2020-05

Possible Challenges and Appropriate Measures for a Resilient WMN-Based Disaster Network

Frick, G

10.1109/wccct49810.2020.9170008
2020 World Conference on Computing and Communication Technologies (WCCCT)
IEEE

Possible Challenges and Appropriate Measures for a Resilient WMN-Based Disaster Network

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

***Abstract*—A wireless mesh network (WMN)-based disaster network shall provide an emergency communication infrastructure in case of a catastrophe destroyed any existing communication infrastructure. Since the hardware of the disaster network is deployed in an environment affected by the outcome of a catastrophe, events such as aftershocks and/or outbreaking fires are likely to occur and may destroy the hardware of the disaster network. To maintain its provided functionality and thus its usability, the network requires to be resilient to these and other events which are affecting the network infrastructure. To achieve a resilient network, the normal state of the network as well as possible challenges affecting the normal state need to be defined in prior. This scientific work deals with the derivation and definition of the required normal state of the WMN-based disaster network, as well as the definition of possible challenges resulting from environmental-based events. Since each possible challenge is influencing the network infrastructure of the WMN-based disaster network, possible measures for preventing and/or reducing the impact of each challenge are defined. In addition, emergency corrections capable of resolving the influences of an occurring challenge are defined.**

Keywords-Wireless Mesh Networks; Network Function Virtualisation; Disaster Networks; Resilience

I. INTRODUCTION

The provisioning of an emergency communication infrastructure for rescue helpers and victims in case of existing communication infrastructures being destroyed by natural disasters (such as earthquakes and floods) or manmade disasters (such as persistent power outages) is assumed to be crucial. For this reason, [1] proposes the deployment of a disaster network for providing such an emergency communication infrastructure, while [2] further specifies the network. The disaster network is intended to be constructed from battery-supplied multi-radio wireless outdoor routers being deployed in the disaster environment by the first responders. The routers are establishing a cluster-based multi-radio multi-channel wireless mesh network (WMN) and are building the basis for an IP-based network infrastructure. By integrating network function virtualisation (NFV) into the WMN-based disaster network, a dynamic and adaptable network service and function provisioning shall be achieved. For this aspect the resources of the routers are being utilised to establish the required NFV infrastructure (NFVI).

The disaster network needs to operate and provide its functionality to the user at any time to remain available and thus usable. This aspect is defined in more detail in [2], which presents various requirements for the WMN-based disaster network. Among other requirements, a continuous working infrastructure as well as the support of a flexible and dynamic infrastructure are crucial for the disaster network. This results from the aspect, that the network infrastructure of the disaster network is permanently exposed to predictable and spontaneous occurring events, such as node failures. These events result from the disaster environment and the concept of the WMN-based disaster network itself. Among other events, an existing node might possibly fail either predictable due to an exhausted battery or spontaneously due to its destruction resulting from an aftershock or outbreaking fire resulting from the catastrophe. In addition, a new node might join the network due to the deployment of a corresponding new outdoor router by the first responders for the purpose of a geographical expansion of the network.

To ensure an operating communication infrastructure in the face of these events, the functionality of the NFV orchestration, mainly responsible for the availability of the network, is distributed among the nodes in the network. This is required since a NFV orchestrator standardised in [3] is a logically centralised component resulting in the possibility of a single point of failure. Due to the missing connection to any external network (such as the internet), the necessary orchestration must operate in-band of the disaster network. Consequently, a centralised orchestrator might get lost due to the possibility of a node failure leading to the loss of the opportunity to orchestrate and manage the disaster network.

Although the distributed NFV orchestration increases the overall availability of the disaster network, specific orchestration targets are required which can deal with the different events affecting the network infrastructure. A network capable of dealing with such events is a resilient network. According to [4], a network is resilient if it can provide and maintain an acceptable level of service even in the event of failures and challenges violating the normal operation of the network. For this purpose, resilience includes and extends various disciplines such as survivability and fault-tolerance, as well as distribution tolerance and

978-1-7281-9738-8/20/$31.00 ©2020 IEEE

traffic tolerance in relation to possible occurring challenges and failures.

A generalised approach, which is introduced in [4], to achieve and maintain resilience is the two-phase strategy D²R²+DR (Defend, Detect, Remediate, Recover + Diagnose and Refine – see Figure 1). The steps in the inner real-time control loop D²R² consist of defending a system against challenges and threads to the systems normal operation, detecting an occurring adverse event or condition, remediate the effects of the adverse event or condition to minimise the impact and recover to the systems normal operation. The outer loop DR consists of the long-time evolution of the system by diagnosing the root cause of a fault and refining the future behaviour of the network accordingly.

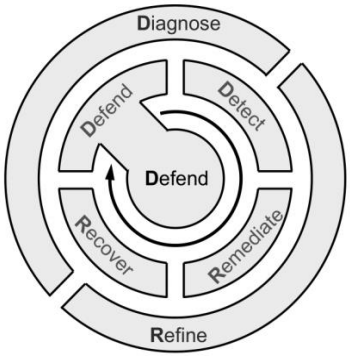

Figure 1. Two-phase resilience strategy D²R²+DR [4]

For a possible adaptation and integration of this resilience strategy for achieving a resilient WMN-based disaster network, different prerequisites must be defined in prior, according to [4]. Service requirements must be defined to understand the level of resilience the network should provide (in terms of quality of service (QoS) or performance). The normal operation of the network needs to be known in order to identify a challenge. While possible challenge models are required in order to be able to detect potential adverse events and conditions and allowing an appropriate reaction to them.

