authors in [3] suggest the utilisation of the Network Function Virtualisation (NFV) concept.. The European Telecommunication Standards Institute (ETSI) standardised an architectural framework in [4] for enabling the concept of NFV. The framework defines various components and (in particular) several management and orchestration (MANO) components for orchestrating and managing physical and virtual resources. The main component of the NFV-MANO is the centralised NFV Orchestrator (NFVO), which is in charge of the resource and network service orchestration in the NFV infrastructure (NFVI) [5]. Due to the standardisation of the NFVO as a centralised unit, the major problem of a single point of failure results from the integration of NFV into the WMN-based disaster network.

Due to the destruction of any existing communication infrastructure by a disaster, the WMN-based disaster network must operate without a connection to any external network such as the Internet since the required access points and gateways have been destroyed by the disaster. Accordingly, the NFV orchestration must also operate within the disaster network. A WMN node hosting the centralised orchestrator defined by ETSI might get damaged, destroyed, or lose its connectivity to large sections of the network due to additional disasters such as aftershocks and outbreaking fires resulting from the environment of a disaster. The loss of the orchestrator is not beneficial, as it will result in losing the possibility to maintain and orchestrate the resources of the NFVI and thus

978-1-7281-4920-2/19/$31.00 ©2019 IEEE

the provided services. To prevent this scenario of a complete breakdown of the NFVI and enable a high availability and fault tolerance of the orchestration, the functionalities of the orchestrator needs to be distributed among the WMN nodes of the disaster network.

Since the distributed orchestration is used in the WMN-based disaster network, its requirements are directly connected to the requirements which are imposed on the disaster network itself. Therefore, the requirements for the WMN-based disaster need to be defined, so that the requirements for the distributed orchestration can be derived from those of the disaster network. The process of the derivation and definition of the requirements is illustrated in Fig. 2. An initial architecture of a distributed NFV orchestration for a WMN-based disaster network that already fulfils parts of the requirements presented in this paper is proposed in [6].

This paper is structured as follows. General challenges a disaster network must overcome are presented in section II. Based on these challenges and the intensions of the parent research project VirtO4WMN, the general requirements for the WMN-based disaster network are derived and defined in section III. The definition of these general requirements will also highlight more specific requirements for the WMN and NFV aspects of the WMN-based disaster network. Afterwards, requirements imposed on the distributed NFV orchestration derived from those of the network are presented in section IV. This paper will close with a summary and conclusion in section V.

II. Challenges of a Disaster Network

The basic idea of providing a communication infrastructure in the event of a disaster is not novel and has been examined before. Challenges a disaster network must overcome have therefore been worked out in the past and are also valid for the WMN-based disaster network. The numerous challenges have been summarised in [3]. In the following these challenges are shortly listed and explained:

- Popularity: a disaster network should support and utilise common technologies, such as smartphones, since most people possess one and can handle it.
- Usability: a disaster network should provide task-oriented communication services (e.g. telephony), support mobility of users and have adequate quality of service (QoS). Additionally, the available resources should have long durability, which might be archivable through rechargeable batteries resulting in an efficient energy consumption.
- Practicability: the network requires to be constructed under limited budgets as easy as possible within shortest time, also the equipment has to be easily accessible.
- Capacity: support sufficient number of concurrent users and overcome traffic congestion
- Sustainability: the communication network should operate until the public network is recovered and it should continually provide service, even if it is broken down, it should recover quickly.
- Adaptability: Due to constant changes due to aftershocks, outbreaking fires and progress of the disaster response, the communication system should be adaptable and flexible.
- Operability: Operation, administration, and maintenance (OAM) functions are needed to keep the system running, adjust network topology, and allocate bandwidth according to the requirements of the user groups, e.g. rescue helpers.

