Published in "Proceedings of EuCNC 2018", 18-21 June 2018, Ljubljana, Slovenia, which should be cited to refer to this work.

On the Disaster Resiliency within the Context of 5G Networks: The RECODIS Experience*

Christian Esposito[1], Antonios Gouglidis[2], David Hutchison[2], Andrei Gurtov[3], Bjarne E. Helvik[4], Poul E. Heegaard[4], Gianluca Rizzo[5], Jacek Rak[6]

***Abstract*—Network communications and the Internet pervade our daily activities so deeply that we strongly depend on the availability and quality of the services they provide. For this reason, natural and technological disasters, by affecting network and service availability, have a potentially huge impact on our daily lives. Ensuring adequate levels of resiliency is hence a key issue that future network paradigms, such as 5G, need to address. This paper provides an overview of the main avenues of research on this topic within the context of the RECODIS COST Action.**

I. INTRODUCTION

RECODIS [1] is a COST Action focusing on improving the level of resiliency offered by current networking solutions, as well as on devising more effective post-disaster communication mechanisms. Overall, these efforts aim at better coping with natural, technology-related, or maliciously-caused disasters. In fact, computer-based communications represents the key factor in our current society, enabling what is called an inclusive digital society and changing peoples' daily social and economic lives. However, disasters may compromise the networking infrastructure to the point that it becomes unavailable or it offers degraded quality services. This can cause cascading effects since during a disaster people may require to communicate and receive updates on the situation or even inform rescue teams with their location. A representative example is the one related with one of the worst fire cases in the Portuguese history in June 2017 [2]. The communications among the rescue teams had been severely affected by the fire and this had been an obstacle for efficient and effective planning, command and execution of operations. It is a general feeling that these communication issues had the side-effect to increase the overall number of causalities in terms of human life losses. Since our society is so dependent on efficient communications, it is crucial to include disaster resiliency among the main requirements for the design of the upcoming communication infrastructure. Indeed, the 5^{th} generation of mobile networks [3], whose commercial deployment is expected to start in 2020, has been designed to provide ultra reliability and low latency communications. 5G envisions a shift in the risk from rare critical events with severe consequences (due to a closed perspective characterizing the critical infrastructures) to more frequent events with limited consequences, mainly due to attacks or malfunctioning (due to the flexible and open perspective of the programmable networks envisioned by the 5G vision), as illustrated in Figure 1. As part of the RECODIS activities, we have investigate how 5G might satisfy such requirements in case of disasters. The present paper provides an overview of the main resiliency issues in present day networks and of the main available solutions in 5G networks, and it briefly highlights some research challenges on this topic.

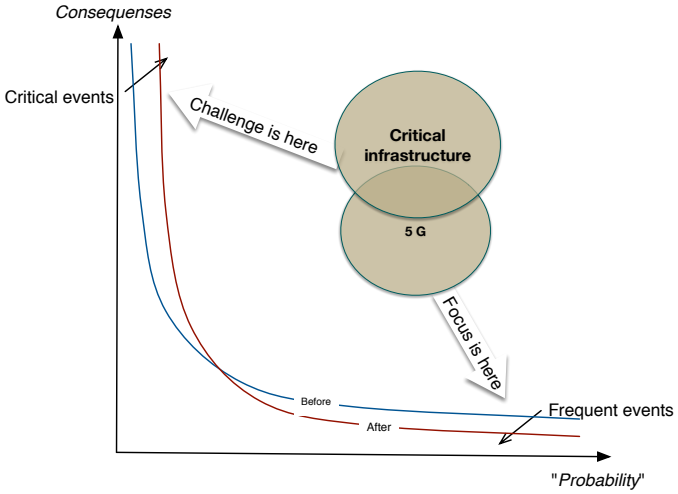

Fig. 1. Focusing on reducing frequent events might lead to challenges with increased consequences of disaster events

II. BACKGROUND ON DISASTER-RESILIENT NETWORKING

A disaster can have considerable negative effects on the networking infrastructure by causing various types of failures [6].