In the following, these prerequisites will be defined and presented for the WMN-based disaster network and shall provide the basis for a resilient network. This paper is structured as follows. Section II will introduce the normal state (corresponds the normal operation) of the network, which also includes the service requirements. Possible challenges and corresponding influences affecting the disaster network are derived and presented in section III. While possible measures and emergency corrections to maintain the normal state of the network for each challenge are presented in section IV. The paper will close with a summary and conclusion in section V.

II. Normal State of the Resilient WMN-Based Disaster Network

A crucial aspect required for achieving and maintaining a resilient network consists of the knowledge of the normal state of the network. By being aware of the normal state of a network, arising challenges influencing a network can be identified and engaged or even prevented. Through this process the resilience of a network can be maintained and ensured. For this reason, the normal state of the WMN-based disaster network (see Figure 2) is defined and presented in the following. The normal state is separated into several normal state conditions (NSC) and together also represent the overall concept of the WMN-based disaster network. It should be noted that the listing of the categories below does not necessarily impose any prioritisation among the normal state conditions.

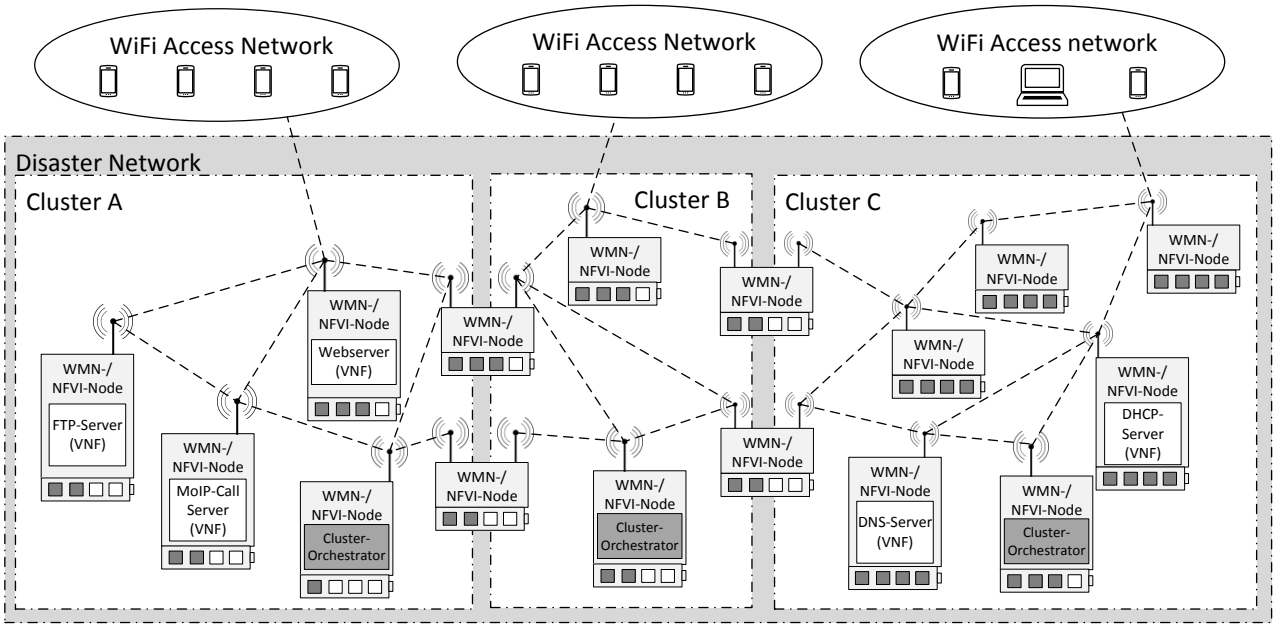

Figure 2. Normal State of the WMN-based Disaster Network

NSC-1. Distributed NFV Orchestration Existing

The NFV orchestration is capable of orchestrating and managing the virtual and physical resources in the network, such as the different services and hardware respectively. It is therefore mainly responsible for achieving and maintaining the resilience of the disaster network through various optimisation processes it can initialise. These optimisation processes, among others, include the reallocation of a service closer to the users to improve the service performance and adaptation of the network topology according to the current network conditions through the reconfiguration of the appropriate physical resources within the infrastructure.

As already mentioned in the introduction, due to the destruction of the existing communication infrastructure, a connection to any external network cannot be expected. The NFV orchestration therefore most operate in-band of the disaster network, making it vulnerable to the possible harmful events, such as failing nodes. The NFV orchestration is, according to [3], a logically centralised component and its loss would result in losing the possibility to orchestrate and manage the resources in the NFVI. Since this scenario is not beneficial, the functionality of the NFV orchestrator is distributed among the nodes in the network enabling a distributed NFV orchestration and therefore eliminating the possibility of a single-point-of-failure.

The architecture of the distributed NFV orchestration is presented in [5] and consists of defining an orchestration unit for each cluster of the disaster network, the Cluster-Orchestrator. The Cluster-Orchestrator is responsible for orchestrating and managing the nodes in its assigned cluster. Through the synchronisation with the other Cluster-Orchestrators within the WMN-based disaster network, a network-wide orchestration is achieved.

