M. Tornatore, J. Andre, P. Babarczi, T. Braun, E. Følstad, P. Heegaard, A. Hmaity, M. Furdek, L. Jorge, W. Kmiecik, C. Mas Machuca,
L. Martins, C. Medeiros, F. Musumeci, A. Pasic, J. Rak, S. Simpson, R. Travanca, A. Voyiatzis
"A Survey on Network Resiliency Methodologies against Weather-based Disruptions"
In Proc. RNDM 2016 - 8th International Workshop on Resilient Networks Design and Modeling, Sept. 13-15, 2016, Halmstad, SE, pp. 23-34
ISBN: 978-1-4673-9023-1 http://dx.doi.org/10.1109/RNDM.2016.7608264 http://ieeexplore.ieee.org/document/7608264/

A Survey on Network Resiliency Methodologies against Weather-based Disruptions

Massimo Tornatore [*], Joao André [xiii], Péter Babarczi [¶], Torsten Braun [**], Eirik Følstad [‡‡],
Poul Heegaard [‡‡], Ali Hmaity [*], Marija Furdek [§], Luisa Jorge [‡], Wojciech Kmiecik [xii],
Carmen Mas Machuca [x], Lucia Martins [xiv], Carmo Medeiros [xiv], Francesco Musumeci [*],
Alija Pašić [¶], Jacek Rak[‖], Steven Simpson [xi], Rui Travanca [††], Artemios Voyiatzis [†]

[*] Politecnico di Milano, Department of Electronics, Information and Bioengineering, Milan, Italy
[‡] Instituto Politécnico de Bragança and INESC Coimbra, Bragança, Portugal
[§] KTH Royal Institute of Technology, Stockholm, Sweden
[¶] MTA-BME Future Internet Research Group, Budapest University of Technology and Economics (BME), Hungary
[‖] Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics, Poland
[**] University of Bern, Switzerland, [†] SBA Research, Vienna, Austria
[††] Dept. of Civil Engineering, Universidade de Aveiro, 3810-193 Aveiro, Portugal
[‡‡] Norwegian University Of Science and Technology, Trondheim, Norway
[x] Technical University Munich, Germany, [xi] Lancaster University, United Kingdom
[xii] Wroclaw University of Technology, Poland
[xiii] National Laboratory for Civil Engineering (LNEC), Lisbon, Portugal
[xiv] Dept. of Electrical and Computer Engineering & INESC, University of Coimbra, Coimbra, Portugal

E-mail: *massimo.tornatore@polimi.it*, *jandre@lnec.pt*, *babarczi@tmit.bme.hu*, *braun@inf.unibe.ch*, *eirik.folstad@item.ntnu.no*, *poul.heegaard@item.ntnu.no*, *ali.hmaity@polimi.it*, *marifur@kth.se*, *ljorge@ipb.pt*, *wojciech.kmiecik@pwr.edu.pl*, *cmas@tum.de*, *cmedeiros@deec.uc.pt*, *lucia@deec.uc.pt*, *pasic@tmit.bme.hu*, *francesco.musumeci@polimi.it*, *jrak@pg.gda.pl*, *s.simpson@lancaster.ac.uk*, *rui.travanca@ua.pt*, *avoyiatzis@sba-research.org*

***Abstract*—Due to the increasing dependence on network services of our society, research has recently been concentrating on enhancing traditional protection strategies to withstand large-scale failures, as in case of disaster events. The recently-formed EU-funded RECODIS project aims at coordinating and fostering research collaboration in Europe on disaster resiliency in communication networks. In particular, the Working Group (WG) 2 of the RECODIS project focuses on developing new network-resiliency strategies to survive weather-based disruptions. As a first step, WG2 members have conducted a comprehensive literature survey on existing studies on this topic. This paper classifies and summarizes the most relevant studies collected by WG2 members in this first phase of the project. While the majority of studies regarding weather-based disruptions deals with wireless network (as wireless channel is directly affected by weather conditions), in this survey we cover also disaster-resiliency approaches designed for wired network if they leverage network reconfiguration based on disaster "alerts", considering that many weather-based disruptions grant an "alert" thanks to weather forecast.**

***Index Terms*—weather-based disruptions; disaster resilient communications; network resilience; disasters; failures;**

I. Introduction

This paper is intended to provide a survey of existing studies on network resiliency against weather-based disruptions. Specific weather conditions (e.g., heavy rain fall, extreme winds, fog) can lead to partial degradation of network performance characteristics, e.g., the capacity of wireless links can decrease significantly due to signal attenuation in the presence of heavy rain [1]. On a larger scale, other more-impacting weather condition (e.g.,weather-based disasters as hurricanes, or tornadoes) can cause very extensive network disruptions (consider, e.g., the extent of damage caused by the hurricane Katrina in New Orleans in 2005 [2]).

Partial degradations usually last for limited time periods, typically shorter than in the case of extensive disaster failures. Yet, these relatively short time periods of disruption (measured in minutes or hours) can be very significant for critical infrastructures, especially nowadays that several crucial activities of our society rely on telecom-network services. Problems considered by existing literature on weather-based network-performance degradation are mostly related to access networks (local and metropolitan) and wireless technologies, which still form an important part of the global communications infrastructure.

As for more extensive weather-based failures (e.g., hurricanes, or tornadoes), the large geographical footprint of such failures makes them relevant also for wired networks and as well as in the core segment of the network. In these cases, it is important to develop the mechanisms of network preparedness to incoming catastrophic weather conditions,

e.g., by reconfiguring network topologies in advance. It is important noting here that one of the main difference between resiliency techniques against natural and man-made disasters (e.g., earthquakes, terrorist attacks, as those studied in the WG1 of the RECODIS project) and weather-based disasters is the fact that, with good probability, changing weather conditions are announced by weather forecast and that grants to network operators some time to reconfigure the network before the disaster strikes (consider, e.g., hurricane forecasts). In the rest of the paper we will refer to this granted interval of time as "alert".

While disaster-resilient planning strategies, as the one studied in WG1, ensure that the network is designed with minimum disaster risks based, e.g., on disaster probabilities, we consider in this survey studies where the probability of an incoming weather disruption can be extremely time-varying. In response to an upcoming disaster alert, such a reconfiguration might need to be performed in a very limited time scale, ranging from minutes to hours depending on the type of alert.

The COST CA15127 RECODIS Action will develop appropriate solutions to provide cost-efficient resilient communications in the presence of disaster-based disruptions, considering both existing and emerging communication network architectures. As a first step towards achieving the goals of RECODIS, and within the context of the activities of Working Group 2, a survey of strategies for communication networks to protect against weather-based disruption is presented here. For reader's convenience, we summarize the proposed contributions, divided per aerea, in Tab. I.

The survey is organized as follows. Section II overviews studies on the modeling of weather-based disruptions on telecom networks. In Section III weather-based resiliency studies in wireless networks are discussed, while in Section IV we present alert-based resiliency studies applicable in wired networks against weather-based disruptions. Section V focuses on the emerging trend of weather-based resiliency in converged networks. In Section VI, the role of more advanced network paradigms, as delay tolerant networking, is discussed. Finally, we conclude our survey in Section VII.

