TU Delft

Delft University of Technology

Technology-related Disasters

A Survey towards Disaster-resilient Software Defined Networks

Mas Machuca, Carmen; Secci, Stefano; Vizarreta, Petra; Kuipers, Fernando; Gouglidis, Antonios; Hutchison, David; Jouet, Simon; Pezaros, Dimitrios; Elmokashfi, Ahmed; Heegaard, Poul

DOI
10.1109/RNDM.2016.7608265

Publication date
2016

Document Version
Accepted author manuscript

Published in
2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)

Citation (APA)
Mas Machuca, C., Secci, S., Vizarreta, P., Kuipers, F., Gouglidis, A., Hutchison, D., Jouet, S., Pezaros, D., Elmokashfi, A., Heegaard, P., Ristov, S., & Gusev, M. (2016). Technology-related Disasters: A Survey towards Disaster-resilient Software Defined Networks. In M. Jonsson, J. Rak, A. Somani, D. Papadimitriou, & A. Vinel (Eds.), *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)* (pp. 35-42). IEEE. https://doi.org/10.1109/RNDM.2016.7608265

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

Technology-related Disasters: A Survey towards Disaster-resilient Software Defined Networks

Carmen Mas Machuca[*], Stefano Secci[†], Petra Vizarreta[*], Fernando Kuipers[§], Antonios Gouglidis[**], David Hutchison[**], Simon Jouet[††], Dimitrios Pezaros[††], Ahmed Elmokashfi[***], Poul Heegaard[†††], Sasko Ristov[§§]

[*]Technical University of Munich (TUM), Germany
[†] Sorbonne Universités, UPMC Univ Paris 06, France
[§] Delft University of Technology, the Netherlands
[**] Lancaster University, UK
[††]University of Glasgow, Scotland
[***]Simula Research Laboratory, Norway
[†††]Norwegian University of Science and Technology, Norway
[§§]University of Innsbruck, Austria

cmas@tum.de, stefano.secci@upmc.fr, petra.vizarreta@lkn.ei.tum.de, f.a.kuipers@tudelft.nl, a.gouglidis@lancaster.ac.uk, d.hutchison@lancaster.ac.uk, s.jouet.1@research.gla.ac.uk, Dimitrios.Pezaros@glasgow.ac.uk, ahmed@simula.no, poul.heegaard@item.ntnu.no, sashko@dps.uibk.ac.at

***Abstract*— Resilience against disaster scenarios is essential to network operators, not only because of the potential economic impact of a disaster but also because communication networks form the basis of crisis management. COST RECODIS aims at studying measures, rules, techniques and prediction mechanisms for different disaster scenarios. This paper gives an overview of different solutions in the context of technology-related disasters. After a general overview, the paper focuses on resilient Software Defined Networks.**

Keywords—software defined networks, resilience, disaster survivability

I. INTRODUCTION

The increase in capacity of communication networks has boosted the importance of their reliability. Apart from random failures such a fiber cuts, disaster-based failures may also occur. These failures are due to natural disasters (e.g. floods or earthquakes), malicious attacks (like denial of service – DDoS) or technology-related disasters. In spite of significant efforts and investments for high-availability, infrastructure systems occasionally experience software/ hardware failures, operation errors, security attacks or natural disasters. Upon the occurrence of such undesired events, it is crucial to recover the system as quickly as possible.

This paper aims at looking into technology-related disasters. This type of disasters encompasses different disruptions, such as power blackouts that affect several nodes, misconfigurations which causes wrong traffic routing, electromagnetic Pulse (EMP) attacks (i.e., an intense energy field) that instantly overload or disrupt multiple electrical circuits in a large geographic area.

Although this paper focuses mainly on resilience of Software Defined Networking (SDN), in the latter part of this section, we first present an overview of three main categories and aspects of technology-related disasters, including: power outages, social resilience, and correlated cascading failures.

A. *Power Outages*

Power blackouts do not only interrupt or limit everyday life but also complicate or even preclude communications, by affecting communication infrastructures. Unavailability of communication infrastructure affects not only regular communications but also public safety communications. Power blackouts can have impact on a large number of customers: India (2012) with 670 million of affected users, Brazil and Paraguay (2009) with 87 million of affected users, Europe (2006) with 10 million affected users [1].

The causes of power blackouts can be classified as failure of production, failure of transmission or due to increased demands (e.g., due to a heat wave). It has been shown that power supply is a terrorism and military target by using bombs, cyber-attacks (e.g., the Stuxnet virus), HEMP (high altitude electromagnetic pulse), and IEMI (Intentional Electro Magnetic Interference) attacks [2].

The impact and risk of communication networks by power blackouts has been analyzed by the German Federal Parliament [3] for three different scenarios: Scenario 1 (outages of less than 8 hours), Scenario 2 (outages of 8-24 hours) and Scenario 3 for outages of more than 1 day. It was shown that mobile networks and Internet access networks could survive Scenario 1 but not Scenarios 2 and 3. This conclusion is based on the batteries availability and duration.