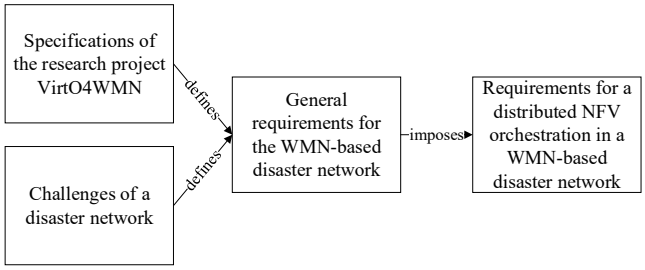

Fig. 2. Derivation process of the requirements for a distributed NFV orchestration in a WMN-based disaster network

- Connectivity: Communication between different user groups, such as rescue team members, headquarters, and victims, must be guaranteed, which represents inter and intra communication.
- Security: Security functions should protect the network also against attackers. In addition, high reliability and availably is necessary.

III. General Requirements imposed on the WMN-based Disaster Network

The challenges listed in the previous section as well as the specifications of the research project VirtO4WMN, which have been presented in the introduction, pose major issues on the WMN-based disaster network. In order to deal with these issues and provide a best possible solution, various requirements have been defined. The requirements and their derivation are described in more detail below. Also, resulting problems for the various technical aspects of the disaster network, caused by the respective requirements, are briefly examined. These technical aspects include WMN-related topics and issues associated with the integration of NFV.

A. Independent of external energy grids through battery-supplied hardware-limited outdoor-routers

It needs to be assumed that a disaster not only destroyed the telecommunication infrastructure, but also damaged the local energy provisioning system. The disaster network should therefore not rely on any energy grid, which is intended to be achieved through a battery-powered system. Due to the limited capacity of a battery, the hardware equipped in the out-door-routers must be limited in order to ensure the longest possible lifetime of the network. By limiting the hardware, however, a reduction of the initial investment is achieved.

This general requirement of a maximal network lifetime results in major issues to be solved in terms of energy efficiency. Based on the assumption that a data transfer will consume energy, a reduction of the traffic in the network is crucial in order to extend the network lifetime to a maximum [7]. Additional traffic overhead required for the connection establishment in the network and the management of resources must be kept to a minimum to avoid unnecessary power consumption.

Furthermore, the network functions and services must be efficiently allocated in the network to optimize the user traffic and thus the overall energy consumption in the network. Such optimisation aspects are part of the NFV resource allocation (NFV-RA) problem described in [8].

The limited available hardware resources provided by the outdoor routers are required to be used efficiently. According to [9], container virtualisation utilises the hardware resources more efficiently than virtual machines. Additionally, as

mentioned in [10], a measurement shows that the network performance of container virtualisation is consuming less energy compared to a kernel-based virtual machine (KVM). Realising the virtualised network function and services in the WMN-based disaster network via container virtualisation is thus promising in terms of energy-efficiency.

B. Providing mission critical communication services

The provision of a communication infrastructure in the event of a disaster is the main driving motivation behind the development of the WMN-based disaster network. Accordingly, the provision and management of the necessary communication services is essential. Currently, civil protection organisations, such as the German Federal Agency for Technical Relief (THW) are relying on the Terrestrial Trunked Radio (TETRA) based Federal Agency for Public Safety (BOS) digital radio network and its services [11]. Since the THW will be one of the main user groups of the disaster network, the services of the current non-IP-based BOS digital radio network need to be provided in the IP-based disaster network by supporting appropriate MoIP-based communication services.

For ensuring the usability of the disaster network, the MoIP-based communication services need to include VoIP (Voice over IP) services and instant message (IM) services. Both service types must enable a one-to-one-based and group-based communication. In addition, data provisioning services (provided by databases and data storage servers) are required.

C. Ensure continuous working infrastructure even in the event of failing nodes

Since the network is intended to provide a communication infrastructure in the event of a disaster, its availability is essential for its use. The disaster network must therefore ensure a continuous working infrastructure even in the event of failures. Failures will be unavoidable and can be divided into two categories: predictable and spontaneous failures.

Predictable errors result from the aspect that the disaster network is a battery-powered system. A node might, and high likely will, fail due to an empty battery. It can be assumed, that the energy consumption and battery status of each node can be read out and thus determined, enabling the network to start optimisation processes in advance. This would minimise the impact of this predicable failure on the network and thus on the communication infrastructure.