[1]C. Esposito is with the Department of Electrical Engineering and Information Technologies (DIETI), University of "Federico II", 80125 Napoli, Italy. christian.esposito@unina.it

[2]A. Gouglidis and D. Hutchison are with the School of Computing and Communications, Lancast er University, LA1 4WA Lancaster, United Kingdom (UK). {a.gouglidis, d.hutchison}@lancaster.ac.uk

[3]Andrei Gurtov is with the Department of Computer and Information Science, Linkoping University, 581 83 Linköping - Sweden. andrei.gurtov@liu.se

[4]Bjarne E. Helvik and Poul E. Heegaard are with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 7034 Trondheim - Norway. {bjarne, poul.heegaard}@ntnu.no

[5]Gianluca Rizzo is with the IIG institute, University of Applied Sciences of Western Switzerland, HES SO Valais - Switzerland. gianluca.rizzo@hevs.ch

[6]Jacek Rak is with the Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, Pl-80-233 Gdansk, Poland. jrak@pg.gda.pl

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

Adverse weather conditions can cause a decrease in communication reliability [8] (with a consequent increase of packet loss rate) when radio frequency (RF) signals are adopted. In fact, flashes and clouds can increase the RF signal interference and attenuation, generating errors in received packets. More severe disaster can cause damages at the links, which can be temporary (possibly recoverable through software-based mechanisms and network reconfiguration) or permanent (so that maintenance and component substitution are required to recover the full link availability). A disaster can damage also the networking devices, such as hubs or routers, or even data centers hosting the core services. Also in this case, we can have temporary or permanent failures, and the fault can be directly caused by the disaster (such as an earthquake destroying the building hosting the networking equipment) or indirectly [9] (such as severe flashing causing a blackout, and the consequent loss of energy making the networking devices inactive). Finally, disasters are known to cause local peaks of traffic demand, often resulting into network saturation and service unavailability.

In order to offer resilient solutions, network and service providers need to ensure diversity – spatial and also in terms of different technologies. To cope with disaster-based disruptions, it is possible to employ various kind of techniques [7], such as redundancy in the hardware of network devices, in the networking topology, and resilient routing strategies, capable of guaranteeing message delivery despite failures. Virtualization technologies may be employed as well, to achieve spatial distribution e.g., in edge and fog-based service architectures and provision of resiliency-supporting approaches [18].

III. A Brief Introduction to 5G

5G has been conceived as a key technology enabling the development of disruptive applications, services and paradigms such as the Internet of Things, Augmented Virtual Reality, Unmanned Aircraft Systems, among others. All of them have in common their reliance on wireless communications, and specifically on high speed, reliable connectivity. The 5G paradigm promises to properly address such requirements by exploiting the large bandwidth available in millimiter-wave bands (with a frequency range from 30GHz to 300GHz), and new waveforms (whose wavelength is between 10mm to 1mm). These frequencies, by requiring [4] the use of modest-size antennas with small beam width, facilitate the implementation of complex antenna arrays, such as those required by Multiple Input- Multiple Output (MIMO) approaches, which can be integrated on chip or PCB. In short, we have a data rate of several Gbps; however, such a millimeter-wave radio communication has very poor propagation properties. Any natural obstacle such as rain or fog is likely to block the link forcing to downgrade to lower frequency radio bands. Therefore, the coverage range of base stations is lower than the one achievable with the traditional 4G equipments. This implies that it is needed to have high density deployments of small cell with the consequent traffic offloading, but this may cause interference phenomena among the base-stations. Moreover, some studies, such as the one described in [5], proved that the raining conditions negatively affect such millimeter wavelengths by increasing the signal distortion.