TABLE I
SUMMARY OF THE PROPOSED CONTRIBUTIONS PER AREA

Contributions			References
Modeling weather-based disruptions on telecom networks	Modeling infrastructure disruption		[3] [2] [4] [5] [6] [7] [8] [9]
	Effect on wireless channel quality		[1] [10] [11] [12]
	Impact of structural design		[13] [14] [15] [16] [17]
Weather-based resiliency studies in wireless networks	Protection strategies		[18] [19] [20] [21] [22] [23]
	Optimization and survivability models	Wireless Mesh Networks	[24] [25] [26]
		Free Space Optics	[27] [8]
Alert-based weather-based resiliency in wired networks	Network connectivity		[28] [29] [30] [31] [32] [33] [34] [35] [36]
	Cloud networks		[37] [38] [39] [40] [41] [42]
Advanced topics in weather-based resiliency	Converged networks		[43] [44] [45] [46] [47] [48]
	Advanced technologies (DTN, ICN)		[49] [50] [51] [52]

II. Modeling the effect of weather-based disruptions on telecom networks

A. Modeling infrastructure disruption

In building disaster models such as a spatial-temporal model described in [3], we need to understand how undesired events occur, how they are correlated, move/propagate, and cascade. The observations made and lesson learnt from major infrastructure disruption are used as a basis for such models. Two examples are the increased knowledge of disaster impact on the telecommunications power infrastructure from the Hurricane Katrina [5] and Great East Japan Earthquake [2], and recovery from these disasters. An on-site survey from the Hurricane Katrina conducted in October 2005 addressed the effects, failure modes, causes, and duration, which are included a fault tree analysis (FTA), and a summary table of the main failure causes and restoration strategies in the wired and wireless communication networks [5]. In [2] a detailed description is given of the damages of the earthquake (main shock and aftershock) and the following tsunami, including how the number of power outages affecting the telecom buildings changes over time after the main shock. Also during Hurricane Ike (strongest hurricane in 2008 - Galveston, Texas, September 13, 2008), the reachability of subnets was evaluated through data related with Border Gateway Protocol (BGP) update messages from subnets in Texas area during September 10-20. The time correlation between the reachability of the network and the overlapping of the storm coverage and the subnet locations (which are known only approximately) was analysed. Some subnets became unreachable before the hurricane reached any subnet region. Power outage and lack of spare power were found as being the most important causes to justify the low correlation obtained [4]. Similar other investigations exist for other weather-based disasters as in [6], [7]. Models of disaster effects on network infrastructures can be used for network survivability quantification. In [8] it is shown a scalable approach using a Markov model approach to describe the transient effects on network performance of an undesired event, until the network is restored to an operational state, and then until it has completely recovered. This is compliant with the survivability quantification definition of ANSI-T1A1.2 given in [9].

B. Effect on wireless channel quality

As wireless networks operation can be heavily affected by weather conditions, in these last years different modeling studies have tried to capture the effect of weather condition on wireless channel quality. In [10], authors focus on the impact of fading from weather conditions on Free Space Optical (FSO) systems and propose a new technique to mitigate the negative influence of atmospheric effects. Various systems

were compared with the Multiple Input Single Output (MISO) multi-hop Decode and Forward (DF) relay FSO system using M-array Pulse Amplitude Modulation (M-PAM), concluding that multi-hop system based PAM modulation have superior performance, especially when increasing the number of relays. Authors in [11] investigate the dynamic property of a tropical-forested channel due to the weather effect on Very High Frequency (VHF) and Ultra High Frequency (UHF) radio-wave propagation. The main idea is to design a fade margin for VHF/UHF communication system in a tropical environment. The experimental results indicate that the wind and the rain can impose an additional attenuation on the propagation signal within critical environment. Authors modeled the temporal fading components due to the weather and draw a specific statistical fading model. Further analysis is made on the effect of the Rician K factor and the intensity of wind and rain. On the other hand, Wireless Sensor Networks (WSN) integrate functions of sensing, computation and communication to monitor a wide range of environmental parameters. In [1] authors study the effect of temperature and humidity on radio signal strength in outdoor WSNs. Experimental measurements were performed using *Atmel ZigBit* 2.4 GHz wireless modules, both in summer and wintertime and testing over all the channels specified by IEEE 802.15.4 for 2.4 GHz ISM frequency band with two power levels. Their finding suggest that temperature has negative, linear effect on signal strength in general, while high relative humidity may have some effect, particularly when temperature is below 0°C. They also show that frequency diversity can alleviate the effects of channel-specific variation. Such finding can be useful for designing algorithms and protocols which are adaptive and robust against the effects of weather variation. Ref. [12] proposes a scheme to reduce the influence of weather conditions for hybrid WSN when hybrid WSN having both Radio Frequency (RF) and Free Space Optics (FSO) links for communication. The main idea is use multiple thresholds to activate transmission of RF and switch from RF to FSO and vice-versa. The experimental results under fog, snow and rain events show that the power consumption saving of RF transmission can be reduced significantly, and that the network lifetime in harsh terrestrial environment is doubled with respect to the case of RF links transmissions only.

C. Ensuring wireless channel quality by structural design

In a typical cellular network, wireless transmission equipment, i.e., mostly the antennas (possibly co-located with some baseband-processing hardware), can be placed in various locations and supporting structures. Figure 1 shows two possible supporting structures: a monopole and a lattice tower. In both cases, the structure is subject to significant deflections and rotations that affect the wireless channel quality. So, considerations regarding structural design need to be discussed.

Standards are a very important part of engineering practices, serving as rules that engineers must comply. Structural design

Fig. 1. Antennas mounted on a lattice tower (on the left), antennas mounted on a monopole (on the right).

standards are typically aimed at ensuring the proper structural safety of the physical infrastructure hosting the antenna within the range of diverse hazards that it will be exposed to. While the prevention of collapse is of primary importance, the real purpose of communication structures is to transmit signals, regardless of the weather conditions. However, this primary purpose cannot be achieved if the flexibility of the structure is such that deflections and rotations at the points of support of the antennas exceed permissible values. The main concern for the network operator is not exceeding the permissible values, but instead the time during which such permissible value is exceeded. In the case of communications structures, the so called “serviceability limit state” is generally defined as the state that will cause an unacceptable reduction in the level of service provided by the antenna system mounted on the structure, i.e., the serviceability limit state is reached when the signal level is reduced below an acceptable limit by loss of alignment caused by twisting or tilting of the antenna. The concept of unacceptable signal, resulting in “outage”, is extremely complex, potentially being influenced by the sensitivity of the electronic equipment and its ability to recover after momentary excessive structural deflection in a short duration gust. Thus, not only the wind speeds, and the associated gusts, are important, but also the performance of the electronic equipment [14]. Other weather conditions, e.g. rain or icing, may also affect the signal performance. In the structural design, many aspects are frequently ignored when estimating deflections of antennas using numerical simulation, e.g., soil-structure interaction, deflection of antenna mounting system, a more refined mass distribution and/or stiffness loss. Such aspects should not be overlooked [15], [16].

Most standards provide guidance to determine the relevant deflections, rotations, or the duration curve to be used to determine time that the wind speed is exceed. The American and Australian standards provides specific limits to allowable deflections and rotations, but for the United Kingdom and Canadian standards, it would be up to the network operator to assess if such outage durations were acceptable. The Eurocode provides no guidance on limits for communication structures, but gives guidance to the network operator on what parameters

need to be considered when setting his specifications or design criteria. However, with the current economic environment and market pressure, many of these structures are ordered by clients whose knowledge of the structural requirements is relatively limited [14], [17]. This is possibly motivated by the relatively low cost of the structure compared with that of the network equipment it supports, thereby concentrating the attention of the network operator on the overall cost. On the other hand, it can also be argued that a relatively small investment in a properly designed supporting structure would not increase significantly the overall cost [14]. The high number of failures observed in structures used as support of cellular antennas motivates the need to treat their design, fabrication, construction and maintenance extremely carefully [14], [13], [17], [16]. The continuous evolution in the constructional field, e.g., with the increasing strength of the materials used and the new structural forms adopted, emphasizes the increasing difficulty of a proper evaluation of the actions and effects of wind on more slender and lightweight structures, such as monopoles. As a static problem, i.e., a cantilever beam with one or more concentrated masses, is probably the simplest in the structural field. However, a deeper investigation on monopoles reveals a completely different scenario, i.e., under wind action they are subject to complex dynamic effects giving rise to potentially unstable conditions [16]. Also, the consequences in the codification sector are evident, i.e., specific standards exist but based on empirical calculation criteria that need to be reviewed and updated. The frequent abnormal vibrations as well as some failures observed in these structures confirm the need for a better understanding of wind-excited behaviour [13], [16].