The existence of a decision-making component, such as the NFV orchestration, deciding about changes and adaptations in the WMN-based disaster network is crucial for achieving and maintaining the normal state of the network. To ensure the existence of the distributed NFV orchestration, [6] introduces an NFV resource advertisement and discovery protocol, which supports the distributed orchestration in identifying and monitoring the resources in the network. In addition, it provides mechanisms for compensating a failing Cluster-Orchestrator, and therefore a unit of the distributed NFV orchestration, by an immediate initialisation of a backup unit. Through this protocol the existence of the distributed NFV orchestration can be ensured, which provides a basis for the overall resilience of the network through its normal state.

NSC-2. Services Requirements Are Met

To ensure a suitable communication for the users of the disaster network, the service requirements of the provided services need to be met in order to achieve the desired normal state for a resilient disaster network. The provided services include common network services and functionalities to enable an IP-based communication (DHCP and DNS), communication-related services (Multimedia over IP (MoIP) and instant message (IM)), data provisioning services, as well as information provision services realised via webservices. Each service is provided within the disaster network via the corresponding server implementation, namely DHCP-Server, DNS-Server, MoIP-Call-Server, FTP-Server and HTTP-Server. To enable a flexible service provisioning, the server implementations are deployed in the disaster network using a lightweight container virtualisation. From a NFV point of view, each service component (i.e. the corresponding server implementation) is interpreted as a virtualised network function (VNF).

To avoid unnecessary complexity within this research work, the service requirements which need to be met are not described in terms of quality of service (QoS) parameters. Instead a more universal approach is considered regarding the description of the service requirements. A common approach, among others used in [4] and [7] and which will also be utilised in the following, is based on describing the service state in a more general way by using the paraphrases acceptable, impaired and unacceptable. In case of the WMN-based disaster network, a service described using the paraphrase acceptable is expected to be available to all users of the disaster network and provides a satisfying performance to them. The paraphrase impaired will be used if a service is available to all users, but its performance is significantly restricted to some users. While a service described using the paraphrase unacceptable is not available to all users of the network, either through connectivity problems or very poor performance. Ensuring that all services are acceptable and that all users can use the communication facilities of the network is therefore a crucial aspect in achieving the normal state of the disaster network.

NSC-3. Distributed NFV Orchestration Is Observing and Maintaining the Complete Network

According to [4], the awareness of occurring challenges affecting a network is crucial for achieving the resilience of the network. Possible emergency corrections engaging the influences of a challenge can only be initialised if the occurring challenge is identified correctly. Observing the resources of the network infrastructure regarding possible challenges can therefore be assumed as essential for achieving the normal state of a network. Regarding NFV, [7] mentions that a global view of the NFVI resource utilisation as well as the VNF performance is an enabler for a resilient NFV environment since it can improve the error detection and remediation.

Based on these aspects, the distributed NFV orchestration must observe the complete network infrastructure to achieve and maintain the normal state of the resilient WMN-based disaster network. In case of the distributed orchestration proposed in [5], each Cluster-Orchestrator must observe the nodes within its cluster. Each node needs to be monitored regarding their virtual and physical resources as well as their connectivity to neighbouring nodes at all time. Through this obtainable knowledge, a Cluster-Orchestrator can identify and react immediate to occurring challenges within its cluster. By the exchange of this information among the Cluster-Orchestrators of the disaster network, a global network view can be maintained achieving the possibility for a derivation

of the current state of the network. Based on this current state, corrections can be performed within the network infrastructure if required to achieve or ensure the normal state of the network.

The NFV resource advertisement and discovery protocol proposed in [6] supports the Cluster-Orchestrators in observing the resources in their assigned cluster especially regarding challenges resulting from a failing node. In the protocol, an observed node is monitoring its own resources including the wireless links to its neighbours. In case of an exceeded threshold or a lost wireless link, the observed node forwards the corresponding information to its Cluster-Orchestrator for further evaluation. A failing node is therefore not only identified by a Cluster-Orchestrator but also by neighbouring nodes. This aspect supports the distributed NFV orchestration in observing and managing the complete network and increases the sensitivity of the network regarding emerging challenges.

NSC-4. Connectivity between All Integrated Nodes Existing

The main motivation for the deployment of the WMN-based disaster network is the provisioning of an emergency communication infrastructure for the rescue helpers and people in need after the occurrence of a disaster. Especially the rescue helpers will communicate with each other to coordinate their tasks during the catastrophe. It is therefore essential that each user in the network can communicate with any other user within the network independent of their current location. This is guaranteed through the connectivity between the nodes. In case of the normal state of the network, all nodes are connected to each other based on the mesh concept. Through the usage of a WMN routing protocol, available paths through the network are identified and maintained. In [8] and [9] WMN routing protocols are evaluated. The routing protocol HWMP [10] provides the best adaptability to changes within the interconnection of the nodes, according to [8].

One major issue arises regarding this normal state condition. According to [4], the resilience enabler medium diversity provides choices among alternative physical media and therefore increases the connectivity through different available paths. This aspect cannot be provided by the WMN-based disaster network since it only utilises the Wi-Fi technology as described in [2]. Due to the limited physical range of a Wi-Fi signal, a failing node might create a network partition if its geographical location, and thereby its wireless links, was critical. In case of a network partition, each partition needs to act as an individual disaster network and therefore maintain the desired normal state until the network partition is recovered. The recovery is achieved through the physical optimisation of the network by the deployment of a new outdoor router merging the network partitions.

