ORIGINAL ARTICLE

Journal Section

Resilience of Communication Networks to Random Failures and Disasters: An Optimization Perspective

Jacek Rak[1 2] | Poul E. Heegaard[3] | Bjarne E. Helvik[3]

[1]Dept. of Computer Communications, Gdansk University of Technology, G. Narutowicza 11/12, Gdansk, 80-233, Poland

[2]The State University of Applied Sciences in Elbląg, Wojska Polskiego 1, Elbląg, 82-300, Poland

[3]Department of Information Security and Communication Technology, NTNU – Norwegian University of Science and Technology, Trondheim, NO-7491, Norway

Correspondence
Jacek Rak[1]
Email: jrak@pg.edu.pl

Funding information
This research is partially 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).

Communication networks are subject to many challenges leading to single or multiple failures of its elements. Example failure scenarios include unintentional failures due to scheduled maintenance activities or massive failures caused by disaster-induced events. Therefore, it is crucial to enhance the networks with redundancy and resilience mechanisms able to maintain the availability of network services after a failure. As these problems are often inherently hard to solve to optimality, the role of time-efficient approximation schemes is essential.

In this paper, we highlight the selected problems of communication networks resilience addressed in this issue of *Networks*.

KEYWORDS
communication networks, optimization, availability, resilience, failures, random failures, disasters

1 | INTRODUCTION

Communication networks are an essential part of our life, providing access to information, services, as well as offering communication possibilities. A multitude of personal and business applications are characterized by stringent needs related to the quality of service (QoS) attributes including capacity, latency, transfer delay variation (jitter), and packet losses [9]. It is a societal necessity that the communication networks providing these services are almost always available (see e.g., [8]), also after disastrous events when traffic demand volume frequently grows substantially as a result of remarkably increased activity of end-users in the network.

In particular, as mentioned in [3], 20% of all failures of network nodes/links are due to maintenance activities following from the scheduled tasks as well as implied by design faults and configuration mistakes. Concerning the other 80% of failure events:

- around 70% of them denote unintentional failures of single links occurring at random locations (e.g., due to dig-ups by third parties) [4],
- the remaining 30% of cases affect more than one link [6], and thus also refer to disaster-induced massive failures, i.e., simultaneous failures of multiple elements at a time due to disaster events. As presented in [10], disaster-induced massive failures can be triggered by:
  - natural disasters, e.g., earthquakes, floods, fires, hurricanes, tornadoes or volcanic eruptions,
  - weather disruptions caused by heavy rain/snow or fog affecting, e.g., high-frequency wireless (radio/optical) communications,
  - technology-related disasters following from, e.g., software/hardware failures or faults of power supply systems,
  - malicious human activities (attacks) affecting the performance of the network either directly (via, e.g., distributed denial of service – DDoS, electromagnetic pulse attack – EMP) or indirectly (see for instance failures of network nodes/links due to their location in the area of use of weapons).

It is worth noting that the impact of failures is dependent on their causes. In particular, concerning failures due to scheduled maintenance activities, unintentional failures of nodes/links, or technology-related massive disruptions, locations of the failed network elements are often distributed across the network, as shown in Fig. 1a. They thus do not depend either on characteristics of network elements or on vulnerabilities characteristic of a given geographical area. However, in the case of massive failures, e.g., due to natural disasters, or adverse weather conditions, affected network elements are commonly located in specific areas called failure regions [5] (see Fig. 1b). For malicious attacks, in turn, we can see a dependency of the attack on the importance of a given network element rather than on its geographical location (Fig. 1c). Therefore, when trying to assure the required QoS level in a post-failure period, the applied strategies should properly match specific characteristics of failures.