The business response is to keep expenditure to a minimum and increase revenues. Mainly due to market pressures, investments are short-term intended, focusing on replacing and renewing as needed rather than modernising key physical infrastructure, and expenditure takes place in response to a crisis rather than proactively planning and managing key physical infrastructures. Also, the focus is on operating at near maximum operational capacity of the physical infrastructure which is viewed as being an optimal and efficient management decision. This, however, causes the systems to be less resilient against anticipated or unknown climatic and socio-demographic changes during the infrastructures lifespan. In conclusion, to properly plan and manage key physical infrastructures it is necessary to gather a correct understanding of the structural behaviour of such structures. Therefore, there is an urgent need to apply advanced research methods, e.g., structural health monitoring, experimental testing and numerical simulation, and develop a comprehensive risk framework to elaborate new, and review existing, design guidelines, which will contribute to overcome the existing weaknesses.

III. Resiliency against Weather-based disruptions in Wireless networks

Wireless technologies play a key role in today's network infrastructures. Originally intended mostly as a support technology for the last mile, they are becoming promising alternative to wired metro networks, due to the long-term planning, high capital expenditures (CAPEX) and operating expenses (OPEX) required by wired (mostly fiber-based) network deployments in metro ares. Wireless networks are relatively fast and cheap to deploy and can work in several topological shapes (ring, star, mesh ect.). Often, when planning a robust and survivable wireless network, mesh networks are considered to be the most reliable solution. However, due to the nature of wireless communications, wireless links are very susceptible to weather disruption and this section aims at providing a survey of the main challenges that weather-based disruption poses to wireless networks.

Several technologies have to be considered when planning a wireless network. These include:

- Millimeter-wave (MW) technology, which can achieve transmission rates of 1-10Gbps per a millimeter-wave link (utilizing the 71-86GHz band) [19]. Note that compared to lower bands, radio waves in this band have high atmospheric attenuation. Therefore, this band is better suited for very short range (1-2 kilometer) point-to-point and point-to-multipoint applications.
- FSO (Free Space Optics), a technology that uses light propagating in free space for wireless data transmission. Most of the manufacturers use the wavelengths between 800 and 1550nm (preferred) [24]. FSO links may carry from 10Mbps to 10Gbps, up to 3km distance. The optical beam is highly attenuated by fog and other airborne particles.
- Microwave technologies (3-30GHz) can achieve transmission rates up to 3Gbps with large coverage distance and are not so vulnerable to precipitation (especially under 10GHz). For instance WIMAX (Worldwide Interoperability for Microwave Access), which works at data rates of 300Mbps to 1Gbps, can provide a coverage distance up to 30km under Line Of Sight (LOS) situations and a typical cell range of up to 8km under No LOS (NLOS) [53].
- Mobile technologies (GSM, UMTS, LTE ect.) utilize lower bands, i.e., from 225MHz to 3700MHZ and provide date rates up to 300Mbps. Note that, these networks are distributed over land areas called cells. The size of these cells varies from 10m (femtocells) to 20km (macrocells). The precipitation susceptibility is not significant.

A. Protection Strategies

1) Wireless Mesh Network (WMN): A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology and has been subject of extensive research. Early papers on wireless survivability focused only on connectivity of a network topology as a measure of fault tolerance in wireless mesh network. As connectivity turned out to be a mostly qualitative measure (not suite for carrier-grade applications), more precise measurements related to signal attenuation and partial link failures gained attention in later studies. Note that WMNs often use routing metrics based

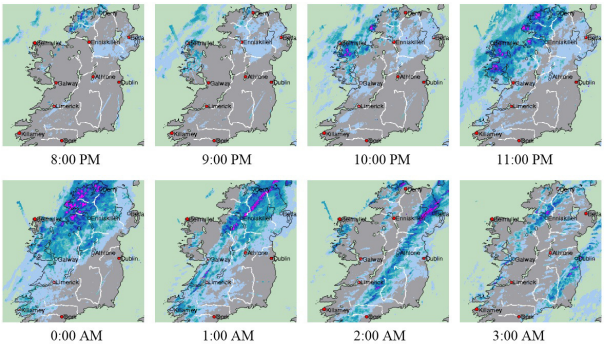

Fig. 2. Example of radar echo rain maps (Ireland, November 26-27, 2011)

on Expected Transmission count (ETX), a metric depending on the quality of the link. This metric (i.e. ETX) can be helpful when improving reliability in case of bad link states by weather impact.

When considering weather-based disruptions, two main protection strategies have to be considered (this will be discussed in details below):

- One option is to periodically update the network topology [19], [20].
- The second is to introduce rain-related link states to improve the routing mechanism [21], [18]. The rain-related link state can be either adjusted according to locally measured data (for example Bit Error Rate) or from externally measured information (e.g., radar data).

Impact of weather-based disruptions on performance of high-frequency communications in WMNs operating in 71-86 GHz band is addressed in [19] and [20]. In particular, these papers focus on the influence of heavy rain falls on the degradation of the effective capacity of WMN links. As shown in these papers, the nominal capacity of WMN links (commonly 1-10 Gbps) utilizing the 71-86 GHz band can be remarkably impacted by even moderate rain falls. To provide a proper solution to this problem, [19] introduces a scheme of proactive preparedness of a WMN network to incoming rain falls by means of periodic updates of a WMN topology in advance based on information on incoming rain falls (derived from radar echo rain maps like Figure 2). In particular, the algorithm of WMN topology reconfiguration is proposed to determine links of predicted low signal attenuation that should be present in the updated topology, as well as those transmitting information over heavy rain areas (which should be deleted). This technique provides a significant improvement in terms of reduction of the impact of rain on signal attenuation along communication paths. Technique of periodic reconfiguration of a WMN topology from [19] can be easily implemented, since it does not involve any updates of routing algorithms. Ref. [20] is an extended version of [19]. In particular, [20] additionally presents the ILP model of weather-resistant links formation problem as well as the proof of its NP-completeness.

Unlike the proposal from [19] and [20], two other techniques (called XL-OSPF and P-WARP [22], [21]) to improve performance of WMNs under weather-based disruptions rely on further enhancements of routing algorithms. In particular, routing in XL-OSPF is done based on a link-cost metric proportional to the observed bit error rate (BER) of WMN links. Instead, link costs of P-WARP (also used in routing) are estimated based on radar information concerning predicted weather conditions. An analysis of the impact of rain storms on MW links and a performance comparison of the two new routing protocols (i.e. XL-OSPF and P-WARP) that use physical-layer information to improve routing at the network level is provided in these papers. The detailed examination of several observed storms shows that most of the times, while a small number of links is severely degraded, a large set of links may be just slightly degraded or unaffected, which motivates the need of domain-specific routing protocols to use lower layer information to improve routing decisions. Both protocols demonstrate some improvement over OSPF during real rain events modelled in simulation.

In [18], authors propose a Predictive Wireless Mesh Network Routing (PWMNR) protocol which makes routing decisions using only information from the wireless link rather than from outside information regarding weather events (e.g. radar information). Note that in PWMNR each node monitors the link BER of all the links with its neighbors and uses an appropriate statistical model to predict the link BERs for certain specified time intervals into the future (unlike the XL-OSPF, where no prediction occurs). The authors present the operational protocol details as well as the implementation of a protocol simulator enabling simulation based on data from real weather events. Finally, they also present a performance comparison with other approaches, including conventional routing protocols (static routing and standard OSPF) as well as link-state-based routing (link-cost OSPF). No comparison to explicitly weather-information-based routing protocols (either reactive or predictive) is provided (although link-cost OSPF as implemented could be similar to XL-OSPF). As a result, without using any sort of weather observation or prediction, PWMNR achieves a throughput performance up to 8% higher than link-quality-based routing that also does not use prediction.

The authors in [23] consider solar powered base stations (BS) as an alternative to the absence of power grid in rural areas or at the occurrence of power outage in disaster-stricken areas. However, it is hard to cope with the dependence of the amount and rate of energy available over time. The authors propose a wireless mesh network exploiting solar energy harvesting BS. The aim is at providing reliable communication network to offer stable communication applications through the energy variation over time. The authors had some field experiments and gave some hints on toward possible performance improvement of WMNs via BS synchronization with changing link states.