NSC-5. Wi-Fi-Based User Access Network Available

The emergency communication infrastructure provided by the WMN-based disaster network shall not only be used by official rescue-helpers, but also from victims in need. The utilisation should therefore be as simple as possible and shall not require any special equipment. For this reason, as described in [2], the access for the users is based on the Wi-Fi technology since it is a common technology. Regarding the normal state of the disaster network, it needs to be ensured that the access network, which is realised through Wi-Fi-based access points (APs), is available and spanning the complete geographical region to ensure the connectivity for the users and thus the usability of the disaster network itself.

NSC-6. Network Infrastructgure Configurated according to Clustering Algorithm

The WMN-based disaster network is designed as a multi-radio multi-channel WMN. This results from the characteristics of the Medium Access Control protocol, the exposed node problem and the hidden terminal problem occurring in a single-channel system, which according to [11] significantly decreases the available bandwidth in a multi-hop communication. As described in [12], a common approach for solving this problem consists of clustering a wireless network. Through the introduction of clustering, each node is assigned to a cluster, which is operating on a specific channel. Two adjoining clusters are connected to each other via cluster gateways operating on the channels of both clusters. The clusters and nodes are configured according to a specific clustering technique or algorithm. The algorithm used in the WMN-based disaster network, which is not further part of this scientific work, is designed to ensure enough bandwidth in a multi-hop communication. It shall be pointed out, that the cluster configuration in Figure 2 does not necessarily represent the output of the algorithm used within the network and is only for illustrating the concept of clustering in general. However, to ensure the best possible performance of the WMN-based disaster network, the nodes in the network infrastructure are required to be configured according to the clustering algorithm at any time to ensure the normal state of the network.

III. Possible Challenges and Resulting Influences Affecting the Normal State of the WMN-Based Disaster Network

To maintain the normal state of the network and therefore its resilience, the different possible challenges that may occur and influence the WMN-based disaster network need to be defined. Their definition helps the distributed NFV orchestration, which is mainly responsible for maintaining the resilience of the network, to identify the occurrence of the possible challenge. This aspect provides the basis for the adaptation and integration of the general concept of a resilience strategy presented in the introduction (see Figure 1) since it enables the detection of challenges as well as the development of mechanisms required for the defence, remediation and recovery.

In the following the different environmental-based events (E*n*), which the network is exposed to, as well as the possible resulting challenges (C*n* – see Table I) are introduced. For an improved description of the relationship between the environmental-based events and challenges, different scenarios (S*n*) are presented and shown in Figure 3.

TABLE I. POSSIBE CHALLENGES AND THEIR INFLUENCES ON THE WMN-BASED DISASTER NETWORK

C*n*	Possible occurring challenge	Resulting from environmental-based event	Influenced normal state condition	Possible influence(s) on the WMN-based disaster network
C1	Loss of wireless link	E2, E3, E6	NSC-4, NSC-6	- Loss of path defined through WMN routing protocol might lead to connection interrupts if lost wireless link was utilised - Violations in the configuration defined through clustering algorithm - Increased possibility for occurrence of network partition (C8) and risk of network partition through critical node(s) (C7)
C2	Loss of physical resources	E2, E3	-	- Possibility for a decrease of the overall network lifetime due to the loss of optimisation possibilities regarding an energy-efficient allocation of services
C3	Loss of service	E2, E3	NCS-2	- Unavailability of the service and its provided functionality - Unavailability or performance constraints of dependent services due to missing dependency - Loss of the service configurations, as well as data and/or session information maintained by service
C4	Loss of cluster gateway	E2, E3	NCS-6, NCS-2, NCS-4	- Errors in the intended cluster configurations defined by clustering algorithm resulting in the possibility of impaired service performance and overall network connectivity - Increased possibility for traffic congestion (C13)
C5	Loss of Wi-Fi-based AP	E2, E3	NCS-5	- Users in range of AP loss connectivity to the network and cannot utilise its services
C6	Loss of distributed NFV orchestration unit	E2, E3	NCS-3, NCS-1	- Resources maintained by lost unit are neither maintained nor orchestrated - Inconsistent global view due to unawareness of resources resulting in possibly undetected challenges
C7	Teardown of the distributed NFV orchestration	E2, E3	NCS-1, NSC-3	- Network is left completely unmaintained and orchestrated making identification of possible challenges impossible
C8	Inconsistent connectivity	E6	NCS-2, NCS-4	- Possibility of connection failures and bandwidth limitations resulting in performance limitations of services if inconsistent link is used
C9	Risk of network partition through critical node(s)	E1, E2, E3	NCS-4	- Increased possibility for the occurrence of traffic congestions (C13) on critical links - Increased possibility for the occurrence of a network partition (C10) in case of critical node failing
C10	Occurrence of network partition	E2, E3	NSC-2, NSC-3, NCS-4, NSC-6	- Missing connectivity between the partitions leads to unavailability of services - Violations in the configuration defined through clustering algorithm - Inconsistent global network view due to missing synchronisation between distributed NFV orchestration resulting from missing connectivity
C11	Gain of physical resources	E4	NCS-3, NCS-6	- Violations in network topology defined by clustering algorithms as well as missing global network view due to unconfigured and unmaintained resources - Increased possibility of merging of network partitions (C12)
C12	Merging of network partitions	E4	NCS-2, NCS-3, NCS-4, NCS-6	- Possibility of duplicates services hampering overall service provisioning - Possibility of IP address conflicts hampering the connectivity within the network - Inconsistent global network due to missing synchronisation within distributed NFV orchestration
C13	Traffic congestion	E5, E6	NCS-2	- Increased possibility for an impaired service performance
C14	Low node battery	E1	-	- Increased possibility to create a critical node/links