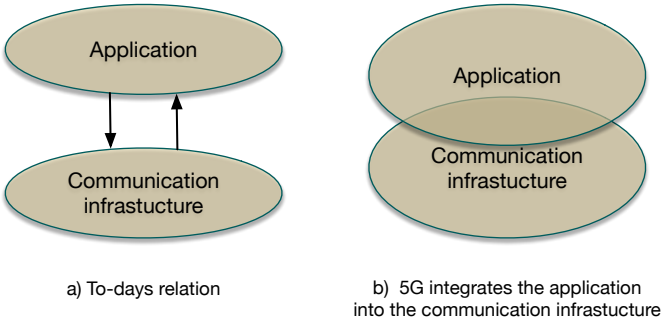

Fig. 2. From the two-way interrelationship to a tight integration of application and 5G communication infrastructure

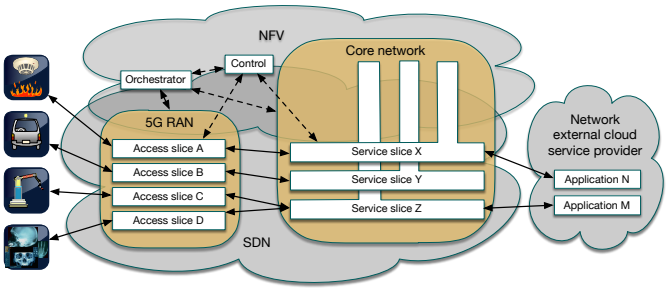

Fig. 3. Network slicing in 5G - both in the radio access network (RAN) and in the core network

The 5G paradigm implies also a shift from static network design and management, to a dynamic model. Indeed, the very high capacity targets of 5G will be achieved also through adaptive (and possibly proactive) strategies which adapt the network configuration to local transmissive conditions, and to spatio-temporal patterns of traffic demand. A central role in such dynamic network configuration is played by such enabling technologies as Software Defined Networking (SDN), Network Function Virtualization (NFV), Network Slicing, and Cloud Radio Access Network (RAN). SDN enables programmable networks, characterized by the decoupling of the control and user planes. NFV consists in determining how virtualized software functions can be deployed within the virtual machines running on common physical resources of the core network. Network slicing (Figure 3) allows telecom operators to define networking services dedicate to particular classes of customers, requiring specialized quality of service. Finally, Cloud RAN enables inter-site scheduling and cooperative techniques. Bottom line, 5G is a disruptive technology that will change the traditional networking service delivery model (Figure 2) by integrating applications (or some of their horizontal features such as the security-related ones) within the programmable network, as part of the SDN or NFV architecture.

IV. State-of-the-Art and Challenges of Disaster-Resilient 5G

Due to the stringent reliability and availability requirements imposed by the telecommunication networks being a vital part of the Critical National Infrastructure, the 5G has been designed to provide higher guarantees than the current networking infrastructure. The softwarization of the networks brought by 5G is a promising way to realize those self-healing capabilities [11] demanded to cope with the effects of disasters (depicted in Figure 4), and to offer the necessary communications in post disaster scenarios. Indeed, a programmable network is superior to the traditional configurable networks in the provision of flexible and fast-failover mechanisms for the mitigation of the effects of link or switch failures. However, in its current design, the SDN is affected by the issue of having a centralized controller, which represent a single point of failure, and the possibility of encompassing robust and reliable distributed controllers is still an open issue [12], [28], despite some attempts to introduce a replication of controllers [13]. As part of the RECODIS activities, a preliminary characterization of the failure dynamics exhibited by the SDN controller has been done by using the formalisms of the Stochastic Activity Networks in [16].

The flexibility provided by NFV has also a great potential in providing the needed fault-tolerance level to achieve disaster resiliency, thanks to the offered deliver agility and flexibility. However, the problem of achieving an high availability and resiliency in NFV-based systems is far from being considered closed, but is still open to investigation [14] and their benchmarking are being conducted [22], [23]. In fact, nowadays, off-the-shelf networking hardware is less reliable that the dedicated network elements currently used for the cellular networks (just to cite an example). The European Telecommunication Standards Institute (ETSI) hosts the ETSI Industry Specification Group for Network Functions Virtualization (ETSI NFV ISG) with the intent of standardizing the requirements and architectures for virtualization various functions within telecoms networks. Such a group has studied the challenges underlying the provision of high availability and resiliency in NFV-based systems. Redundancy has been seen as the solution for high availability by having separate virtual machines hosting the Control Element (CE) and data plane Forwarding Elements (FE), each of them protecting with a master-slave replication where the replica is hosted in a different virtual machine and can take over a failed master. The main issue is to proper determine a placement plan for the NFVs within the available hardware commodities and the virtual machines running on them so as to achieve the suitable level of availability and resiliency. Among the RECODIS activities, a first solution to this problem based on heuristics has been formulated and validated in [15].