2) Free Space Optics (FSO): As mentioned before, FSO (Free Space Optics) is another promising alternative for creating WMNs. Ref. [24] presents an overview of FSO communications technology enabling high-bandwidth optical wireless

transmission between stationary nodes. Characteristics of FSO technology are described with special focus on signal attenuation, scattering, scintillation (additional attenuation on the laser beam caused by atmospheric temperature and pressure variations), alignment, and full duplex transmission. The paper also points out disadvantages of FSO related to point-to-point transmission, implying e.g., that each transceiver requires accurate initial alignment as well as selftracking to preserve the proper alignment for instance during strong winds. It also highlights challenges leading to degradation of the effective capacity of FSO links, in particular related to the influence of fog, smoke, wind, sand, or heavy rain. Ref. [25] compares different FSO networks that have been implemented in Graz (Austria) and Nice (France). Although any common optical wavelength could be initially used, most of the systems use 1550nm wavelength. In this work two systems are compared: 100m and 300m range. The two systems have one receiver (photo-PIN-diode) but the 100m has one transmitter (LED - Light-Emitting Diode) whereas the 300m has 8 transmitters (LED). When replacing LEDs by Vertical-Cavity Surface-Emitting Lasers (VCSELs), the reach can be increased to 800m. These network elements can be used in different types of FSO networks, mainly using rings, star or mesh topologies. The best solution for FSO configurations will be a meshed network (unsurprisingly). This architecture combines shorter distances and high reliability, because of the location of the Optical Multipoint Unit. The combination of FSO and microwave-links is also a possible solution for increasing reliability and availability, because terrestrial FSO is most affected by fog, whereas the microwave propagation is mainly influenced by rain. These networks are called Hybrid RF/FSO Networks. In [26], authors investigate the reliability of such networks. Note that FSO links have a much higher link capacity (20-25 times of a RF link), however, they are much more vulnerable, especially to bad weather (fog, snow). Hybrid RF/FSO networks combine the merits of FSO and RF technologies by providing parallel transmission via RF and FSO links. This means that if the FSO link fails, the RF link transmits the critical data (high-priority traffic), while the non-critical data has to be rerouted in the FSO domain, if possible. To ensure the proper differentiation of recovery actions after FSO link failures, several traffic criticality classes have to be introduced. In particular, in [26], the weather-based disruption of FSO links is addressed by taking into account weather predictions and how they influence quality of FSO link existence. Note that, until now the routing and network resource allocation was determined offline, periodically. Upon failure of an FSO link, redirection of traffic in the FSO domain was considered (i.e., low-priority traffic not protected by the corresponding RF backup link), but 100% restoration was not guaranteed. In [26] a new routing metric (cost) was defined based on weather forecasts, in order to establish obscuration-tolerant paths in the FSO domain. The scheme is based on link-disjoint FSO paths providing preplanned protection in case of FSO link failures. This routing problem was proven to be NP-hard, which is why an Integer Linear program and a heuristic algorithm has been proposed.

B. Optimization and survivability models

In recent years, several useful general optimization models for survivability in WMNs were introduced. In [27], an original optimization model is presented for the Flow-Thinning Problem (FTP), formulated as non-compact linear programming problem. A resolution method based on a path generation approach is also presented. FTP is inspired by diversity path strategy and elastic rerouting, previously proposed, and therefore each demand may be routed through an over-dimensioned set of paths, not necessarily disjoint, and only a fraction of the flows traversing the affected links are saved. Some encouraging numerical results were presented comparing FTP with the global rerouting strategy, a strategy that restores flows from scratch in surviving capacity, but the authors concluded that further studies need to be carried out to evaluate the applicability of this approach. The optimization model proposed is suitable for broadband wireless networks with non-interfering point-to-point links.

Another interesting approach was introduced in [8]. The authors present survivability and network performance models (including a phased recovery model of rerouting and restoration) to study network survivability. The modeling approaches are applied to both small and real-sized network examples. Three different scenarios have been defined, including single link failure, hurricane disaster, and instabilities in a large block of the system (transient common failure). To avoid state space explosion while addressing large networks, the models are decomposed in space by studying the nodes independently, and in time by decoupling the analytic performance and recovery models, giving a closed form solution. The main purpose of the approximations proposed in the paper is to reduce the computational effort of obtaining transient solutions in large network models without an undue loss in the accuracy (under a set of assumptions described). Network survivability is quantified in terms of performance metrics like packet loss probability and the delay distribution of non-lost packets. The results provided show good correspondence between the transient loss and delay performance in the simulation and analytic approximations.

IV. Alert-based Reconfiguration against Weather-based disruptions in Wired networks

Large-scale weather-based disruptions (e.g., hurricanes, floods) are expected to be more frequent in future due to global warming. The affected areas in case of such destructive events might also affect wired networks, e.g., Wide Area Networks (WANs). In the following, as explained in the introduction, we concentrate on disaster-resiliency techniques based on the concept of “alert”, to avoid overlaps with RECODIS WG1, and we classify the surveyed approaches in techniques focused on ensuring network connectivity vs. techniques focused on cloud networks (where the role of datacentres is crucial).

A. Alert-based Reconfiguration of Network Connectivity

By modeling possible disasters (e.g., using hazard maps), their likelihood and the severity of their consequences, three degrees of preparedness (including the *post-disaster actions*) to a weather-based disruption can be obtained [28]. *Normal preparedness* entails utilizing knowledge of risky regions to pro-actively allocate network resources so that the network disruption and data losses are minimized. Although traditional protection approaches provide 100% deterministic recovery from single link failures, multiple correlated failures caused either by the primary or the cascading effects of weather-based disruptions might require unsustainable amount of backup resources to provide full protection. Thus, a promising strategy may focus on providing full-disaster protection for mission-critical services and degraded service to other applications [29]. Note that, some services are sensitive to the amount of capacity provided, while others (e.g., video streaming or file transfers) can operate with reduced bandwidth and can still achieve lower but acceptable quality. As available resources decrease dramatically during large-scale disasters, the approach of degraded-service tolerance [29] can reduce protection cost, reduce network disruption, and support maximal carried traffic.

Instead of pro-actively design (costly) recovery from random geographic failures [30], with alert-based reconfiguration of the network the risk of disruptions can be minimized in a cost-efficient manner by re-allocating critical network resources when an alarm is issued, called *enhanced preparedness* [28]. Luckily, current networking trends give excellent support for the alert-based reconfiguration of wired networks in order to maintain network connectivity. One of these trends is *Software-Defined Networking (SDN)*, which facilitates network reconfigurability and programmability and opens up new ways to reconfigure the network in reaction to a disaster alert by centralizing control logic and separating it from the physical equipment. Another trend is *network virtualization*, which enables multiple tenants to share the same underlying SDN infrastructure to improve its resource efficiency. For this, each tenant contracts a Service Level Agreement (SLA) with the physical SDN infrastructure provider, which declares minimal QoS requirements for its *virtual topology*. The responsibility of the provider is to embed the tenants' virtual topology into the *physical topology* satisfying these requirements [31]. Therefore, in order to satisfy the required resilience declared in the SLA, virtual networks might be *migrated* [32] from the current physical resources to new ones as part of the alert-based reconfiguration. Migration of virtual SDN networks (i.e., rearrangement of the existing flow configuration) boils down to the task of removing old forwarding rules from the switches and installing the new forwarding rules corresponding to the desired (e.g., failure safe) flow configuration. However, the failure of the control channel or the asynchrony of switch updates might cause performance degradation, state inconsistency and temporal over-utilization of the links, which have to be considered when an alert-based reconfiguration is initiated.

Another related trend is *Network Function Virtualization (NFV)* that can also potentially allow significant flexibility and network programmability so as to react and respond fast to a generic unpredicted network disruption (either weather-based or others). An example of industrial research project heading towards this direction is described in [33], where authors develop novel testing tools (e.g., fault injection technologies) and systematic guidelines to help telecom operators to evaluate the reliability of their NFV-capable infrastructure. The authors focus on virtual machines, cloud management stacks, and hypervisors and investigate the risks for NFV reliability inherently associated to the adoption of virtualization.

In the remainder of this subsection, we notice that some alert-based reconfiguration approaches concetrate on data plane survivability while others on control plane survivability.