Spontaneous failures result from the disaster environment and possible subsequent disasters, such as blazing fires or aftershocks. These scenarios could destroy an already established and integrated node in the network without prior notice. This failure would have to be detected quickly in order to make necessary adjustments in the network infrastructure to ensure the availability of the disaster network.

In order to be able to cope with the possibilities of spontaneous and predictable errors and to enable a continuously working infrastructure, certain aspects must be considered. Firstly, the WMN routing protocol used in the network must allow a dynamic route discovery for identifying new routes in case of a node failing which was participating in a data transmission. Additionally, no centralised management component should exist especially regarding the NFV MANO, which also needs to ensure a continuous resource and service orchestration. Lastly, in the worst case, a failing node might cause a network partition (see Fig. 3).

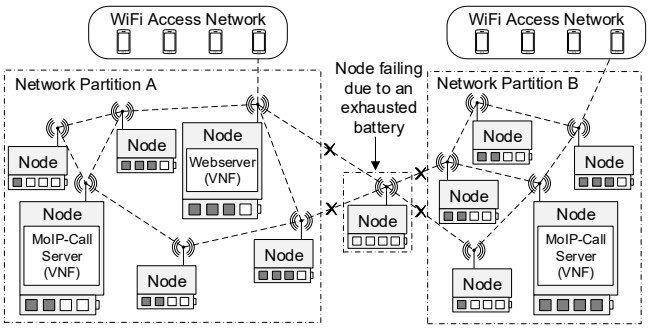

Fig. 3. Scemario of a failing node resulting in a network partition

The network should be tolerant regarding network partitions and should also provide the possibility for merging into one partition again.

D. Multi-tenants support for different user-groups

Various user-groups in the disaster environment (such as THW, police, firefighters, victims, and volunteers) will require the communication infrastructure and its services. It can be assumed that each user group (or tenant) will require an individual logically separated virtual network with different requirements.

The different virtual networks require to be isolated from each other. A volunteer, as an example, should not be able to participate in the network of the THW without specific allowance. Also, should the traffic of volunteers or victims not influence the service availably and user experience of official rescue helpers. According to [12], the concept of network slicing is known to enable such logically separated virtual networks. An adaptation of this concept could therefore enable a multi-tenant support for different user-groups in the WMN-based disaster network.

E. Support of flexible and dynamic infrastructure

The hardware of the disaster network is intended to be deployed by the first responders. Based on the self-configuration characteristics of a WMN, the network can be extended at any time by deploying additional outdoor routers in the environment of the disaster. This functionality will be essential due to the limited range of a wireless transmission technology and the geographical area the network must cover. This results in a flexible and dynamic network infrastructure which needs to be considered during the design of the disaster network. In order to limit the dynamic of the network to a certain degree, it is assumed that the deployed nodes will be stationary. Therefore, a mobility of the nodes is not intended.

Nevertheless, some challenges result from the dynamic and flexible infrastructure. Newly deployed nodes must be integrated into the network immediately in order to use their resources. Furthermore, the underlying WMN routing protocol must be scalable to ensure routing in a larger network, while the management and orchestration of available resources in a larger network must also be guaranteed. The support of a sufficient data transfer rate in a multi-hop communication must be assured, which can, according to [13], become a problem due to issues related to the characteristics of the Medium Access Control protocol, the exposed node problem and the hidden terminal problem occurring in a single-channel system.

F. Protection against internal and external attacks

A disaster event will not prevent morally questionable individuals from initialising attacks on the disaster network in

order to take over or harm the infrastructure. For this reason, the disaster network must be secured and protected. This includes a secure access network for users as well as a secure air interface between the WMN nodes to prevent the possibility of traffic injections.

In case of the event of an intrusion into the network, the existing communications require to be encrypted. The encryption of the MoIP communication should prevent an unlawful interception of the rescue helper's communication, while an encrypted communication of the administrative and management components in the network should prevent the shutdown or manipulation of deployed services.