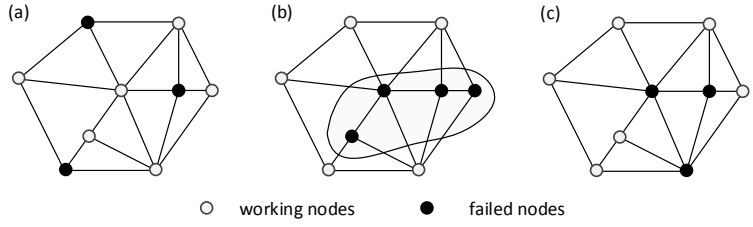

FIGURE 1 Examples of a representative set of failure scenarios.

2 | THE NEED FOR RESILIENCE

Resilience is defined in [11] 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. It can be achieved using either proactive or reactive set up of

the alternate communication paths, such as, e.g., backup paths being disjoint with the affected working paths [9]. As resilience commonly involves redundancy, other ways to improve the performance of communication networks after failures require careful planning of the network architecture itself with a particular focus on the increased connectivity (for instance by the addition of network links) [7] or replication of servers/data centres [1]. Also, the respective measures of network resilience [2] can help evaluate the resilience of given network architecture. They can also be used in computations of communication paths with improved resistance to failures (e.g., measures for link vulnerability serving as metrics of link costs).

However, the related optimization problems are often NP-hard, as they involve the respective subproblems known to be NP-hard (see, e.g., schemes of resilient path computation such as Suurballe's algorithm [12]). Therefore, the use of suboptimal methods is often necessary to obtain the solutions in an acceptable time.

The objective of this issue of *Networks* is to present relevant optimization schemes and verification of their properties for selected network resilience problems. A particular focus of this issue is on the current problem of disaster-resilience of communication networks addressed by four papers in the context of detection of regions in communication networks vulnerable to disasters, design of attack-resilient network architectures, geo-diverse routing, and protection of the content delivery network (CDN) against link-cut attacks. The other three papers focus on the resilience of networks to dual failures, protection of traffic in networks with variable link capacity, and robust virtual network function provisioning under random failures.

In particular, the paper by Vass et al. entitled "The Earth is Nearly Flat: Precise and Approximate Algorithms for Detecting Vulnerable Regions of Networks in the Plane and on the Sphere" focuses on the identification of vulnerable regions and the related shared risk link groups (SRLGs) in the context of disaster-induced failures. The majority of the state-of-the-art works refer to a simplified scenario of networks embedded on a Euclidean plane, which causes distortion. To solve this problem, the authors provide useful generalizations of SRLG algorithms on the plane to the sphere.

In "Design/Upgrade of a Transparent Optical Network Topology Resilient to the Simultaneous Failure of its Critical Nodes", Barbosa et al. focus on techniques for the design of transparent optical networks with enhanced resilience to simultaneous failures of multiple critical nodes. In particular, two problems are considered, namely the design problem and the upgrade problem. The first one is to identify the set of links connecting a given set of nodes. The latter one is, in turn, to determine the set of additional links to be added to maximize for a given budget the resilience of the network to simultaneous failures of its critical nodes.

Girão-Silva et al. investigate the problem of 1+1 protection considering maximally SRLG-disjoint geo-diverse paths to provide the resilience of optical networks to disaster-based region failures in "Shared Risk Link Group Disjointness and Geodiverse Routing: A Trade-Off Between Benefit and Practical Effort". A particular focus is on the estimation of the increase in path lengths and the cost of needed transponders when providing the disaster-resilience.

Natalino et al. address protection of the content delivery network (CDN) against link cut attacks in "Content Placement in 5G-enabled Edge/Core Data Center Networks Resilient to Link Cut Attacks". In particular, the paper introduces a methodology based on integer linear programming for finding Pareto-optimal solutions characterized by the minimal distance between the user and the content as well as by the maximized robustness to targeted link cuts.

Protection of transmission in communication networks against dual failures, i.e., simultaneous failures of two network elements, is considered by Castillo et al. in "Dual-Failure Restorability Analysis of Span-Restorable Meta-Mesh Networks". Two integer linear programming models are proposed with the objectives to minimize the total cost of the network able to survive all dual failures, and to maximize the dual-failure restorability by minimizing the total number of non-restored flows, respectively.