In order to ensure *data plane survivability*, when a hurricane or tornado alert is issued we need to calculate a virtual SDN embedding which is disjoint from the predicted disaster area. Thus, given the original embedding of the virtual network and the desired disaster-aware embedding, we need to migrate the virtual nodes and links onto the new physical resources [32]. As part of this, we have to remove the old and install the new forwarding rules in the switches. If the state of the virtual nodes have to be migrated as well, the time of the migration would depend on the memory size and (inverse proportionally) on the available bandwidth along the links between its old and new location. In this scenario a deadline T (depending on the alert) might be added to the optimization problem, before which the whole migration process must reach its desired state (e.g., before the hurricane reaches the mainland or the tornado hits the ground).

In order to preserve network connectivity, also the *control plane* of the network requires to be disaster resilient, especially in a scenario where a reaction to an alert is required and therefore quick network reconfiguration is needed [34]. Hence, in an alert-based control plane design we have to avoid that switches getting disconnected from the control logic or the network falls into several connected islands upon a controller failure [34]. Several distributed SDN controller architectures have been proposed to mitigate the risks of overload and failure, but they are optimized for limited faults without addressing the extent of large-scale disaster failures [35]. Thus, in [34] the authors present a novel disaster-aware control-plane design and mapping scheme, formally model this problem, and demonstrate a significant reduction in the disruption of controller-to-controller and switch-to-controller communication channels. While minimizing the resource usage, they also consider inter-controller and switch-to-controller delay to be able to respond to failures promptly. Further note that, if the communication channel of a switch to the primary controller fails, finding another operating controller upon disaster might be slow or would not be feasible at all. Thus, multiple controllers have to be assigned to each switch (i.e., a secondary, tertiary, etc. controller to be contacted if the primary fails) [35] in a resilient control plane design. Considering disasters in the controller placement problem becomes especially important if

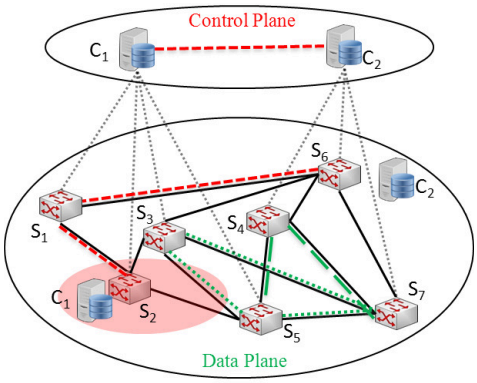

Fig. 3. After an alert is issued (red cricle), switches served by the affected controller C_1 have to be assigned to their secondary controller (i.e., C_2). The virtual network embedded to switches $S_7 - S_5 - S_3$ have to be re-allocated as well, including the migration of a virtual node (S_3 to S_4) and two virtual links (S_3, S_5) and (S_3, S_7).

the secondary controller might be responsible for controlling a migrated virtual SDN, and, thus, it has different latency constraints (to different physical locations of virtual nodes) than the primary controller. An example is presented in Fig. 3 to demonstrate the required tasks.

Upon an alarm is issued and the reconfiguration process is initiated, *migrating flows* from the old configuration to their new location in one step would lead to temporal over-utilization of links even if both the old and new configuration of the flows were congestion-free, owing to the asynchrony of forwarding rule updates at different switches. On the one hand, one approach is to accept this temporal performance degradation (i.e., congestion and packet loss) of the network but trying to minimize its effect. However, such service degradation is often unacceptable in production environments like data centers and WANs. On the other hand, migrating multiple flows at the same time in a provably congestion-free manner without making any assumptions about the timing of these updates at switches is a challenging problem and has been thoroughly investigated. It was shown in [36] that instead of performing forwarding rule update in a single step there often exists a sequence of consistent network updates (i.e., congestion-free and without temporary demand reduction [29]) that deploys the desired flows in the network. A polynomial-time algorithm was introduced in [36] to decide whether a consistent sequence of forwarding rule updates (i.e., migration plan) exists or not. However, if the flows are not allowed to be split – flows have to be switched at once or in integer parts from the current to their desired paths – then it is NP-hard to decide whether such a migration plan exists or not.

Although the first steps were made to address these questions, alert-based reconfiguration against weather-based disruptions in software defined networking is a largely unexplored research area.

B. Alert-based Reconfiguration in Cloud Networks

In cloud networks, a service request can be served by any of the datacentres (DCs) which host the required content, following the anycast communication paradigm. Under the Infrastructure as a Service (IaaS) model, cloud service provisioning comprises the selection of the most suitable DC to handle a service request and the assignment of network infrastructure to connect the source node of the request to the selected DC. Targeted attacks and natural disasters can lead to huge data loss and service disruptions in cloud networks. Considering the important role of cloud services today, any disruption of content/service, DC and network link failure is a major concern and network operators are investigating proactive and reactive measures to design disaster-resilient networks. As weather disruptions tend to grant a certain period of time in advance to the incoming disaster, a warning time, in this section we survey research studies that try to exploit such knowledge. In disaster-survivable IaaS clouds, backup virtual machines (VMs) are employed in standby mode, and are activated in a disaster. A disaster-resilient IaaS cloud requires incorporating the knowledge of disaster risks and consequences into the planning, modelling and disaster recovery selection [37]. In the planning phase, the possible risks are combined with resilience requirements and constraints. The requirements are typically expressed as the recovery time objective (RTO) and the recovery point objective (RPO). The RTO accounts for the time needed to restore a service, and it depends on the time needed to detect a failure, restore the affected VMs from a backup site, restart all the services running in these VMs, and redirect the network traffic from the original site to the backup site. The RPO refers to the data loss due to the time lapse between the last backup of the service components (e.g., copy of virtual disks) and the disaster [26]. When it comes to modelling, the interplay between the available bandwidth between DC sites and the offered RPO levels is still an open issue. The disaster recovery mechanism selection focuses on disaster detection mechanisms (e.g., periodical probing of DC sites, or using alarms), VM recovery mechanisms (e.g., using VM snapshots), and network reconfiguration mechanisms (typically relying on anycast) [37]. A cloud resiliency approach that utilizes service relocation and service differentiation for restoration of cloud services after a single-link failure was proposed in [38]. The paper leverages on the anycast nature of cloud services to improve service restorability by relocation to a datacentre with enough available IT (storage and processing) resources when the shortage of network resources prohibits restoration to the DC used by the failed working path. Moreover, applying service differentiation can prioritize recovery of higher-class services.

In [39], authors present novel techniques for disaster-aware DC placement and content management in cloud networks that can mitigate such loss by avoiding placement in given disaster vulnerable locations. The problem is first solved as a static disaster-aware DC and content placement problem by adopting an integer linear program (ILP) with the objective to minimize risk, defined as expected loss of content. Risk, as defined by authors in this study, is a measure of how much, in terms of cost or penalty, a network operator may lose probabilistically due to possible disasters in a cloud

network. It is also shown how a service provider's budget constraint can affect disaster-aware placement design. Since disaster scenarios, content popularity, and/or importance are always changing in time (e.g., as a reaction to incoming alert of a weather-related disruption), content placement should rapidly adapt to these changes. Authors propose a disaster-aware dynamic content-management algorithm that can adjust the existing placement based on dynamic settings. Besides reducing the overall risk and making the network disaster-aware, reducing network resource usage and satisfying QoS requirements can also be achieved by this approach. A cost analysis of employing a dynamic disaster-aware placement design in the network based on real-world cloud pricing. In [40], the case of large-scale disasters, as a hurricane (refer to the description of Hurricane Sandy in Section II), cloud networks can suffer massive service disruptions and data loss. To save critical data under such circumstances, contents could be *evacuated in response to an upcoming disaster alert* from a likely disaster region to a safe location before the disaster occurs and causes serious data damage. Depending on the forecasted disaster scenario, content evacuation can be greatly constrained by limited available network resources and strict deadlines (evacuation times). Hence, in [40], authors propose a rapid-data-evacuation heuristic that selects the least-delay paths (considering propagation delays, network bandwidth, and congestion) through an anycast network model, and schedules critical and vulnerable contents for evacuation such that the maximum amount of contents can be evacuated within the evacuation deadline or equivalently, a given amount of contents can be evacuated in minimum time. The proposed heuristic is compared with a nearest-evacuation approach, which evacuates data only to the nearest DC using the shortest path. Results show that, for typical scenarios considered in the study, compared to nearest evacuation, the rapid-evacuation approach provides about 64% time savings, or equivalently, about 97% more volume of evacuated contents for a given deadline. Since the algorithm is based on a greedy approach, authors also present an enhanced rapid-data-evacuation algorithm based on the simulated annealing metaheuristic as a benchmark. It is shown that the proposed heuristic performs very close to the simulated annealing based algorithm and is much faster in computation time and, hence, it is suitable and efficient for rapid evacuation.