G. Usage of common wireless transmission technologies

The communication infrastructure of the disaster network should not only serve official rescue workers such as the THW or the fire brigade. It is also intended to serve as a communication possibility for the civilian population to make emergency calls if necessary or to access news regarding the further course of action of the affected civilian population. For this purpose, a common connectionless technology should be used in the access network of the disaster network. As mentioned before, an enormous proportion of the population owns a smartphone, which is the reason for the access being based on Wi-Fi, since the connection to a Wi-Fi-based access point is well known and no additional knowledge and technology is required.

The intra-WMN communication should also be based on the Wi-Fi technology as it provides the enough bandwidth for the establishment of MoIP-based communication. Other wireless technologies are inadequate for the disaster network compared to Wi-Fi. As an example, Wi-Fi has a higher range than Bluetooth and can provide more bandwidth than LoRa (Long Range Wire Area). In addition, the realisation of a Wi-Fi based mesh is more common and less expensive than with WiMAX or LTE (Long Term Evolution).

H. Minimal workload for network administrators

Due to the disaster and its impact in the affected region, all existing emergency forces are expected to be needed for urgent activities, such as locating and recovering victims or dealing with the consequences of the disasters, such as fires. It is therefore doubtful that deployed emergency forces can explicitly deal with the deployment and maintenance of the disaster network. For this reason, the disaster network must operate with an absolute minimum of external administration. The required administration of the network should be limited to the deployment of the routers in the disaster environment and should not require any complex additional manual configuration. To accomplish this aspect, the disaster network needs various autonomous automation processes. These processes must enable the configuration of the network infrastructure and its resources, as well as the deployment and management of the various required services.

IV. Requirements imposed on the Distributed NFV Orchestration

In this section, the initial requirements for the distributed NFV orchestration of the WMN-based disaster network are derived and described in detail. As mentioned before, the requirements should enable a precise definition of the characteristics and properties of the distributed orchestration in order to design and develop a meaningful concept. Some requirements have already been mentioned in section III as a subset of a general requirement of the WMN-based disaster network but will be defined and discussed in more detail in the following.

A. Distributed and decentralised architecture

The possibility of a single point of failure through the logically centralised NFVO is the main barrier preventing the integration of NFV into the WMN-based disaster network. As mentioned before, nodes can be destroyed at any time due to various events in the disaster environment. A node operating the centralised orchestrator could thus be destroyed, resulting in irrevocably losing the orchestration of the infrastructure, its provided services, and all previous configurations.

In order to eliminate this aspect and to ensure the availability of the network and its services even in case of failure, the functionality of the NFVO must be distributed among the nodes in the network. This provides the basis for achieving a high fault tolerance, a load distribution and balancing as well as the increased reliability and availability of the orchestration and thus the complete network.

B. Capability of NFV resource and network service orchestration

Due to the integration of NFV into the disaster network, the distributed orchestration requires to have the capability for the NFV resource and network service orchestration. As previously mentioned, ETSI defines in [4] and [5] various MANO components with each component providing a specific functionality. The overall functionality must also be provided by the distributed orchestration, especially including the lifecycle-management of the virtual network functions and network services as well as the resource allocation.

C. Self-healing architecture

Since an entity of the distributed orchestration might fail due to a destroyed node or an exhausted battery, the architecture of the orchestration needs to cope with these situations to achieve a persistent availability of the orchestration and thus provide the basis for a continuous resource orchestration. An architecture based on redundant units is too resource-intensive for the resource-limited disaster network, whereby the scenario of a failing entity should be compensated by an architecture having self-healing capabilities. The algorithm required for the distributed orchestration should therefore decide autonomously whether the failed entity should be compensated by the initialisation of a new entity or whether the tasks of the failed entity are taken over by another entity.

D. Continuous and autonomous orchestration

The network infrastructure of the disaster network is exposed to dynamic changes resulting from the possibilities of destroyed nodes, exhausted batteries, and occurring and possibly persistent interferences resulting from the wireless medium. The distributed orchestration must continuously monitor and orchestrate the infrastructure in order to react to these dynamic changes to ensure a high availability of the services and thus of the entire communication infrastructure. As an external administration cannot be guaranteed, the orchestration must adapt to those changes autonomously.