The network infrastructure of the WMN-based disaster network is permanently exposed to different environmental-based events (E*n*). Those following events might result in a challenge (C*n*) which is in return influencing the desired normal behaviour of the network. Since the nodes in the WMN-based disaster network are battery-supplied, their battery will drain over time and will nearly be exhausted (E1). In case of the battery being completely exhausted, the corresponding node fails predictably since the battery status is retrievable (E2). However, an integrated node in the network might also fail spontaneously due to its destruction (E3) by an event resulting from the disaster environment such as an aftershock or outbreaking fires. Additional outdoor routers might be deployed by the rescue helpers to expand the geographical range of the disaster network resulting in new nodes spontaneously joining the network (E4). Due to the progress of the disaster and its management, there might be a high number of users in one section of the network (E5). Lastly, due to the environment of a disaster and the usage of a wireless transmission medium, one or multiple links in the network might be affected by ongoing short-lasting interferences (E6) hampering the connection between the nodes. A long-lasting interference cutting off a node from other nodes and thus from the network itself is interpreted as a spontaneous node failure (E2) in this context.

Each of these environmental-based events might result in one or multiple challenges (Cn) affecting the disaster network. The amount of occurring challenges is depending on the current configuration within the disaster network. The possible challenges (Cn) are shown in Table I. Each challenge that may result from a possible environmental-based event is described by the main normal state condition (NSC) it is influencing and the influences it might has on the WMN-based disaster network. It shall be noted, that challenges related to security and abnormal behaviour of a service related to a malfunction within the implementation of the service are assumed not to take place. As presented in [2], security related aspects are prevented through a secure client access, as well as the encryption of the user communication and traffic related to the management of the network.

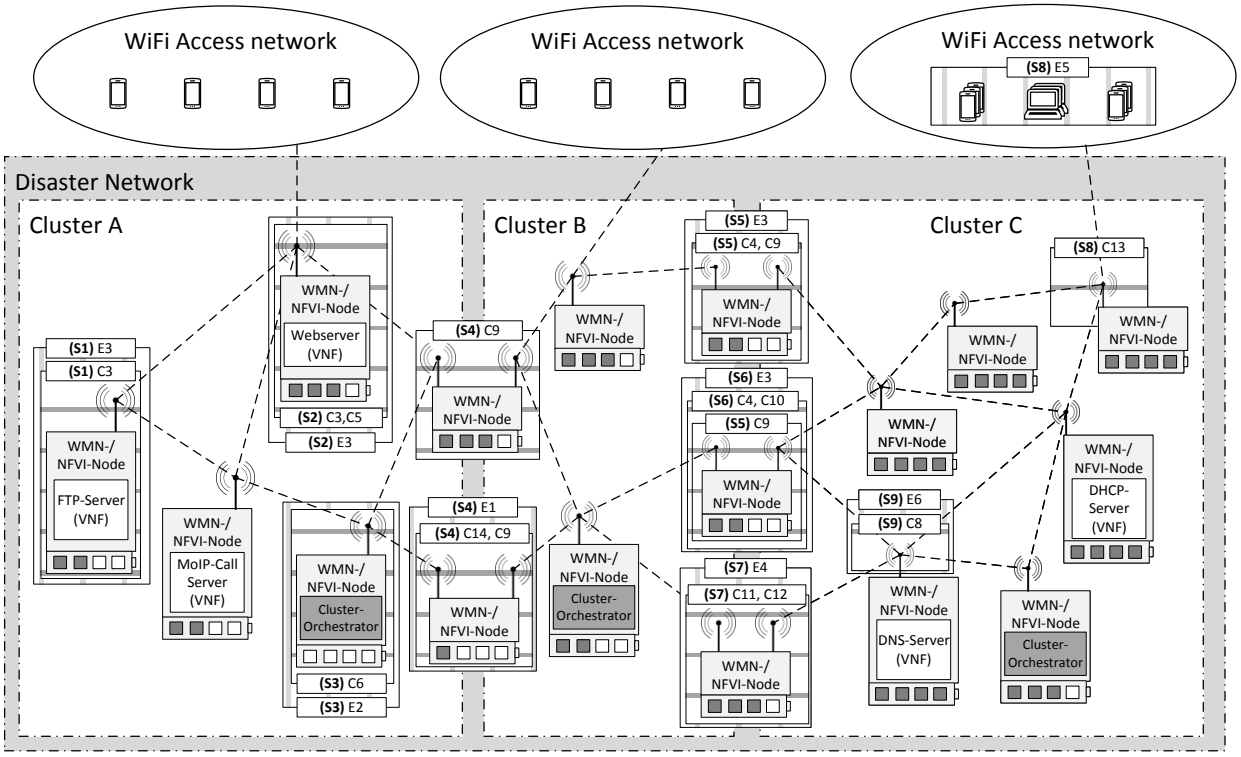

Figure 3. Possible challenges and resulting influences affecting the normal state of the WMN-based disaster network

As already mentioned, Figure 3 shows the relation of occurring environmental-based events (E*n*) and the resulting challenges (C*n*) based on the configuration of the infrastructure of the WMN-based disaster network by using different scenarios (S*n*), which are described in the following. It shall be noted that the scenarios do not necessarily follow any chronological order expect for scenarios S5 to S7, which will be explained in more detail later. Additionally, it shall be pointed out that a node failure at least results in the challenges C1 and C2 and are not explicitly mentioned within the figure nor within the following description of the scenarios.