Network vulnerability due to weather conditions is closely related with the weather characteristics of the geographic region where the network is deployed. In [41] a nonuniform region vulnerability map was defined based on disaster occurrence probability and intensity of the region. The vulnerability map is used as an input of an ILP formulation to identity the optimal placement of DCs and contents that minimizes failure risk due to disaster. Since content placement needs to be optimized within a given warning time, ILP solutions, due to their long running time, are not adequate and therefore an heuristic is also suggested. If pre-fault recovery mechanisms are not able to cope with network disruption post-fault recovery schemes involving physical infrastructure repair or replacement in a staged progressive manner is carried out. The network will operate for some time in a degraded manner and progressively recover to its pre-fault initial condition. In [42] four post-fault progressive recovery schemes are proposed. Uniform Placement, where repair resources are distributed in an even manner across damaged nodes and links. Random Placement , where repair resources are distributed in a random manner. Physical Node and Link Degree, where repair resources are assigned to failed nodes with the highest number of physical links prior to failure and Virtual Node and Link Degree that assigns repair resources to failed nodes/links with higher numbers of embedded virtual/links prior to failure. In all recovery schemes repair resources are distributed among failed nodes/links that have at least one non-failed neighbour node/link. This placement selectivity helps to improve the network connectivity. Results indicate that uniform resource placement gives faster initial recovery. However, uniform and physical node degree placements, at the final stage, presents slightly more efficient usage of network bandwidth resources.

V. Resiliency against Weather-based disruptions in converged networks

Recent traffic explosion in telecom networks and the expectation of an even faster increase of traffic represent a big challenge for network operators that have to minimize the total cost of ownership while serving such traffic. In particular, network operators must operate and maintain several access technologies, either wired (DSL, FFTx) and wireless (WiFi, 3G, 4G) while minimizing costs, power consumption and spectrum utilization in the wireless section. In 2009 a novel wireless cloud architecture called Centralized Radio Access Network (C-RAN) was proposed in [54] to ensure better scalability to mobile cellular network archtiecures. In this architecture the cellualr base station is divided into two parts, the base band unit (BBU) and the remote radio head (RRH). C-RAN implementation is often associated to other complementary architectures, such as, e.g., NFV and SDN (see e.g. [55], [43], [56]). The C-RAN provides benefits to operators and end-customers by enabling improved interference control, and thereby improved throughput, and by providing higher elasticity and scalability thanks to centralisation of BBUs. The two key challenges for C-RAN realization is to devise a bandwidth-efficient and latency-bounded transmission techniques between the RRHs and the BBUs. In fact the so-called fronhaul traffic (i.e, the traffic linking RRHs and BBBUs) has very strict latency requirements coming from the air protocols, as Time-Division Duplexing Long Term Evolution (TDD-LTE), and from the coordination requirements. Moreover, the fronthaul traffic is extremely bandwidth-intensive. Ref. [44] presents results from field trials in the China Mobile's TD-LTE C-RAN, where compression techniques and wavelength-division multiplexing (WDM) have been used to reduce fibre count between the RRH and BBU pools. This field trial shows that using C-RAN inter-cell interference may be significantly reduced, with throughput gains of 20 to 50% at good coverage areas (such gain may reach 50 to 100% at cell edge areas).

More importantly for our survey, [44] describes the severe effect on the performance of failures in the transmission network or in the BBU pools.

Some preliminary works are currently appearing that deal with resiliency of the C-RAN architecture. In [43] the trade-off between distributed and centralized RAN functionalities is discussed depending on the actual needs as well as network characteristics. A flexible functional split of the radio protocol stack between the central RAN as a service (RANaaS) and the local radio access points is proposed. The key requirement for flexible functional split is the requirement for dynamic adaptation of network routes depending on available transmission resources. This functionality may be used in case of a weather alert to redistribute user traffic to the available base stations. In [45] the problem of latency and reliability of a mobile heterogeneous network with backhaul provided by an optical passive network (PON) is considered. Typically, the coverage areas of macro- and small-cells are overlapped. Furthermore, the concept of WiFi offloading is considered. Since WiFi is mainly an indoor technology, therefore offloading traffic from impaired mobile networks to indoor networks could be a good option. This network architecture provides to operators some degree of freedom to modify user distributions across the networks by means of traffic steering to improve network performance according to network failures or a weather alert.

The virtualization of network functions, such as, e.g., C-RAN, provides an architecture for elasticity and scalability of of resources on demand. As discussed earlier in this section, the C-RAN puts strict requirements on the latency in transmission between the RRH and BBUs. In [46] the localisation and capacity of the BBU pools are formulated as a optimisation tasks where the cost of transmission and BBUs is taken into consideration. This shows the potential limitation of available fibres in the access network. It also indicates that the number of redundancy between BBU pools may be a challenge.

Ref. [47] addresses the survivability aspects of Next Generation - Passive Optical Networks (NG-PONs) and hybrid Fibre-Wireless (FiWi) access networks, taking both optical and wireless protection into account. The paper investigates different selection schemes to find a small set of Optical Network Units (ONUs) and equip them with wireless communication capabilities in order to guaranteeing a high degree of survivability. The performance is examined for a wide range of fibre link failure scenarios and different NG-PON topologies.

The redundancy-based restoration of virtualized network functions due to malfunction has to take into consideration the signalling messages between the the various network entities. For instance, a re-instantiation of a virtualized mobility management entity (MME) in the evolved packet core (EPC) has an effect on the traffic to/from user equipment (UE) handled by the affected MME [48]. In [48] two proactive VNF failure restoration approaches are proposed aimed at the reduction of the network overload that may happen due to restoration control signalling messages where as soon as a MME VNF goes off or starts malfunctioning, a new MME VNF instance is initiated. The first mechanism is based on bulk signalling, i.e., it creates only one single message to replace a certain number of signalling messages in a bulk, while the second one creates message profile, i.e., reduces the signalling message header by replacing repetitive information element by a profile identifier. The bulk signalling was the most effective mechanism to reduce the signalling.

VI. Advanced Technology for Resiliency against Weather-based disruptions

We have described in previous sections how weather conditions can significantly affect the performance of different categories of communication networks (wired, wireless, converged), e.g., by causing long delays that cannot be sustained in existing Internet architectures. In this last section we move our focus on a heterogeneous class of novel and experimental networking technologies to see if they can offer new abilities for realizing resilience when exposed to weather-based disruption.

Delay Tolerant Networking. Based on existing literature on this topic Delay Tolerant Networking (DTN) seems to be the most promising approach to overcome specific weather-related outages. The Delay Tolerant Networking Architecture [57] departs from the established Internet architecture paradigm of end-to-end communication but it concentrates on techniques to sustain long delays (order of hours or even more) and continuous disruptions. Such events are considered unavoidable and are part of the design. Hence, DTN inherently copes with them by introducing the notion of storage inside the network stack, transforming the "store-and-forward" paradigm to a "store-carry-forward" one.

A large number of works explored DTN applications in different weather-challenged operation environments [49]. Here, we highlight three examples. AX.25 is a link-layer protocol for packet radio networking over HF, VHF, and UHF links of 1.200 bps. A series of experiments (cf. [43-47] of [49]) revealed that DTN over TCP/IP Convergence Layer outperforms established IPv4-based approaches in different AX.25 network configurations, especially in cases of severe winds that affected link-layer connectivity. A second example is maritime communication with varying environmental and weather conditions. Using real-world traces of WiMax links for ship communications in the busy Strait of Singapore, it was shown (cf. [93] of [49]) that DTN-based routing approaches outperform ad hoc routing protocols (AODV and OLSR) in packet delivery rates on the expense of greater delay that DTN can cope with. A third example is a communication system for underground mines, where radio communication is severely limited by the (changing) topology of the mining tunnels and the environmental conditions (e.g., humidity), and the mining equipment. A DTN-based software system allowed to reliably establish communication channels between the data sources (drills), the intermediaries (pickups used to ferry workers to/from the drill), and the sinks (wireless access points with limited range), despite the lack of an end-to-end path and the sporadic connectivity episodes [50].