However, it has been shown that in case of power-based disasters, communications is possible by using short-radio technologies, by making creative use of the remains of the technological landscape by users [4] or by allowing private wireless routers to transition to an emergency mode creating a supportive wireless mesh network [5]. Furthermore, network

operators consider also techniques to limit the impact of power outages like using different power suppliers and associating nodes of the same power supplier to the same shared risk group.

B. Social resilience

Maclean et al. in [6] investigate the social aspects of resilience, and identify six attributes for resilience, namely, knowledge, skills and learning; community networks; people-place connections; community infrastructure; diverse and innovative economy; and engaged governance. Nevertheless, the authors argue that a distinct knowledge gap with regards to resilience's social aspects, still remains. This was the result of exploring social resilience using grounded theory, and by identifying the context of resilience in several areas, e.g., complex systems, social and health sciences, etc. Further recommendations are provided by the authors, which are mostly focused on building the six attributes of resilience. This may lead, eventually, to strengthening the ability of societies, communities and people to adapt, transform, and become stronger in the face of various challenges.

In [7] Mark et al. examine citizens' response to disasters. Specifically, investigations are performed on how people tend to use technology, and how people adapt technologies in the presence of a critical threat. Such investigations can provide information about the systemic changes and implications with regard to how technology can support people to be resilient in disrupted environments. The approach applied by the authors, includes a set of ethnographic studies that helped them in identifying properties of resilience within the group of interviewees. A major contribution of this work is the provision of a better understanding of peoples' culture in relation with technology adoption.

C. Correlated cascading failures

Disaster disruptions can result in a cascade of failures that impact several seemingly independent infrastructures. For example, the failure of three power plants in mid-august 2003 triggered a cascading of power failures affecting 50 million people in the US northwest and the province of Ontario in Canada [8]. This failure had also a visible impact on the interrelated Internet infrastructure, affecting almost half of all Internet autonomous systems. Pahwa et al. [9] used simulations to analyze the vulnerability of power grids to cascading failures. They found that careful post-failure load redistribution can help averting cascades. Further, building a loosely-coupled grid of islands of different power sources, e.g. renewables, can also reduce the risk for cascades. Motivated by the large-scale cascading failure that crippled the Italian power and Internet infrastructures on September 28, 2003, Buldyrev et al. [10] studied and modeled the interplay between the underlying topologies and vulnerabilities to cascades in interdependent networks. Surprisingly, unlike a single isolated network a broader degree distribution makes interdependent networks more vulnerable to random failures. Their findings stressed the importance of taking interdependence into account when designing networks.

Lawler et al. [11] reviewed traditional disaster recovery approaches and disaster tolerance techniques in general as well as the risk for cascades triggered by IT applications downtime. They found that disaster recovery and business continuity plans are often laid out after an application has been designed and implemented which does not scale given the increasing complexity of today's systems. Instead, they argue for the inclusion of an appropriate level of disaster tolerance when building systems. Further, this must also include a proper understanding of independencies between systems.

D. Proposed solutions

Several efforts have proposed solutions for maintaining connectivity at times of massive failures caused by natural and technological disasters. Operating ad-hoc information or content centric (ICN or CCN [12]) networks that relay data packets based on their contents is viewed as a promising approach.

Oh et al. [13] showed that building a content-centric network on top of a large scale mobile ad-hoc network can provide a simple content search and delivery systems in environment with high mobility and poor performance such as in battlefields and emergency situations. Inspired by Information Centric Networking (ICN) concepts, [14] proposed a name-based communication framework to forward messages between nearby nodes in an infrastructure-less environment. The proposed approach focuses on replicating messages based on their content, instead of blindingly routing all messages, to increase the chance of successfully transmitting critical messages e.g., between first responders. The authors of [15] have proposed a similar solution that derives message priorities from node names. Monticelli et al. [16] extended this further by leveraging delay tolerant networks concepts to deliver data between fragmented ICNs such as ambulances and police cars. Each node maintains a state that captures the likelihood of encountering nodes that belong to different networks. This probability is then used to determine whether a node is a suitable data mule.

Software Defined Networking (SDN) has attracted a great deal of attention, because by centralizing the control logic and separating it from the data plane, SDN enables high flexibility and programmability of the network, as well as vendor-agnostic equipment, control and management. Therefore, this paper focuses on disaster Resilient SND. Section II summarizes the measures to characterize network failures and the methodology to counter them. Section III gives an overview of different techniques towards reliable SDN in terms of data and control plane. Section IV focuses on some first disaster-specific reliable SDNs, and finally Section V concludes the paper.

II. MEASURES AND METHODOLOGY

In this section, we provide a survey on experimental works that characterize network failures and how, with such knowledge, to obtain high-level network design methodologies and best practices for network operators.

A. *Modelling for quantitative assessment*

A method towards resilience analysis of networked systems-of-systems is proposed in [17] by Filippini and Silva, i.e., a modeling framework for the resilient analysis of networked systems-of-systems based on functional dependencies. The originality of that research work is concentrated mostly in the modeling and analysis of complex and heterogeneous systems. Specifically, important features of the framework include the support for functional dependencies, and the possibility of performing a sensitivity analysis with respect to system variability. Although the framework provides a method and analysis based on resilience sets, there are still several topics that may require refinements, viz. the language used for constructing elements, the model of the network response, resilience analysis models, etc.