E. Suitable for single administrative domain

The network infrastructure of the WMN-based disaster network is one coherent network and is thus realising a single administrative domain. The separation of the WMN into

administrative or technically separated domains is not intended since only official rescue helpers, such as THW, are responsible for the deployment and the general administration of the network. In addition, a separation of the WMN into several separated administrative domains would be a barrier during the deployment and establishment of the disaster network. The division of the network into separate administrative domains would require a manual configuration of each battery supplied wireless outdoor router at its deployment by the emergency forces. Priority planning of the domains in the network would also be necessary. To avoid this enormous effort and to keep the workload of the network administration as low as possible, the WMN-based disaster network is one coherent network as mentioned before. For this reason, the distributed orchestration requires to be especially designed for the use in a single administrative domain.

F. *Efficient resource allocation across the complete network infrastructure*

NFV has been defined for the use in data centres for enabling telecommunication providers to dynamically adapt their networks to certain requirements. In comparison to data centres, the disaster network is a constraint network in terms of existing hardware and link capacity of the wireless connections. To offer a suitable communication infrastructure, the resources must be allocated efficiently across the entire network infrastructure by the distributed orchestration. During the placement and allocation of services, different service requirements may have to be provided, which could include the provision of a low delay connection for a VoIP session or a maximum bandwidth connection for exchanging large amounts of data. An additional aspect that must be considered during the allocation of resources is the energy-efficiency. Since the infrastructure of the disaster network must have a maximum lifetime, it is essential to consider the individual energy levels of each outdoor router during the allocation of resources. Also, in terms of energy-efficiency, a knowledge of the user density in the network is indispensable. By allocating services and resources in the user's premise (see Fig. 4), unnecessary routing and forwarding of messages through the network can be prevented, which saves energy.

G. *Network partition tolerance*

As already mentioned before, in the worst-case a node failing due to an exhausted battery or aftershock, might create a network partition, resulting in two or more separated networks (see Fig. 3). The distributed orchestration needs to be capable of identifying and dealing with such network partitions. For providing the required communication services, even in a subset of the disaster network, each partition of the disaster network should be orchestrated as an individual disaster network by the distributed orchestration. Due to the size of a resulting partition and the resulting available resources, the scope of the services provided within a partition might be limited. In case of rescue helpers deploying one or more new nodes in the environment might result in two or multiple partitions getting merged together into one larger network. The distributed orchestration must also identify this scenario and needs to merge with the newly discovered entities in order to reorganise the services in the larger network.

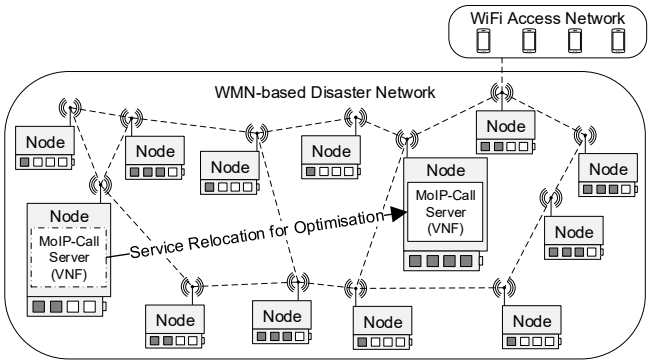

Fig. 4. Process of relocating a service in the user's premise for optimising the routing and forwarding of messages through the network

H. *Automatic resource integration*

One main characteristic of the disaster network consists of its extensibility. First responders can deploy battery-supplied outdoor-routers in the region effected by the disaster. Due to the self-configuration characteristics of a WMN, a newly deployed outdoor router is automatically integrated into the network infrastructure if it is in range of another node inside the WMN. A similar mechanism is required for integrating the hardware resources of the outdoor router into the NFVI. Since the management of the NFVI is a task of the distributed orchestration, it also needs to be capable of integrating the resources automatically into the NFVI in order to use them during the resource allocation processes.