Moreover, supporting different technologies may allow network operators and service providers to automatically relocate network services in case of a network failure or disaster. However, the proper orchestration of this multi-tenant model

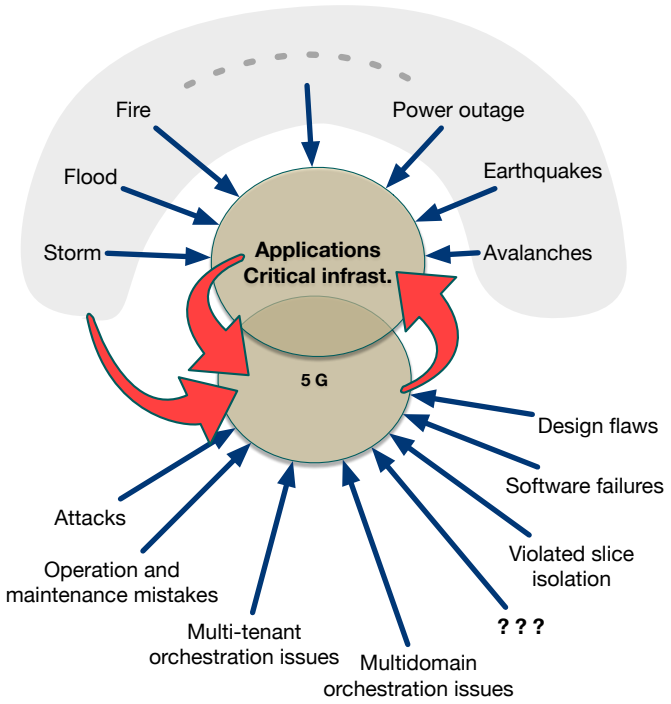

Fig. 4. Threats caused by extreme weather, natural disasters, and embedded in the ICT system leads to escalations of disasters

is a key issue for providing dependability, still under investigation [29]. In virtualized network infrastructures based on SDN and NFV technologies, novel approaches are able to provide service orchestrators that can automate the deployment and dynamic re-optimization of network services [19]. Such approaches may also provide support for achieving network convergence, e.g., among wired Ethernet, WiFi and Free Space Optics (FSO) technologies. As presented in [20], hybrid solutions that consist of FSO links and back-up links in the GHz frequency may result in higher availability. Specifically, a prominent FSO technology under investigation in that context is LiFi [21], which has been described as an enabling 5G technology capable of achieving high transmission speeds, providing even complete cellular networks. Such technologies can be considered for deployment in areas where weather conditions may deviate from the norm in order to provide network availability.

The resiliency of networks is directly related also to the safety of the physical infrastructure used for communication networks, such as monopoles, lattice towers and guyed masts, able to resist to the stress resulting from natural causes. The work done in RECODIS and presented in [17] consisting in overviewing the recent design practices for such physic components and highlights their safety issues.

Security in the 5G is also a serious concern [24], an in general for any communication infrastructure [10], and the softwarization of the networking functions opens up novel vulnerabilities to be exploited to implements attacks aiming at compromising the overall availability of the network or even a

part of it [25]. During RECODIS, the placement of virtualized security functions in data centers has been investigated in [26].

V. CONCLUSIONS

5G provides the upcoming network technologies that potentially will radically change how the network works and is managed. However, if it fails to provide resiliency to disasters, it will miss the opportunity to offer the level of availability and quality required by current and upcoming ICT infrastructures. RECODIS is a COST Action focused on disaster resiliency, and among its activities, it has investigated some key aspects in 5G to provide these requirements. Some of them have been briefly introduced in this paper.