The aforementioned examples highlight one of the core principles of the DTN architecture. DTN does not try to hide large delays or communication disruptions. Rather, such events are considered unavoidable and become part of the design.

Information Centric Networking (ICN) is a family of more clean-slate architectural approaches (e.g., CCN [58] and NDN [59]) with the aim to evolve the Internet infrastructure from a host-centric paradigm based end-to-end connectivity to a network architecture in which the main target to be reached is a "named information" (e.g., a content). ICN is expected to to be helpful to support communications in emergency situations, such as in the case of natural and weather disasters. In [51] several advantages of ICN are discussed, including resilience due to multi-homing and connectionless communication, as well as open issues and research challenges, such as discovery of information sources, management support, robust and resilient routing, and push-based communications, as currently ICN are pull-based. The need for push-based notification is addressed in [60], where a new packet primitive is specified for CCN, namely "Notification".

Content Centric Networking (CCN) is an example of an Information Centric Networking (ICN) architecture, where "content" is addressable and routable. CCN and caching can be useful alternatives in case of link failures at a local scale (e.g., due to extreme weather conditions). A performance evaluation assuming realistic network topologies and simulations showed that CCN can reduce by a factor of two the number of hops to be traversed for retrieving information and thus, improve network resilience [52]. Also CCN, therefore, might enable new solutions against weather-based disruption especially in content-centric network environments.

VII. Conclusions

Weather conditions can affect the performance of telecom networks. In this survey, we classified and discussed relevant studies in the field of network survivability against weather-based disruptions. We considered first the modeling of the impact of weather conditions on wireless channel quality, with a specific emphasis on the structural impact of winds on cellular towers. We then surveyed protection strategies proposed in wireless networks (mostly, WMNs and FSO network), wired networks (on which we focused on alert-based reconfiguration techniques) and converged networks. Finally, the role of advanced and innovative network architectural proposal as DTN, NFV and ICN have been also discussed. The importance of these topics is expected to grow in the next years considering, e.g., the important role that wireless links are expected to play in 5G networks (both in the access and backhaul segments) and the increasing occurrences of extreme weather conditions associated to global warming.

Acknowledgment

We would like to thank the participants of WG2 (Weather-based disruptions) of COST Action CA15127 whom indirectly collaborated in this task: Rasa Bruzgiene, Lina Narbutaite, Adomkus Tomas.

This article is based upon work from COST Action CA15127 ("Resilient communication services protecting end-user applications from disaster-based failures – RECODIS") supported by COST (European Cooperation in Science and Technology).

References

[1] J. Luomala and I. Hakala, "Effects of temperature and humidity on radio signal strength in outdoor wireless sensor networks," in *2015 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Sept 2015, pp. 1247–1255.

[2] A. Kwasinski, W. Weaver, P. Chapman, and P. Krein, "Telecommunications power plant damage assessment for hurricane katrina - site survey and follow-up results," *IEEE Systems Journal*, vol. 3, no. 3, pp. 277–287, 2009.

[3] F. Iqbal and F. Kuipers, "Spatiotemporal risk-averse routing," in *Proceedings of the IEEE INFOCOM Workshop on Cross-Layer Cyber-Physical Systems Security (CPSS 2016)*, April 2016.

[4] S. Erjongmanee and C. Ji, "Large-scale network-service disruption: Dependencies and external factors," *IEEE Transactions on Network and Service Management*, vol. 8, no. 4, pp. 375–386, December 2011.

[5] T. Adachi, Y. Ishiyama, Y. Asakura, and K. Nakamura, "The restoration of telecom power damages by the Great East Japan earthquake," in *IEEE Telecommunication Energy Conference, 2011*, vol. 4, June 2011, pp. 178–183.

[6] E. Kuligowski, F. Lombardo, L. Phan, M. Levitan, and D. Jorgensen, "Technical investigation of the May 22, 2011, tornado in Joplin, Missouri," *Rep. NIST NCSTAR*, vol. 3, 2014.

[7] S. A. Cauffman, *Performance of Physical Structures in Hurricane Katrina & Hurricane Rita: A Reconnaissance Report*. DIANE Publishing, 2006.

[8] P. E. Heegaard and K. S. Trivedi, "Network survivability modeling," *Computer Networks*, vol. 53, no. 8, pp. 1215–1234, 2009.

[9] "Technical report on enhanced network survivability performance, Tech. Rep. 68, ANSI T1A1.2," Working Group on Network Survivability Performance, Tech. Rep., 2001.

[10] M. Abaza, R. Mesleh, A. Mansour *et al.*, "Performance analysis of miso multi-hop FSO links over log-normal channels with fog and beam divergence attenuations," *Optics Communications*, vol. 334, pp. 247–252, 2015.

[11] Y. S. Meng, Y. H. Lee, and B. C. Ng, "The effects of tropical weather on radio-wave propagation over foliage channel," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4023–4030, Oct 2009.

[12] F. Nadeem, E. Leitgeb, M. S. Awan, and S. Chessa, "Comparing the life time of terrestrial wireless sensor networks by employing hybrid FSO/RF and only RF access networks," in *Fifth International Conference on Wireless and Mobile Communications (ICWMC)*, Aug 2009, pp. 134–139.

[13] R. Travanca, H. Varum, and P. V. Real, "The past 20 years of telecommunication structures in portugal," *Engineering Structures*, vol. 48, pp. 472–485, 2013.

[14] B. Smith, *Communication Structures*. Thomas Telford, London, 2007.

[15] P. Antunes, R. Travanca, H. Varum, and P. Andre, "Dynamic monitoring and numerical modelling of communication towers with fbg based accelerometers," *Journal of Constructional Steel Research*, vol. 74, pp. 58–62, 2012.

[16] G. Solari and L. Pagnini, "Gust buffeting and aeroelastic behaviour of poles and monotubular towers," *Journal of Fluids and Structures*, vol. 13, pp. 877–905, 2012.

[17] U. Stottrup-Andersen, "Masts and towers," in *Proceedings of the International Association for Shell and Spatial Structures (IASS) Symposium*, E. A. Domingo and C. Lazaro, Eds., June 2009, pp. 127–128.

[18] N. Javed, E. Lyons, M. Zink, and T. Wolf, "Adaptive wireless mesh networks: Surviving weather without sensing it," in *22nd International Conference on Computer Communication and Networks (ICCCN)*, July 2013, pp. 1–7.

[19] J. Rak, "Design of weather disruption-tolerant wireless mesh networks," in *Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2012 XVth International*, Oct 2012, pp. 1–6.

[20] ——, "A new approach to design of weather disruption-tolerant wireless mesh networks," *Telecommunication Systems*, vol. 61, no. 2, pp. 311–323, 2016.

[21] A. Jabbar, J. P. Rohrer, V. S. Frost, and J. P. Sterbenz, "Survivable millimeter-wave mesh networks," *Computer Communications*, vol. 34, no. 16, pp. 1942–1955, 2011.

[22] A. Jabbar, J. P. Rohrer, A. Oberthaler, E. K. Cetinkaya, V. Frost, and J. P. G. Sterbenz, "Performance comparison of weather disruption-tolerant cross-layer routing algorithms," in *IEEE INFOCOM*, April 2009, pp. 1143–1151.

[23] Z. M. Fadlullah, T. Nakajo, H. Nishiyama, Y. Owada, K. Hamaguchi, and N. Kato, "Field measurement of an implemented solar powered bs-based wireless mesh network," *IEEE Wireless Communications*, vol. 22, no. 3, pp. 137–143, June 2015.

[24] S. V. Kartalopoulos, "Protection strategies and fault avoidance in free space optical mesh networks," in *4th IEEE International Conference on Circuits and Systems for Communications (ICCSC)*, May 2008, pp. 797–801.