The paper "A Robust Optimization Model for Affine/Quadratic Flow Thinning: A Traffic Protection Mechanism

for Networks with Variable Link Capacity" by Kalesnikau et al. focuses on the protection of traffic in networks with variable link capacities (e.g., wireless networks) by applying the flow thinning mechanism. Under flow thinning, unicast traffic demands are served by dedicated logical tunnels which are subject to thinning according to fluctuations of the available capacities of links. The authors present the appropriate cutting-plane and path-generation algorithms to solve the real-life network dimensioning problems and assess the efficiency of the proposed schemes with other protection methods.

The last paper by Lin and Zhou on "Robust Network Function Virtualization" considers the robust virtual network function (VNF) provisioning problem with the minimal number of VNF instances deployed to maximize the introduced minimum network function reliability. The respective ILP-based schemes are introduced and followed by approximation algorithms.

We do hope that this issue of *Networks* will be found by the readers inspiring and answering essential questions related to optimization problems in the design of resilient communication networks. We would like to express our gratitude to Prof. Bruce Golden and Prof. Douglas Shier, Editors-in-Chief of *Networks*, for their support in the preparation of this issue.

References

[1] O. Ayoub, F. Musumeci, M. Tornatore, and A. Pattavina, *Efficient routing and bandwidth assignment for inter-data-centre live virtual-machine migrations*, IEEE/OSA J. Optical Commun. Networking **9** (2010), B12–B21.

[2] L. da F. Costa, F. Rodrigues, G. Travieso, and P. Boas, *Characterization of complex networks: A survey of measurements*, Advances Phys. **56** (2007), 167–242.

[3] C. Diot, G. Iannaccone, A. Markopoulou, C.N. Chuah, and S. Bhattacharyya, *Service availability in ip networks*, Sprint atl research report RR03-ATL-071888, Sprint ATL, 2003.

[4] T. Fujimura and H. Miwa, *Critical links detection to maintain small diameter against link failures*, Proc. 2010 International Conference on Intelligent Networking and Collaborative Systems – INCOS'10, 2010, pp. 339–343.

[5] M. Habib, M. Tornatore, M. De Leenheer, F. Dikbiyik, and B. Mukherjee, *Design of disaster resilient optical datacenter networks*, IEEE/OSA J. Lightwave Technology **30** (2012), 2563–2573.

[6] S. Kini, S. Ramasubramanian, A. Kvalbein, and A. Hansen, *Fast recovery from dual link or single-node failures in IP networks using tunneling*, IEEE/ACM Trans. Networking **18** (2010), 1988–1999.

[7] C. Natalino, A. Yayimli, L. Wosinska, and M. Furdek, *Link addition framework for optical CDNs robust to targeted link cut attacks*, Proc. Int. Workshop on Resilient Networks Design and Modeling – RNDM'17, IEEE, 2017, pp. 1–7.

[8] National Emergency Number Association (NENA) – Interconnection Security Committee – NG9-1-1 Architecture Subcommittee – Emergency Services IP Network Design Working Group., Emergency services ip network design (esind) information document. Accessed on March 9, 2020.

[9] J. Rak, *Resilent Routing in Communication Networks*, Springer, 2015.

[10] J. Rak, D. Hutchison, E. Calle, T. Gomes, M. Gunkel, P. Smith, J. Tapolcai, S. Verbrugge, and L. Wosinska, *RECODIS: Resilient communication services protecting end-user applications from disaster-based failures*, Proc. International Conf. on Transparent Optical Networks – ICTON'16, IEEE, 2016, pp. 1–4.

[11] J. Sterbenz, D. Hutchison, E. Cetinkaya, A. Jabbar, J. Rohrer, M. Schoeller, and P. Smith, *Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines*, Comput. Networks **54** (2010), 1245–1265.

[12] J. Suurballe and R. Tarjan, *A quick method for finding shortest pairs of disjoint paths*, Networks **14** (2010), 325–336.