B. *Measures*

Rare are the works in the communications and networking literature characterizing node and/or link failures in operational networks in a way that can be exploited by researchers to emulate the failures and to design advanced network management and design algorithms.

We focus in the following on three works that, with different scopes and levels of detail, try to characterize such failures. We describe a recent work characterizing failures happening in a regional network provider network in Scandinavia [18]. Then we describe another research about failures in an inter-continental network centered in North America [19], where a particular focus is given to transient failures. Moreover, we describe a work on the characterization of long-lasting failures, in particular happening after a large scale disaster in Japan.

First, the authors in [18] focus on the time-between-failure process, in particular on finding best-fitting well-known distributions. They found that the time-between-failures process for routers and short distance links can be characterized by a Weibull distribution. On the other hand, they found that the time-between-failures of long distance links is better fit by a gamma distribution.

The authors in [19] go beyond a characterization based on the geographical reach of the links, and also distinguish between planned failures and unplanned failures. For an inter-continental carrier network, it is shown that 20% of all failures are planned failures. The unplanned failures are further classified into individual link failures and shared link failures (router-related or optical related). Individual link failures account for 70% of the unplanned failures. An interesting observation is that 55% of all individual link failures are caused by 2.5% of the links. These are denoted high failure links. It is also important to report that all high failure links are backbone links, while low failure links are mainly access links. Most of high failure links are inter-POP links, and half of them share a router with another high failure link. Once classified in the two classes of high failure and low failure links, two power law regimes were identified.

Empirical Cumulative Distribution Functions (CDFs) of the time-between failures for high failure links are given, because a corresponding analytical approximation could not be found. It is shown that a subset of the high failure links experiences very bursty failures, i.e., most of failures occur over a short time period, and at a different extent [19]. On the other hand, some other subsets of high failure links exhibit failure patterns that persist over the entire time period. Therefore, the time-between-failure process presents quite heterogeneous cases.

The empirical CDFs of the time-to-repair for the unplanned link failures are also reported, distinguishing between high failure links, low failure links and shared (router and optical layer) failures. The three distributions significantly differ from each other. For example, the ratio of links having a time-to-repair less or equal than 25s is roughly 50% for high failure links, 30% for low failure links, and only 6% for shared failures. All in all, the time-to-repair for high failure links is generally much shorter than for the other types of unplanned failures.

With the motivation that failures that last longer and that affect a large amount of users are those that should be addressed first by any resilient network planning logic, the authors in [20] focus on failures lasting more than 2 hours and affecting more than 30,000 users. Their major finding is that the time-between-failures follows a Poisson distribution, while their duration (hence not counting the time-to-repair) follows a Pareto distribution. They also analyzed other aspects related to the scale of a failure – for instance they report that the number of users affected by such serious failures follows a piecewise Pareto distribution.

C. *Methodology*

It is widely recognized that the Internet is not sufficiently resilient, survivable, and dependable, and that significant research, development, and engineering is necessary to improve the situation. Resilience must be viewed as an essential design and operational characteristic of future networks in general, and the Global Internet in particular. Sterbenz et al. [8] define network resilience as the ability of a network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation. The paper also provides a survey of the disciplines that resilience encompasses, along with significant past failures of the network infrastructure. This includes scientific disciplines (trustworthiness, with dependability, security, performability), and challenge tolerance (with survivability, fault-tolerance, traffic tolerance, disruption tolerance). The "ResiliNets" framework in [8] provides a resilience strategy to defend against, detect, and remediate challenges, presented as a "rule of thumb" set of principles for designing resilient networks, as well as related techniques described to analyze network resilience.

The authors in [1], [10] and [21] further investigate network resilience, arguing that network resilience methodologies and solutions should be taking into account dependencies between network components and between systems at large to avoid large scale serious failures.

In [21], it is stressed that today's infrastructure, e.g. transportation, commerce and other economic activity, and

interaction of all kinds may be regarded as a set of interconnected and interdependent networks. The kernel of these networks is constituted by the ICT infrastructure. These networks of networks are complex and poorly understood and their interdependence makes them vulnerable to failures/unforeseen events and may cause an unforeseen global spread of events with disastrous consequences, i.e., they pose a hyper-risk. The paper advocates a paradigm shift in thinking: systemic instabilities can be understood by a change in perspective from a component-oriented to an interaction- and network-oriented view. This calls for a fundamental change in the design and management of complex dynamical systems. The main contribution in the paper is to put this issue authoritatively on the research agenda and to make a state of the art overview of the insight we have in this problem domain, with respect to drivers and examples of systemic instabilities, and available mathematical models to get a fundamental understanding of the problem.

Under a similar view, the authors in [10] study the case where two networks are interdependent in such a way that failures of a node in one of the networks may result in the failure of dependent nodes in the other network, and vice versa. This is considered to be important as it may lead to a cascade of recursive failures and result in a system breakdown. The blackout that affected much of the Italian power grid on September 28, 2003 is used as a motivating and illustrative example: the shutdown of power stations led to the failure of nodes in the communication network, which again caused loss of control and failure of power stations. [10] proposes a methodology for understanding the robustness of interacting networks subject to cascading failures. A model of such phenomena is introduced and analyzed to obtain its better understanding and its dependence of the basic network topology and parameters. Analytical solutions are obtained for the critical fraction of nodes that, on removal, will lead to a failure cascade and to result in a complete fragmentation of the two interdependent networks.