The scenarios S1, S2, and S3, taking place in cluster A of the network shown in Figure 3, are showing exemplary challenges (C3, C5, C6) related to the loss of a resource allocated on a node failing due to a harmful environmental-based event. The loss of the corresponding resource results in possible influences on the network which are further explained in Table I.

Scenario S4 taking place between cluster A and cluster B of the disaster network shown in Figure 3 shows, that an occurring environmental-based event, other than in the previous scenarios, does not necessarily result in a challenge located at the location of the event itself, but can also cause challenges on other nodes or sections within the network. In case of scenario S4, a nearly exhausted battery (E1) creates critical nodes which are increasing the risk of a network partit-ion (C9) since their failures will create a network partition.

This aspect is also shown in scenario S5 located between cluster B and cluster C, in which a spontaneous node failure (E3) is causing another node to become a critical node and thus increases the possibility of a network partition (C9). This network partition is taking place in scenario S6 due the failure of the previously denoted critical node (E3). The occurrence of a network partition (C10) is the worst-case scenario in regard of the usability of the WMN-based disaster network. Due to the limited range of a Wi-Fi signal and the resulting physical separation, users in one partition are not able to communicate with users in the other partition. However, in the case of a network partition, each partition is required to provide and maintain the normal state defined in section II to ensure a suitable communication within each partition until the network partition is recovered.

The recovery of a network partition is achieved through the physical optimisation of the disaster network by the first responders through the deployment of a new battery-supplied wireless outdoor router. This is shown in scenario S7 where a new node is joining the network (E4) resulting in the gain of additional physical resources (C12). Due to the geographically deployment, the node is also responsible for the merging of the previous network partitions (C11). Although the gain of additional physical resources and the merging of network par-titions is not negative, it does cause a challenge in the disaster network due to the required adaptations in the configuration of the network infrastructure to achieve the normal state.

Scenario S8 and S9 are not affecting the hardware of the network infrastructure directly through a node failure but may cause a degradation of the service performance. This result either from an occurring traffic congestion (C13) being a consequence of a large number of users (E5) in one region

of the disaster network in scenario S8 or from ongoing short-lasting interferences (E6) hampering the performance on the corresponding links (C8) in scenario S9.

IV. Appropriate Measures and Emergency Corrections for Engaging the Challenges

The possible challenges presented in section III impose a large variety of influences onto the normal state of the WMN-based disaster network presented in section II. Maintaining the normal state of the network is the most important aspect for achieving resilience and therefore the usability of the network even in the event of occurring challenges. Since the distributed NFV orchestration is majorly responsible for maintaining the normal state of the disaster network, different mechanisms and actions are required which the orchestration can utilise. These actions and mechanisms are shown in Table II. For each possible challenge, possible measures are defined which shall reduce the influences of the challenge or even prevent the challenge itself. Additionally, different emergency corrections are proposed for each challenge which shall support the distributed NFV orchestration in achieving the normal state again quickly after the occurrence of a challenge has been identified. The emergency corrections are either immediate or long-lasting. Immediate corrections shall be executed right after the identification of an occurring challenge, while long-lasting corrections shall be executed afterwards.

The possible measures and emergency corrections listed in Table II can be reflected onto the inner real-time control loop D^2R^2 of the resilience strategy described in the introduction (see Figure 1). The possible measures for preventing and/or reducing the impact of a challenge can be interpreted as defensive mechanisms for the network. The immediate emergency corrections, which shall be used directly after the detection of a challenge, are representing the remediation part, while the long-lasting emergency corrections are responsible for retrieving the normal state of the network and thus corresponds the recovery part of the inner control loop.

An analysation of Table I shows that most of the harmful challenges and corresponding influences, such as the loss of any kind of resource (C1-C6) as well as challenges related to a possible network partition (C9-C10), result from environmental-based events of a node failure either through an exhausted battery (E2) or through the nodes destruction (E3). Defending the disaster network against these events through possible measures can therefore be assumed as crucial. Regarding the node failure through an exhausted battery (E2), the disaster network is required to maintain a uniform energy-consumption to avoid relatively high energy-consumption on a single node through a high workload and thus its early failure. This can be achieved through the monitoring and analysation of the network infrastructure in regard of the energy consumption of each individual node. In case of the identification of a relatively high energy consumption on one node to its surrounding nodes, the node can be relieved from the workload by the reallocation of the energy-consuming resources onto another node and therefore avoid an arising challenge (C14) and ensure a uniform energy level among the nodes.

The information collected during the monitoring process can also be used to prevent other challenges. By monitoring the traffic load on the links and the numbers of users at the different access points in the network, it is possible to observe trends regarding an upcoming traffic congestion (C11) and if necessary, to intervene prematurely by optimising the placement and allocation of resources within the network.