ACKNOWLEDGMENT

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) [1]. The research presented in this paper is also supported the project *DataWay*: Real-time Data Processing Platform for Smart Cities: Making sense of Big Data - PN-II-RU-TE-2014-4-2731.

REFERENCES

[1] J. Rak, D. Hutchison, E. Calle, T. Gomes, M. Gunkel, P. Smith, J. Tapolcai, S. Verbrugge, L. Wosinska, "RECODIS: Resilient Communication Services Protecting End-user Applications from Disaster-based Failures", in Proc. 18th Intl. Conf. Transparent Optical Networks (ICTON), 2016, pp. 1-4.

[2] S.Jones, "Portugal forest fires under control after more than 60 deaths", The Guardian article, available at https://www.theguardian.com/world/2017/jun/19/portuguese-wildfires-water-dropping-planes-spain-france-italy.

[3] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, G. Wunder, "5G: A Tutorial Overview of Standards, Trials,Challenges, Deployment and Practice", IEEE Journal on Selected Areas in Communications, vol. 35, no. 6, June 2017, pp. 1201-1221.

[4] T. S. Rappaport, R. W., Jr. Heath, R. C. Daniels, J. N. Murdock, "Millimeter Wave Wireless Communications", Prentice Hall, 2014.

[5] A. Maitra, M. Kundu, "Wideband Propagation at Millimeter Wavelengths Through the Dispersive and Absorptive Atmosphere", International Journal of Infrared and Millimeter Waves, vol. 24, no. 11, November 2003, pp: 1841?1851.

[6] A. Mauthe, D. Hutchison, E. K. Ceetinkaya, I. Ganchev, J. Rak, J. P. G. Sterbenz, M. Gunkel, P. Smith, T. Gomes, "Disaster-resilient communication networks: Principles and best practices", in Proc. 8th Intl. Wksp Resilient Networks Design and Modeling (RNDM), 2016.

[7] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. Andre , L. Jorge, L. Martins, P. Ortiz Ugalde, A. Pasic, D. Pezaros, S.Jouet, S. Secci, M. Tornatore, "A Survey of Strategies for Communication Networks to Protect against Large-scale Natural Disasters", in Proc. 8th Intl. Wksp Resilient Networks Design and Modeling (RNDM), 2016.

[8] M. Tornatore, J. Andre, P. Babarczi, T. Braun, E. Folstad, 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. 8th Intl. Wksp Resilient Networks Design and Modeling (RNDM), 2016.

[9] C. Mas Machuca, S. Secci, P. Vizarreta, F. Kuipers, A. Gouglidis, David Hutchison, S. Jouet, D. Pezaros, A. Elmokashfi, P. Heegaard, S. Ristov, "Technology-related Disasters: A Survey towards Disaster-resilient Software Defined Networks", in Proc. 8th Intl. Wksp Resilient Networks Design and Modeling (RNDM), 2016.

[10] M. Furdek, L. Wosinska, R. Go?cie?, K. Manousakis, M. Aibin, K. Walkowiak, S. Ristov, J.L. Marzo, "An Overview of Security Challenges in Communication Networks", in Proc. 8th Intl. Wksp Resilient Networks Design and Modeling (RNDM), 2016.

[11] J. Sánchez, I. G. B. Yahia, N. Crespi, T. Rasheed, D. Siracusa, "Softwarized 5G Networks Resiliency with Self-Healing", in Proc. 1st Intl. Conf. 5G for Ubiquitous Connectivity (5GU), 2014, pp: 229-233.

[12] K. ElDefrawy, T. Kaczmarek, "Byzantine Fault Tolerant Software-Defined Networking (SDN) Controllers", in Proc. IEEE 40th Annual Conf. Computer Software and Applications (COMPSAC), 2016.

[13] A. J. Gonzalez, G. Nencioni, B. E. Helvik, A. Kamisinski, "A Fault-Tolerant and Consistent SDN Controller", in Proc. IEEE Global Communications Conf. (GLOBECOM), 2016.