Also, the authors in [1] propose a methodology on the resilience analysis of systems-of-systems. A special instance in their analysis is that of infrastructures. The analysis of infrastructures under disturbance or malfunctioning, as well as their ability to resist, react and recover (resilience) is identified as one of the most challenging issues in this paper.

The important features that are identified to be of importance in their methodology are:

(1) functional dependencies, and
(2) the possibility of performing a sensitivity analysis with respect to system variability.

The proposed methodology is claimed to provide along with its analysis tool-set a standalone framework for assessing the resilience of complex networked systems-of-systems.

As a common denominator of these works, we can therefore summarize that certainly it is important to understand individual failures as described in the previous subsection, however, the most dangerous failures, such as those impacting a large number of users and lasting for long time are most likely to trigger a cascade of failure and increase the scale of service disruption perceived by end-users. Hence methodologies meant to propose countermeasures for serious failures should be rooted on the dependability analysis of networks in particular and distributed interconnected systems in general.

III. RELIABLE SOFTWARE DEFINED NETWORKS

The concept of Software Defined Networking (SDN), in which the data and control planes are decoupled [22], [23], has drawn tremendous attention in recent years, and provides new possibilities in traffic engineering and, hence, also in reacting to failures. In SDN, the control plane, represented by SDN controllers, computes the forwarding rules and installs them in the data plane switches, which forward the packets according to those rules.

Doerr and Kuipers [24] have provided a taxonomy of Internet failures, which revealed that many failures are outside of the scope of existing protection schemes.

Special attention is being paid to security issues which can be mainly classified as:

(1) Denial of Service (DoS) attacks, which causes overloading of controllers by the creation of new and unknown flows (in case a switch does not have a rule associated to a flow, it forwards it to the controller),
(2) conflicting rules,
(3) malicious applications,
(4) unreliable control-switch communications by taking the role of the controller or the attacker, etc.

All these issues have not been studied in detail yet.

Let us summarize the state of the art of data and control plane reliability related to physical failures (mostly link and/or node failures).

A. *Data Plane reliability*

For SDN to be able to deal with the plethora of failures that may occur, it itself needs resiliency mechanisms. As pointed out by Sharma et al. [25], when a failure occurs, obtaining new rules from the controller will take more time than the carrier-grade recovery requirement of 50 ms permits. Hence, some form of local rerouting needs to be introduced.

Sharma et al. [25] assume preconfigured primary and backup paths for the flows and make use of (path-based) Bidirectional Forwarding Detection (BFD) to detect failures. BFD, which can be used over any transport protocol, uses control and echo messages between preconfigured end-points to detect whether links or paths are up. Sharma et al. also use OpenFlow's fast-failover mechanism (which is part of the group table concept present in OpenFlow versions 1.1 and later; OpenFlow being a popular SDN protocol to communicate between switch and controller) to reroute without involvement of the controller. Their approach is tested on several networks and shown to achieve failover times between 42 and 48 ms.

Van Adrichem et al. [26] use link-based BFD to realize an order of magnitude speed-up in the failover time, compared to

the path-based approach of Sharma et al. However, both Sharma et al. and van Adrichem et al. focus on failure detection and failover to preconfigured paths, but they do not address the problem of how to find the best alternate paths to preconfigure.

The approach by Tilmans and Vissicchio [27] is somewhat different, but does include a mechanism for alternate paths to be found (eventually). They propose a hybrid approach in which SDN takes care of the overall network configuration, but the controller also instructs the "local agents" of the nodes to run a link-state IGP protocol (like OSPF or IS-IS). The idea is that when a failure occurs, and since asking the controller is too time consuming, the IGP protocol will have to adjust to the situation and can point to alternate routes. One disadvantage of this approach is that IGP convergence may be too slow for carrier-grade recovery. The authors mention that by adopting IGP with fast reroute mechanisms, fast failover should be possible (although no failover times are reported in the paper).

Braun and Menth [28] do use fast reroute in SDN. IP fast reroute finds loop-free alternative hops by examining the distance estimates (which are computed anyway to populate the routing table). Which alternative neighbours to use depends on the desired level of protection (e.g., single link failure protection or single node failure protection). Unfortunately, the stricter the protection level, the fewer alternatives may exist. On the other hand, the lower the protection level, the more loops may appear, if failures manifest that were not part of the protection scheme. To detect loops, Braun and Menth propose to encode some failure information in the packets. However, since the approach remains quite close to IP fast reroute, by relying on shortest path distance estimates, the potential of centralized control logic is not fully harnessed.

Van Adrichem et al. [29] therefore argue to enable failure recovery in SDN networks by using:

(1) fast failure detection through liveliness monitoring protocols, as done in [26],
(2) failure protection by having the SDN controller preconfigure backup rules, which would lead to the fastest recovery approach possible, but may lead to a temporary non-optimal network configuration, and
(3) re-computation of optimal primary and backup rules, once the controller is notified of the failure.