[25] E. Leitgeb, M. Loschnigg, U. Birnbacher, G. Schwarz, and A. Merdonig, "High reliable optical wireless links for the last mile access," in *2008 10th Anniversary International Conference on Transparent Optical Networks*, vol. 4, June 2008, pp. 178–183.

[26] J. Rak and W. Molisz, "Reliable routing and resource allocation scheme for hybrid rf/fso networks," in *2014 16th International Conference on Transparent Optical Networks (ICTON)*. IEEE, 2014, pp. 1–4.

[27] M. Piro, D. Nace, and Y. Fouquet, "On protected traffic routing in wireless networks with partial multiple link failures," in *8th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, Oct 2013, pp. 22–28.

[28] B. Mukherjee, M. F. Habib, and F. Dikbiyik, "Network adaptability from disaster disruptions and cascading failures," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 230–238, May 2014.

[29] S. S. Savas, M. F. Habib, M. Tornatore, F. Dikbiyik, and B. Mukherjee, "Network adaptability to disaster disruptions by exploiting degraded-service tolerance," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 58–65, December 2014.

[30] S. Neumayer and E. Modiano, "Network reliability with geographically correlated failures," in *IEEE INFOCOM, 2010 Proceedings*, March 2010, pp. 1–9.

[31] R. L. Gomes, L. F. Bittencourt, E. R. Madeira, E. Cerqueira, and M. Gerla, "Bandwidth-aware allocation of resilient virtual software defined networks," *Computer Networks*, vol. 100, pp. 179–194, 2016.

[32] E. Keller, S. Ghorbani, M. Caesar, and J. Rexford, "Live migration of an entire network (and its hosts)," in *Proceedings of the 11th ACM Workshop on Hot Topics in Networks*. ACM, 2012, pp. 109–114.

[33] D. Cotroneo, L. D. Simone, A. K. Iannillo, A. Lanzaro, R. Natella, J. Fan, and W. Ping, "Network function virtualization: Challenges and directions for reliability assurance," in *2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Nov 2014, pp. 37–42.

[34] S. S. Savas, M. Tornatore, M. F. Habib, P. Chowdhury, and B. Mukherjee, "Disaster-resilient control plane design and mapping in software-defined networks," in *2015 IEEE 16th International Conference on High Performance Switching and Routing (HPSR)*, July 2015, pp. 1–6.

[35] B. P. R. Killi and S. V. Rao, "Optimal model for failure foresight capacitated controller placement in software-defined networks," *IEEE Communications Letters*, vol. 20, no. 6, pp. 1108–1111, June 2016.

[36] S. Brandt, K.-T. Förster, and R. Wattenhofer, "On consistent migration of flows in SDNs," in *Proc. IEEE INFOCOM*, 2016.

[37] R. Couto, S. Secci, M. E. M. Campista, and L. H. M. K. Costa, "Network design requirements for disaster resilience in IaaS clouds," *IEEE Communications Magazine*, vol. 52, no. 10, pp. 52–58, October 2014.

[38] C. N. da Silva, L. Wosinska, S. Spadaro, J. C. W. A. Costa, C. R. L. Frances, and P. Monti, "Restoration in optical cloud networks with relocation and services differentiation," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 8, no. 2, pp. 100–111, Feb 2016.

[39] S. Ferdousi, F. Dikbiyik, M. F. Habib, M. Tornatore, and B. Mukherjee, "Disaster-aware datacenter placement and dynamic content management in cloud networks," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 7, no. 7, pp. 681–694, July 2015.

[40] S. Ferdousi, M. Tornatore, M. F. Habib, and B. Mukherjee, "Rapid data evacuation for large-scale disasters in optical cloud networks," *IEEE/OSA Journal of Optical Communications and Networking (JOCN)*, vol. 7, no. 12, pp. 163–172, Dec 2015.

[41] L. Ma, X. Jiang, B. Wu, A. Pattavina, and N. Shiratori, "Probabilistic region failure-aware data center network and content placement," *Computer Networks*, vol. 103, pp. 56–66, 2016.

[42] M. Pourvali, K. Liang, F. Gu, H. Bai, K. Shaban, S. Khan, and N. Ghani, "Progressive recovery for network virtualization after large-scale disasters," in *2016 International Conference on Computing, Networking and Communications (ICNC)*, Feb 2016, pp. 1–5.

[43] P. Rost, C. J. Bernardos, A. D. Domenico, M. D. Girolamo, M. Lalam, A. Maeder, D. Sabella, and D. Wübben, "Cloud technologies for flexible 5G radio access networks," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 68–76, May 2014.

[44] C. L. I, J. Huang, R. Duan, C. Cui, J. Jiang, and L. Li, "Recent progress on C-RAN centralization and cloudification," *IEEE Access*, vol. 2, pp. 1030–1039, 2014.

[45] H. Beyranvand, W. Lim, M. Maier, C. Verikoukis, and J. A. Salehi, "Backhaul-aware user association in Wi-Fi enhanced LTE-A heterogeneous networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 6, pp. 2992–3003, June 2015.

[46] H. Holm, A. Checko, R. Al-obaidi, and H. Christiansen, "Optimal assignment of cells in c-ran deployments with multiple bbu pools," in *Networks and Communications (EuCNC), 2015 European Conference on*, June 2015, pp. 205–209.

[47] N. Ghazisaidi, M. Scheutzow, and M. Maier, "Survivability analysis of next-generation passive optical networks and fiber-wireless access networks," *IEEE Transactions on Reliability*, vol. 60, no. 2, pp. 479–492, June 2011.

[48] T. Taleb, A. Ksentini, and B. Sericola, "On service resilience in cloud-native 5G mobile systems," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 483–496, March 2016.

[49] A. Voyiatzis, "A survey of delay-and disruption-tolerant networking applications," *Journal of Internet engineering*, vol. 5, no. 1, 2012.

[50] T. Karkkainen, M. Pitkanen, and J. Ott, "Applications in delay-tolerant and opportunistic networks," *Mobile Ad Hoc Networking: Cutting Edge Directions, Second Edition*, pp. 315–359, 2013.

[51] M. Yamazaki, K. Takahagi, T. Ishida, K. Sugita, N. Uchida, and Y. Shibata, "Proposal of information acquisition method utilizing CCN in a time of large scale natural disaster," in *10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, Nov 2015, pp. 645–650.

[52] G. Tyson, E. Bodanese, J. Bigham, and A. Mauthe, "Beyond content delivery: can information centric networks (ICNs) help emergency scenarios?" *IEEE Network*, vol. 28, no. 3, pp. 44–49, May 2014.

[53] Y. Abdulrahman and M. Bwanga, "Wimax: The innovative broadband wireless access technology," *Retrieved June*, vol. 29, p. 2012, 2008.

[54] Y. Lin, L. Shao, Z. Zhu, Q. Wang, and R. K. Sabhikhi, "Wireless network cloud: Architecture and system requirements," *IBM Journal of Research and Development*, vol. 54, no. 1, pp. 4:1–4:12, January 2010.

[55] M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Vasilakos, "Software-defined and virtualized future mobile and wireless networks: A survey," *Mobile Networks and Applications*, vol. 20, no. 1, pp. 4–18, 2015.

[56] V.-G. Nguyen, T.-X. Do, and Y. Kim, "SDN and virtualization-based LTE mobile network architectures: A comprehensive survey," *Wireless Personal Communications*, vol. 86, no. 3, pp. 1401–1438, 2016.

[57] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay-tolerant networking architecture," Internet Requests for Comments, RFC Editor, RFC 4838, April 2007, http://www.rfc-editor.org/rfc/rfc4838.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4838.txt

[58] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *Proceedings of the 5th international conference on Emerging networking experiments and technologies*. ACM, 2009, pp. 1–12.

[59] L. Zhang, A. Afanasyev, J. Burke, K. C. Van Jacobson, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, July 2014.

[60] R. Ravindran, A. Chakraborti, M. Mosko, and I. Solis, "Support for notifications in CCN," Working Draft, IETF Secretariat, Internet-Draft draft-ravi-ccn-notification-01, March 2016, http://www.ietf.org/internet-drafts/draft-ravi-ccn-notification-01.txt. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ravi-ccn-notification-01.txt