[14] R. Mijumbi, J. Serrat, J. L. Gorricho, N. Bouten, F. De Turck, R. Boutaba, "Network Function Virtualization: State-of-the-Art and Research Challenges", IEEE Communications Surveys & Tutorials, vol. 18, no. 1, 2016, pp: 236-262.

[15] M. Casazza, P. Fouilhoux, M. Bouet, S. Secci, "Securing virtual network function placement with high availability guarantees", in Proc. IFIP Networking Conf. (IFIP Networking), 2017, pp: 1-9.

[16] P. Vizarreta, P. Heegaard, B. Helvik, W. Kellerer, C. Mas Machuca, "Characterization of failure dynamics in SDN controllers", in Proc. the 9th Intl. Wksp Resilient Networks Design and Modeling (RNDM), 2017.

[17] R. Travanca, J. André, "Safety of 5G Network Physical Infrastructures", Chapter 8, book: ?A Comprehensive Guide to 5G Security?, Edited by M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, M. Ylianttila, Wiley, Jan. 2018, pp. 165-193.

[18] N. S. Noorulhassan, A. Gouglidis, F. Arsham, D. Hutchison, "The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog from a Security and Resilience Perspective", IEEE Journal on Selected Areas in Communications, 2017, pp. 2586-2595.

[19] C. Rotsos, A. Farshad, N. Hart, A. Aguado, S. Bidkar, K. Sideris, D. King, L. Fawcett, J. Bird, A. Mauthe, N. Race, D. Hutchison, "Baguette: Towards end-to-end service orchestration in heterogeneous networks", in Proc. Intl. Conf. Ubiquitous Computing and Communications and Intl. Symp. Cyberspace and Security (IUCC-CSS), 2016, pp. 196-203.

[20] F. Nadeem, V. Kvicera, S. Muhammad, E. Leitgeb, S. Muhammad, G. Kandus, "Weather effects on hybrid FSO/RF communication link", IEEE journal on selected areas in communications, 2009.

[21] H. Haas, "LiFi is a Paradigm-Shifting 5G Technology", Reviews in Physics, Elsevier, 2017.

[22] D. Cotroneo, L. De Simone, R. Natella, "NFV-Bench: A Dependability Benchmark for Network Function Virtualization Systems", IEEE Trans. Network and Service Management, vol. 14, no. 4, 2017, pp: 934-948.

[23] D. Cotroneo, R. Natella, S. Rosiello, "NFV-Throttle: An Overload Control Framework for Network Function Virtualization", IEEE Trans. Network and Service Management, vol. 14, no. 4, 2017, pp: 949-963.

[24] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, "Overview of 5G Security Challenges and Solutions", IEEE Communications Standards Magazine, vol. 2, no. 1, 2018, pp: 36-43.

[25] M. Monshizadeh, V. Khatri, A. Gurtov, "NFV Security Considerations for Cloud-Based Mobile Virtual Network Operators", in Proc. 24th Intl. Conf. Software, Telecommunications and Computer Networks (SoftCOM 16), 2016.

[26] A. Ali, C. Anagnostopoulos, D. P. Pezaros, "On the Optimality of Virtualized Security Function Placement in Multi-Tenant Data Centers", in Proc. of the IEEE Intl. Conf. Communications (ICC 2018), 20-24 May 2018.

[27] G. Nencioni, B. E. Helvik, P. E. Heegaard, "Failure Correlation in Availability Modelling of a Software-Defined Backbone Network", IEEE Transactions on Network and Service Management, vol. 14, no. 4, Dec. 2017, pp: 1032 - 1045.

[28] P. E. Heegaard, B. E. Helvik, V. B. Mendiratta, "Achieving Dependability in Software-Defined Networking - A Perspective", in Proc. 7th Intl. Wksp. Reliable Networks Design and Modeling (RNDM 15), October 2015.

[29] A. J. Gonzalez, G. Nencioni, A. Kamisinski, B. E. Helvik, P. E. Heegaard, "Dependability of the NFV Orchestrator: State of the Art and Research Challenges", Accepted for publication in IEEE Communications Surveys & Tutorials, 2018.