Steps 2 and 3 essentially involve the same computations. Van Adrichem et al. [29] provide the algorithms to compute those primary and backup rules and which can handle both single link and single node failures at only a limited cost in the increase of the flow and group tables.

Cascone et al. [30] have presented SPIDER – a stateful mechanism to detect and protect against failures in SDN. Their approach is based on OpenState [31], which is an extension of OpenFlow to allow switches to apply different rules depending on their "state" rather than induced by the controller. Failure or packet-level events could then, for example, trigger a change in state. The use of states is interesting as it, in principle, allows reacting differently to different types of failures. However, which actions to best take in which states is still a complex question and is not addressed in the paper. The authors refer to their prior work [32] to indicate that primary and backup paths could be computed. However, the technique used in [32] is that of mixed integer linear programming, which has an exponential running time and may be too costly to execute on large realistic networks. Fortunately, SPIDER can operate with any algorithm. For example, it could use the algorithms of van Adrichem et al. [29], which run in polynomial time, possibly together with other algorithms for different types of failures. See [33] for an overview of protection algorithms.

While the work mentioned above may adequately handle single failures, it may have to rely on the controller to give instructions when large-scale disasters manifest. Moreover, the work assumes that the controller platform itself is unaffected by the failure. More work is needed for SDNs in order to be able to deal with disasters and/or controller failures.

B. Control Plane Reliability

Reliable controller placement is a special subset of controller placement problems, which focuses on optimization of different reliability aspects of the control plane, such as improvement of survivability and fault tolerance and minimization of expected control path loss.

The goal of resilient routing is to find optimal working and backup paths between source and destination. Resilient anycast routing focuses on finding optimal working and backup paths between the source and any of the replicas of the destination node [34], which can also be applied to the resilient controller placement problem.

Both aspects complement each other for resilient SDN control plane design, hence in the following sections, an overview of the related work on reliable controller placement and resilient routing is presented.

The controller placement has a significant impact on the reliability and fault tolerance of the SDN control plane. The SDN controller is the brain of the network and its failure can have an impact on a large number of forwarding devices.

Hu et al. [35] discuss different reliability measures. Deterministic reliability measures focus on connectivity, i.e. number of disjoint paths between the nodes and the controller or cardinality of minimum cut set. Probabilistic reliability measures include the probability of the failure of individual physical components to calculate the expected control path loss.

Expected loss of the control path is formulated as a mixed integer linear programming (MILP) problem. In [36] Hu et al. use several approaches to minimize the expected control path loss. Random placement, *l-w*-greedy and simulated annealing algorithms were compared to a brute-force approach. Performance is evaluated as the ratio between the best solutions found by a given algorithm to the best solutions found by brute force. Simulated annealing, *2-1*-greedy and *1-1*-greedy show the best performance.

Another approach proposed by Zhang et al. [37] is based on a modified version of min-cut clustering. A cluster is defined as a set of nodes controlled by the same controller. The algorithm first finds a clustering of the network with the smallest number of edges belonging to different clusters (min-cut) and then it assigns a controller to the node that has shortest average distance to all the other nodes in the same partition.

Muller et al. [38] use the node connectivity to find the best placement for the controllers. The placement is defined as an MILP problem that maximizes the number of node disjoint paths between the controllers and the assigned switches. Connectivity is pre-calculated for every pair of nodes in the network and it is given as an input to a MILP solver. This algorithm outperforms the one based on modified min-cut clustering defined in [37] in terms of number of disconnected network elements for different failure scenarios.

Network should be resilient against controller failure, network component failure, load imbalance and inter-controller latency. Hock et al. [39] introduced a framework for resilient Pareto-based Optimal COntroller placement (POCO), which provides all Pareto-optimal controller placements. The authors show that more than 20% of the nodes should be controller nodes in order to keep alive at least one connection between a node and a controller, if an arbitrary double link or node fails. Since all mentioned issues and problems are opposite proportional, and it is very difficult, or even impossible, to find the optimal values, Pareto-optimal solutions give an adequate trade-off.

Adding one or more backup controllers could mitigate the risk of compromising the network resilience, but some mechanisms for coordination between the primary controller and other backup controllers are necessary in order not to lose the gathered information and the latest configuration. Fonseca et al. [40] present a mechanism that can increase the resilience in SDN by using a component organization that handles the updates received by the network or other components. Their CPRecovery component increases the resilience by handling several failure types as it allows an easy transition between the failed and the backup controller, which has the latest network state. Introducing the component does not require deep changes in the SDN protocol, neither produces a significant overhead

In [41] Jimenez et al. define an algorithm named *k*-Critical to minimize the number of controllers necessary to provide latency guarantees, while also minimizing the number of hops it takes to reach a controller. The logic behind this is that a smaller number of hops in a control path has a positive impact on its reliability, since there are fewer nodes and switches whose failures can interrupt the connection.