Spontaneous node failures resulting from the destruction of the nodes hardware cannot be prevented from happening. To defend the network against this harmful event and the resulting challenges, the possibility of any resource in the network failing at any time needs to be expected. To take precautions and measures against this scenario, the resources must be secured against its possible failure through the maintenance of fallback resources or fallback configuration.

Some challenges (C8, C11, C12) cannot be prevented nor can their impact be reduced. This results from the spontaneous nature of their corresponding environmental-based events of the deployment and therefore joining of a new node (E4) and the occurrence of ongoing short-lasting interferences (E6).

In case of a scenario of an occurring challenge, which could not be prevented in prior, emergency corrections (see Table II) are executed. An immediate emergency correction resolves and remediates the influences resulted from a challenge and avoid a serious misbehaviour of the network. Further long-lasting emergency corrections shall retrieve the desired normal state and thus recover the network in general.

A challenge resulting in the loss of a resource (C1-C6) is compensated instantly through the initialisation of a fallback component or the enforcement of fallback configurations, which are both been maintained through the previously presented measures. Since the network location of the fallback component or configuration might not be ideal in terms of an optimal normal state of the network, the long-lasting emergency corrections are further evaluating the state of the network through different algorithms and will recover the network to its optimal normal state.

Special issues are resulting from challenges related to network partitions. As already mentioned in section II, in case of a network partition, each partition needs to operate as an individual disaster network and thus provide the defined normal state. To ensure this aspect, the distributed NFV orchestration needs to coordinate itself in case of an identified risk for a network partition (C9). The coordination includes the determination of the most suitable configurations that need to be executed after the occurrence of a network partition (C10). These predefined configurations shall enable a fast attainment of the normal state in the possible future network partitions. In addition, arrangements must be made to reduce the management complexity resulting from the merging of network partitions (C12). To provide the distributed NFV orchestration these mechanisms special algorithms are used, which are not further part of this research project.

TABLE II. MEASURES AND EMERGENCY CORRECTIONS FOR POSSIBLE CHALLENGES AFFECTING THE WMN-BASED DISASTER NETWORK

C*n*	Possible occurring challenge	Possible measure for preventing/reducing the impact of the influence(s)	Immediate and/or long-term emergency corrections to maintain normal state
C1	Loss of wireless link	- Maintenance of fallback forwarding paths through the network and fallback cluster configurations	- Immediate: Usage of fallback forwarding path or rediscovery of new forwarding path through WMN routing protocol if lost wireless link was part of a used path - Long-term: Determination whether cluster configuration is still valid according to clustering algorithm and reconfiguration of clusters if required
C2	Loss of physical resources	- Maintaining and ensuring a uniform energy consumption within the network if node failed due to exhausted battery	- Immediate: Remove all resources linked to the lost physical resources from global network view to maintain its correctness
C3	Loss of service	- Maintenance of a fallback unit of the service - Maintenance of a data backup of crucial service data/information through a redundant geographically distributed data storage	- Immediate: Initialisation of the fallback unit of the service with service data/information from maintained data backup - Long-term: Creation and maintenance of a new fallback unit and new data backup for preventing an additional service failure
C4	Loss of cluster gateway	- Maintenance of a fallback cluster configuration for possible gateway failures	- Immediate: Reconfiguration of the clusters according to the fallback cluster configuration to maintain latest output of clustering algorithm - Long-term: Reconfiguration of clusters according to new output of clustering algorithm
C5	Loss of Wi-Fi-based AP	- Maintenance of fallback APs in range for each AP to ensure geographical coverage of access network	- Immediate: Initialisation of maintained fallback APs to ensure geographical coverage of access network
C6	Loss of distributed NFV orchestration unit	- Maintenance of a geographical distributed fallback unit for each unit of the distributed NFV orchestration - Monitoring the availability of the units among themselves - Distribution of configurations/information of responsible resources to other units for the purpose of redundancy	- Immediate: overtaking responsibility of failing unit by another unit of the distributed NFV orchestration using the previously distributed information - Long-term: Initialisation of the fallback unit for permanently taking over tasks/responsibilities - Long-term: Initialising new fallback instance for new orchestrator unit
C7	Teardown of the distributed NFV orchestration	- See “Possible measure for preventing / reducing the impact of the influence(s)” of challenge C6	- Immediate: Execution of algorithm for the reinitialization of the distributed NFV orchestration including the discovery of current configurations within the network
C8	Inconsistent connectivity	- Not possible due to the spontaneous nature of wireless interferences (E6)	- Immediate: Prevent traffic forwarding via inconsistent link by defining or discovering new network paths - Long-term: Reallocation of affected service(s) to increase service performance if required
C9	Risk of network partition through critical node(s)	- Observation and analysation of possible critical areas within the network regarding node density	- Immediate: Ensuring maximal lifetime of critical node(s) by optimising its energy consumption through cluster reconfiguration and service reallocation to relief node from workload - Immediate: Notification towards network administrators for required physical optimisation - Long-term: Coordination within distributed NFV orchestration regarding possible occurrence of network partition (definition of configurations regarding services and clusters after network partition took place) and aspects for decreasing the complexity in case of a possible merging of the partitions
C10	Occurrence of network partition	- See “Immediate and/or long-term emergency corrections to maintain normal behaviour” of challenge C7	- Immediate: Notification towards network administrators for immediate required physical network optimisation - Immediate: Execute plans defined in prior (see “Immediate and/or long-term emergency corrections to maintain normal behaviour” of challenge C9) - Long-term: Provide normal behaviour in all network partitions and expect merging of network partitions (C12)
C11	Gain of physical resources	- Not possible since the deployment of new battery-supplied outdoor routers is occurring spontaneously without any previous notification by the network administrators	- Immediate: Integration of unconfigured and unmaintained resources into the NFVI through the distributed NFV orchestration to ensure a global network view - Long-term: Reconfiguration of clusters according to cluster algorithm using obtained new global network view
C12	Merging of network partitions	- In case of previous network partition was predictable: see “Immediate and/or long-lasting emergency corrections to maintain normal behaviour” of challenge C7, otherwise not possible	- Immediate: Synchronisation between units of the distributed NFV orchestration to obtain new global network view - Long-term: Reorganising services, clusters and address spaces to achieve normal behaviour within the newly created partition
C13	Traffic congestion	- Analysation of user location and movement as well as their traffic - Optimisation of user traffic within the network through service reallocations	- Immediate: Reallocation of clusters according to algorithm with specific focus on overcoming the traffic congestion - Immediate: Scale-out of service(s) to distributed workload (if possible) - Immediate: initialisation of additional APs in affected region to relief access networks (if congestions result from too many users)
C14	Low node battery	- Maintaining and ensuring a uniform energy consumption within the network	- Immediate: reduce workload on node to a minimum - Immediate: Notification towards network administrator for required physical optimisation - Long-term: analysing the impact of a possible node failure and resulting possibly subsequent challenges