I. *Support for a scalable distributed infrastructure*

Since a disaster can affect a large geographical area, the disaster network must cover this region by the deployment of a possibly huge number of outdoor routers required due to the limited range of a Wi-Fi signal. According to [14], each deployed outdoor-router providing its resources represents a NFVI-Node in the NFV context. Based on this aspect, the disaster network realises a possibly large-scaled distributed NFVI. This aspect must be considered by the distributed orchestration to enable scalability by an evenly distribution of load regarding the management of the NFVI by the entities of the distributed orchestration.

J. *Wireless connection awareness*

Due to the distribution and decentralisation of the orchestration, some form of message exchange will be necessary for the purpose of synchronisation and coordination among the entities. This message exchange and other information exchanges related to the management, such as resource monitoring, will be transmitted using the infrastructure of the disaster network. Due to the nature of wireless connections and suddenly occurring interferences, the required message exchange is likely to be influenced by the mentioned aspects. The distributed orchestration therefore needs to be capable of dealing with dynamic delays and bandwidth limitations, because a missing or delayed message, for example, should not immediately indicate a malfunction.

K. *Minimal communication overhead required for synchronisation and coordination*

As previously mentioned, a message exchange will be required for the coordination of the entities of the distributed orchestration. This message exchange should only produce a minimal communication overhead, since the available capacity of wireless links is limited and is required for the actual communication of the rescue helpers.

L. *Capability of multi-tenant network slicing orchestration*

The provisioning of individual logically separated networks is required for supporting a multi-tenant environment with different requirements. As previously

mentioned, the concept of network slicing can provide this environment. The distributed orchestration therefore needs to be capable of providing the functionality for orchestrating and managing network slicing.

M. Robust and transparent decision-making process

The decision-making process of the orchestration is mainly responsible for the actions executed from the orchestration towards the infrastructure. The process decides whether the current conditions in the infrastructure requires adaptions by executing certain actions. It is therefore mainly responsible for identifying malfunctions or optimisation opportunities in the disaster network. In order to take a consistent decision, the process requires various information about the network, such as aspects about the general network topology, current traffic loads and the utilisation of resources. Since the distributed orchestration therefore requires this information, it is assumed that the entities share at least a subset of these information among each other. Due to the possibilities of dynamic delays and failing nodes the information might be obsolete the moment it has been received by the entities. To deal with these aspects the decision-making process required to be robust. Additionally, the process output should be transparent enabling the entities to retrace and comprehend a taken decision.

N. Retrievable global network status

Rescue helpers, especially the group responsible for deploying the battery-supplied outdoor-routers, must have the possibility to retrieve the current global network status. The retrievable status should consist of the current network topology and resource related information, such as current battery levels. The information should enable the rescue helpers to physically optimise the disaster network. As an example, a draining battery could be replaced in advance to prevent a failure, while the deployment of a new outdoor-router in a very user-crowded area could prevent a possible traffic congestion. To ensure the usability, the information should be retrievable through a single entity of the distributed orchestration.

O. Lightweight and resource-efficient architecture

Known implementations of an NFVO following the ETSI standard, such as Open Source MANO (OSM) [15], have relatively high minimal hardware requirements (as an example: OSM requires at least 2 CPUs and 4 GB RAM). The available hardware resources provided by the battery-supplied wireless outdoor-routers are limited making it difficult to operate such a hardware resource intensive implementation. In order to avoid wasting the available hardware resources and thus energy, the actual architecture of the distributed orchestration requires to enable a lightweight and resource-efficient implementation in terms of its hardware requirements and corresponding hardware utilisation.

P. Secure against violators

As already pointed out before, the disaster network might become a target for attackers. To ensure the service availably, a potential attacker should not be able to influence the output of the decision-making process of the distributed orchestration with false information. Also, should an attacker not be able to act as an entity of the distributed orchestration and thus become a part of it. To prevent these scenarios, the architecture of the distributed orchestration requires a set of security and authentication functionalities.