Ros et al. [42] use control plane reliability to find how many controllers each node should be connected to in order to achieve ”five nines reliability” commonly required in typical communication systems. The goal was to provide a required degree of reliability with minimum number of controllers. An interdependent network approach was used by Guo and Bhattacharya in [43] to find the optimal controller placement and to study how the cascading of failures affect the control plane reliability.

Resilient controller placement is adding a new dimension to resilient anycast routing, because the positions of the server replicas (or in our case SDN controllers) are not known in advance. Vizarreta et al. [44] provide two resilient controller placement models for joint optimization of controller placement and resilient control path routing.

IV. Disaster-resilient Software Defined Networks

This section focuses on the first solutions towards disaster resilient SDN networks. Cheng et al. [45] have proposed a cross-layer framework to improve the survivability of the network suffering from multiple correlated failures. The proposed framework relies on GeoDivRIP a novel routing protocol that provides resilience through geographically diverse paths. An SDN controller running a failure detection module analyses the link-layer network statistics, focussing on network delay and congestion state to calculate the distance of separation between paths. Based on the distance, the geodiverse paths for GeoDivRP are calculated, and traffic allocation optimizations are performed. The optimized traffic allocation, as well as the set of geodiverse paths are passed to ResTP, a resilient transport protocol. Furthermore, the applications can provide expected threat models to ResTP and GeoDivRP to allocate different routes based on expected threats. However, this approach relies on the controller keeping a complete and up-to-date view of the network statistics and link-sate to compute the geodiverse paths which might be impractical in large-scale deployments.

To ensure resilient services in a multi-domain system (a “digital ecosystem”), requires flexible and scalable solutions for exchange of information between the different domains. Today’s Border Gateway Protocol (BGP) severely constrains how networks can deliver traffic over the Internet and how to guarantee performance and dependability. Gupta et. al. [46] argue that Software Defined Networking (SDN) could revolutionize wide-area traffic delivery, by offering direct control over packet-processing rules that match on multiple header fields and perform a variety of actions. The paper describes a Software Defined IXP (called “SDX”), which provides:

(1) “application-specific peering”,
(2) programming abstractions that allow participating networks to create and run these applications,
(3) correct running when interacting with BGP,
(4) ensures that applications do not interfere with each other, and
(5) system scalabilty (rule-table size and computational overhead).

Sedef Sadav et al. [47] address the resilience aspect of the network under man-made attacks, such as electromagnetic pulse (EMP) or Weapon of mass destruction (WMD), with a particular emphasis on the cascading failures after the main event. The authors are proposing to use SDN to address today’s inability to respond in a timely fashion to large and complex disasters. Differently from early work on SDN-based resilient systems relying on a physical centralized control plane architecture suffering from scalability, performance and reliability problems in large deployments, this paper proposes

to design a control plane to be disaster-aware by designing it as a virtual network and solving it through a virtual-network-embedding (VNE) approach. The proposed approach decides on the number and placement of controllers across the network and maps them onto the physical network. To assess their approach, the authors use a probabilistic disaster model and use it to calculate a vulnerability metric that captures the expected connectivity loss of the control-plane due to controller node failure, inter-controller communication failure and controller-to-switch failure. Finally, they present a mathematical formulation for jointly optimizing the virtual topology design and VNE such that control-network connectivity is ensured after failure.

Although SDN provides an abstraction and an architecture that is flexible and can allow the administrators an easy configuration of network devices, still there is a lack of support in orchestrating many services that should cooperate among each other in order to implement network-wide resilience. Future networks will probably consist of more closed devices, such as security appliances, which opens a challenge: How to use the resilience management in settings that include coupled and decoupled deployment models? Smith et al. [48] introduced a resilience management framework, which can be applied to the problem of orchestration of OpenFlow-based services toward network resilience implementation. The framework consists of policy-controlled management patterns, which describe the process of orchestration of individual resilience services. These services are implemented as OpenFlow applications, possibly over several distributed controllers. The resilience mechanisms include detection of attacks and anomalies (e.g., IDSs and bandwidth monitoring), as well as their remediation. The patterns specify how to reconfigure the deployed mechanisms in order to address some specific network challenge.

V. Conclusion

This paper aims at giving an overview of different technology-related disasters affecting communication networks. Due to the importance of Software Defined Networking (SDN), special attention has been devoted to present the state of the art on the resilience issues and approaches towards resilient SDN networks. However, there are still some open issues, such as security and consideration of disaster scenarios, which will be studied in the framework of the COST RECODIS Action.

Acknowledgment

This article is based upon work from COST Action CA 15127 ("Resilient communication services protecting end-user applications from disaster-based failures – RECODIS") supported by COST (European Cooperation in Science and Technology).

References

[1] C. Reuter "Power Outage Communications: Survey of Needs, Infrastructures and Concepts", ISCRAM 2013 Conference, Baden-Baden, Germany, May 2013.

[2] CRO Forum, "Power Blackout Risks: Risk Management Options" Position Paper, November 2011.

[3] Deutscher Bundestag, *Gefährdung und Verletzbarkeit moderner Gesellschaften –am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung*, 2011.