V. Conclusion and Summary

The usability of an emergency communication infrastructure is its most crucial aspect. It can be ensured by achieving a resilient the communication infrastructure. To achieve a resilient network, some aspects need to be defined in prior. The normal state of the network needs to be defined as well as different challenges that might affect the normal state. These aspects have been defined and derived in detail for a resilient WMN-based disaster network.

The defined normal state of the resilient WMN-based disaster network consists of multiple conditions. A distributed NFV orchestration needs to be existing since it is mostly responsible for maintaining the resilience of the network. The service requirements must be met to ensure a useful user communication within the network. The complete network infrastructure needs to be maintained and observed by the orchestration for identifying occurring challenges affecting the network. The connectivity between all nodes within the network must be existing to ensure that all users can communicate with each other independent of their location. Wi-Fi-based access points need to be available to provide the users a suitable access to the network and its functionality. While the network infrastructure itself needs to be configurated according to a specific clustering algorithm to ensure enough bandwidth within a multi-hop communication.

To achieve the desired resilience, this normal state needs to be defended against challenges resulting from the environmental-based event affecting the WMN-based disaster network. Through the definition of the challenges and their possible influences, the distributed NFV orchestration can detect their occurrence. To defend the network against the challenges or even prevent them, individual measures are defined for each challenge. In addition, emergency corrections for remediating the influences of an occurring challenge as well as recovering the network to its normal state were defined, which the distributed NFV orchestration can utilise.

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

[2] G. Frick, A. P. Tchinda, B. Shala, U. Trick, A. Lehmann, and B. Ghita, "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)*, 2019, pp. 1–6, doi: 10.1109/ICT-DM47966.2019.9032953.

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

[4] E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Comput. Networks*, vol. 54, no. 8, pp. 1245–1265, Jun. 2010, doi: 10.1016/J.COMNET.2010.03.005.

[5] G. Frick, A. Lehmann, G. Frick, A. P. Tchinda, and B. Ghita, "Distributed NFV Orchestration in a WMN-Based Disaster Network," in *International Conference on Ubiquitous and Future Networks, ICUFN*, 2018, vol. 2018-July, pp. 168–173, doi: 10.1109/ICUFN.2018.8436705.

[6] G. Frick, A. P. Tchinda, U. Trick, A. Lehmann, and B. Ghita, "NFV Resource Advertisement and Discovery Protocol for a Distributed NFV Orchestration in a WMN-based Disaster Network," in *2019 27th International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2019*, 2019, doi: 10.23919/SOFTCOM.2019.8903694.

[7] ETSI, "Network Functions Virtualisation (NFV); Resiliency Requirements," *ETSI GS NFV-REL 001 V1.1.1*, vol. 1, no. 1, pp. 1–82, 2015, doi: DGS/NFV-0011.

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

[9] J. Núñez-Martínez and J. Mangues-Bafalluy, "A Survey on Routing Protocols that really Exploit Wireless Mesh Network Features," *Journal of Communications*, vol. 5, no. 3. pp. 211–231, 2010, doi: 10.4304/jcm.5.3.211-231.

[10] A. Joshi, H. Gossain, J. Jetcheva, M. Audeh, and M. Bahr, "HWMP specification," *IEEE P802.11 Wirel. LANs Doc. IEEE 802.11-06/1778r1*, vol. 11, 2006.

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

[12] V. Sucasas, A. Radwan, H. Marques, J. Rodriguez, S. Vahid, and R. Tafazolli, "A survey on clustering techniques for cooperative wireless networks," *Ad Hoc Networks*, vol. 47, pp. 53–81, 2016, doi: 10.1016/j.adhoc.2016.04.008.