V. SUMMARY

In this paper requirements for a distributed NFV orchestration in a WMN-based disaster network have been derived and defined. The requirements for the disaster network were used as a basis and reference point for the derivation of the requirements of the orchestration. Among other things, a major requirement consists of the NFV orchestration having a distributed and decentralised architecture with self-healing capabilities to eliminate the possibility of a single point of failure. Additionally, the orchestration requires to deal with the constrained resources in the disaster network by allocating the services efficiently in the network infrastructure. The requirements presented in this paper will be used to further extend and improve the architecture of a distributed NFV orchestration for a WMN-based disaster network proposed in [6].

ACKNOWLEDGMENT

The research project VirtO4WMN providing the basis for this publication is partially funded by the Federal Ministry of Education and Research (BMBF) of the Federal Republic of Germany under grant number 13FH018IX6. The authors of this publication are in charge of its content.

REFERENCES

[1] ITU-T Focus Group on Disaster Relief Systems Network Resilience and Recovery, “Technical report on Telecommunications and Disaster Mitigation,” 2013.

[2] VirtO4WMN, “BMBF-Forschungsprojekt: Optimierung von Wireless Mesh Networks mit Netzwerkvirtualisierung für den Katastropheneinsatz (VirtO4WMN),” 2019. [Online]. Available: https://www.e-technik.org/forschung/virto4wmn.htm. [Accessed: 25-Apr-2019].

[3] A. Lehmann, A. Paguem Tchinda, and U. Trick, “Optimization of wireless disaster network through network virtualization,” *INC (2016), Frankfurt*, pp. 165–170, 2016.

[4] ETSI, “Network Function Virtualisation (NFV); Architectural Framework,” *ETSI GS NFV 002 V1.2.1*, 2014.

[5] ETSI, “Network Function Virtualization (NFV); Management and Orchestration,” *ETSI GS NFV-MAN 001 V1.1.1*, 2014.

[6] G. Frick, A. Paguem Tchinda, U. Trick, A. Lehmann, and B. Ghita, “Distributed NFV Orchestration in a WMN-Based Disaster Network,” in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2018, pp. 168–173.

[7] Y. Jahir, M. Atiquzzaman, H. Refai, A. Paranjothi, and P. G. LoPresti, “Routing protocols and architecture for disaster area network: A survey,” *Ad Hoc Networks*, vol. 82, pp. 1–14, Jan. 2019.

[8] J. Gil Herrera and J. F. Botero, “Resource Allocation in NFV: A Comprehensive Survey,” *IEEE Trans. Netw. Serv. Manag.*, vol. 13, no. 3, pp. 518–532, Sep. 2016.

[9] Q. Zhang, L. Liu, C. Pu, Q. Dou, L. Wu, and W. Zhou, “A Comparative Study of Containers and Virtual Machines in Big Data Environment,” Jul. 2018.

[10] R. Morabito, “Power Consumption of Virtualization Technologies: An Empirical Investigation,” *Proc. - 2015 IEEE/ACM 8th Int. Conf. Util. Cloud Comput. UCC 2015*, pp. 522–527, 2015.

[11] Federal Agency for Public Safety Digital Radio, “BDBOS - Digital Radio,” 2018. [Online]. Available: https://www.bdbos.bund.de/EN/Digitalradio/digital_radio_node.html. [Accessed: 17-May-2019].

[12] F. Xenofon, P. Georgios, E. Ahmed, and K. M. Mahesh, “Network Slicing in 5G: Survey and Challenges,” *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 94–100, 2017.

[13] Y. Zhang, J. Luo, and H. Hu, *Wireless mesh networking: architectures, protocols and standards*. Auerbach Publications, 2007.

[14] ETSI, “Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV,” *ETSI GS NFV 003 V1.3.1*, 2018.

[15] ETSI, “Open Source MANO (OSM),” 2018. [Online]. Available: https://osm.etsi.org/. [Accessed: 25-Apr-2019].