[4] A. Al-Akkad, L. Ramirez, S. Denef, A. Boden, L. Wood, M. Büscher, and A. Zimmermann, "Reconstructing Normality: The Use of Infrastructure Leftovers in Crisis Situations As Inspiration for the Design of Resilient Technology," In Proceedings of the Australian Computer-Human Interaction Conference, Adelaide, Australia, November 2013 (pp. 457–466).

[5] K. Panitzek, I. Schweizer, A. Schulz, T. Bönning, G. Seipel, and M. Mühlhäuser, „Can We Use Your Router, Please? Benefits and Implications of an Emergency Switch for Wireless Routers," International Journal of Information Systems for Crisis Response and Management, 4(4), 59–70, 2012.

[6] K. Maclean, M. Cuthill, and H. Ross, "Six attributes of social resilience," Journal of Environmental Planning and Management, 57(1), 144-156, 2014.

[7] G. J. Mark, B. Al-Ani, and B. Semaan, "Resilience through technology adoption: merging the old and the new in Iraq," In Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems, pp. 689-698, April 2009.

[8] J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," Comput. Netw. 54, 8 (June 2010), 1245-1265.

[9] S. Pahwa, C. Scoglio, and S. Noel, "Topological analysis and mitigation strategies for cascading failures in power grid networks," *arXiv preprint arXiv:1212.5620* (2012).

[10] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," Nature, 464(7291):1025–1028, 04 2010.

[11] C. M. Lawler, S. A. Szygenda, and A. T. Mitchell, "Techniques for disaster tolerant information technology systems," *1st Annual IEEE Systems Conference*, 2007.

[12] J. Rak, *Resilient routing in communication networks*, Berlin: Springer, 2015 (section: "The concept of survivable anycasting" pp. 58-70).

[13] S. Y. Oh, L. Davide, and M. Gerla, "Content centric networking in tactical and emergency manets," *2010 IFIP Wireless Days (WD),* 2010.

[14] I. Psaras, L. Saino, M. Arumaithurai, K. K. Ramakrishnan, and G. Pavlou, "Name-based replication priorities in disaster cases," In *INFOCOM WKSHPS,* pp. 434-439, 2014.

[15] J. Seedorf, A. Tagami, M. Arumaithurai, Y. Koizumi, N. B. Melazzi, D. Kutscher, and T. Yagyu, "The Benefit of Information Centric Networking for Enabling Communications in Disaster Scenarios," In *IEEE Globecom Workshops,* pp. 1-7, 2015.

[16] E. Monticelli, B. M. Schubert, M. Arumaithurai, X. Fu, and K. K. Ramakrishnan, "An information centric approach for communications in disaster situations," In *IEEE 20th International Workshop on Local & Metropolitan Area Networks (LANMAN)*, pp. 1-6, May 2014.

[17] R. Filippini and A. Silva, "A modeling framework for the resilience analysis of networked systems-of-systems based on functional dependencies," Reliability Engineering and System Safety 125, pp. 82-91, 2014.

[18] A. J. Gonzalez and E. B. Helvik, "Characterisation of router and link failure processes in UNINETT's IP backbone network," International Journal of Space-Based and Situated Computing 7, 2(1), 3-11, 2012.

[19] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C. Chuah, Y. Ganjali, and C. Diot, "Characterization of failures in an IP backbone," *IEEE/ACM Trans. Netw.*, vol. 16, no. 4, 2008.

[20] M. Uchida, "Statistical characteristics of serious network failures in Japan," Reliability Engineering & System Safety, 131, 126-134, 2014.

[21] D. Helbing, “Globally networked risks and how to respond,” Nature, 497:51 – 59, May 2, 2013.

[22] J. Rak, D. Papadimitriou, H. Niedermayer, P. Romero, “Information-driven network resilience: Research challenges and perspectives,” *Optical Switching and Networking*, *Elsevier,* pp. 1-23, 2016, doi: 10.1016/j.osn.2016.06.002

[23] J. Rak, M. Pickavet, K.S. Trivedi, J.A. Lopez, A. Koster, J.P.G. Sterbenz, E.K. Cetinkaya, T. Gomes, M. Gunkel, K. Walkowiak, D. Staessens, “Future research direction in design of reliable communication systems,” *Telecommunication Systems, Springer*, vol. 60, no. 4, pp 423-450, 2015.

[24] C. Doerr and F.A. Kuipers, “All quiet on the Internet front?”, IEEE Communications Magazine, vol. 52, no. 10, pp. 46-51, October 2014.

[25] S. Sharma, D. Staessens, D. Colle, M. Pickavet, and P. Demeester, “OpenFlow: Meeting carrier-grade recovery requirements,” Computer Communications, vol. 36, no. 6, pp. 656–665, March 15th, 2013.

[26] N. van Adrichem, B. van Asten, and F.A. Kuipers, “Fast Recovery in Software-Defined Networks,” Proc. of the European Workshop on Software Defined Networking (EWSDN 2014), Budapest, Hungary, September 1-3, 2014.

[27] O. Tilmans and S. Vissicchio, “IGP-as-a-backup for robust SDN networks,” Proc. of the 10th International Conference on Network and Service Management (CNSM) and Workshop, Rio de Janeiro, Brazil, 17-21 Nov. 2014.

[28] W. Braun and M. Menth, “Loop-Free Alternates with Loop Detection for Fast Reroute in Software-Defined Carrier and Data Center Networks,” Journal of Network and Systems Management, pp. 1-21, April 5th, 2016.

[29] N. van Adrichem, F. Iqbal, and F.A. Kuipers, “Fast All-to-All Link and Node Failure Recovery in Software-Defined Networks,” arXiv preprint arXiv:1605.09350, 2016.

[30] C. Cascone, L. Pollini, D. Sanvito, A. Capone, and B. Sansò, “SPIDER: Fault Resilient SDN Pipeline with Recovery Delay Guarantees,” Proc. of the 2nd IEEE Conference on Network Softwarization (IEEE NetSoft), Seoul, Korea, June 2016.

[31] G. Bianchi, M. Bonola, A. Capone, and C. Cascone, “OpenState: programming platform-independent stateful OpenFlow applications inside the switch,” SIGCOMM Comput. Commun. Rev., vol. 44, no. 2, pp. 44-51, Apr. 2014.

[32] A. Capone, C. Cascone, A. Q. Nguyen, and B. Sansò, “Detour planning for fast and reliable failure recovery in SDN with OpenState,” Proc. of the 11th International Conference on the Design of Reliable Communication Networks (DRCN), March 2015.

[33] F.A. Kuipers, “An Overview of Algorithms for Network Survivability,” ISRN Communications and Networking, vol. 2012, Article ID 932456, 19 pages, 2012.

[34] K. Walkowiak and J. Rak, “Joint optimization of anycast and unicast flows in survivable optical networks,” in Proceedings of 14th International Telecommunications Network Strategy and Planning Symposium, Sept. 2010.

[35] Y. Hu, W. Wang et al., ”On reliability-optimized controller placement for Software-Defined Networks,” in China Communications, vol. 11, no. 2, 2014, pp. 3854.

[36] Y. Hu, W. Wendong, X. Gong, X. Que and C. Shiduan, “Reliability-aware controller placement for Software-Defined Networks,” Integrated Network Management (IM 2013), pp. 672-675), 2013.

[37] Y. Zhang, N. Beheshti, and M. Tatipamula, ”On resilience of split-architecture networks,” in 2011 IEEE Global Telecommunications Conference (GLOBECOM), Dec. 2011, pp. 16.

[38] L. F. Muller et al., ”Survivor: An enhanced controller placement strategy for improving SDN survivability,” in IEEE Global Telecommunications Conference (GLOBECOM), 2014, pp. 19091915.

[39] D. Hock, M. Hartmann, S. Gebert, M. Jarschel, T. Zinner, and P. Tran-Gia, “Pareto-optimal resilient controller placement in SDN-based core networks,” *25th International Teletraffic Congress (ITC),* Shanghai, 2013, pp. 1-9.

[40] P. Fonseca, R. Bennesby, E. Mota, and A. Passito, “A replication component for resilient OpenFlow-based networking,” *IEEE Network Operations and Management Symposium*, Maui, HI, 2012, pp. 933-939.

[41] Y. Jimenez, C. Cervell-Pastor, and A. J. Garca, ”On the controller placement for designing a distributed SDN control layer,” in IFIP Networking Conference, 2014.

[42] F. J. Ros and P. M. Ruiz, ”Five nines of southbound reliability in software defined networks,” in Proc. 3rd Workshop Hot Topics Software Defined Networks, 2014, pp. 31-36.

[43] M. Guo and P. Bhattacharya, “Controller Placement for Improving Resilience of Software-Defined Networks,” *International Conference on Networking and Distributed Computing (ICNDC),* pp. 23-27, 2013

[44] P. Vizarreta, C. Mas Machuca, and W. Kellerer “Controller Placement Strategies for a Resilient SDN Control Plane” RNDM, Sweden, 2016.

[45] Y. Cheng, M. M. Rahman, S. Gangadhar, M. J. F. Alenazi, and J. P. G. Sterbenz, “Cross-layer framework with geodiverse routing in software-defined networking” in Proc. 11th International Conference on Network and Service Management (CNSM 2015), Nov. 2015

[46] A. Gupta, L. Vanbever, M. Shahbaz, S. P. Donovan, B. Schlinker, N. Feamster, J. Rexford, S. Shenker, R. Clark, and E. Katz-Bassett, “SDX: a software defined internet exchange,” *SIGCOMM Comput. Commun. Rev.* 44, 4, August 2014, 551-562 DOI=http://dx.doi.org/10.1145/2740070.2626300

[47] S. Sedef Savas, M. Tornatore, M. Farhan Habib, P. Chowdhury, and B. Mukherjee, “Disaster-Resilient Control Plane Design and Mapping in Software-Defined Networks” 16th International Conference on High Performance Switching and Routing (HPSR 2015), July 2015.

[48] P. Smith, A. Schaeffer-Filho, D. Hutchison, and A. Mauthe, “Management patterns: SDN-enabled network resilience management,” *IEEE Network Operations and Management Symposium (NOMS)*, Krakow, 2014, pp. 1-9.