RECODIS: Resilient Communication Services Protecting End-user Applications from Disaster-based Failures

Jacek Rak[1], David Hutchison[2], Eusebi Calle[3], Teresa Gomes[4], Matthias Gunkel[5], Paul Smith[6], Janos Tapolcai[7], Sofie Verbrugge[8], Lena Wosinska[9]

[1]Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics, PL
[2]Lancaster University, School of Computing and Communications, UK
[3]University of Girona, ES
[4] Department of Electrical and Computer Engineering, University of Coimbra / INESC Coimbra, PT
[5]Deutsche Telekom Technik, Fixed Mobile Engineering Deutschland, Optical Packet Transport, Darmstadt, DE
[6]AIT Austrian Institute of Technology GmbH, AT
[7]Budapest University of Technology and Economics, Dept. of Telecommunication and Media Informatics, HU
[8]Ghent University – iMinds, Internet-based Communications Networks and Services research group (IBCN), BE
[9]KTH Royal Institute of Technology, School of Information and Communication Technology, SE

e-mail: [1]jrak@pg.gda.pl, [2]d.hutchison@lancaster.ac.uk, [3]eusebi@silver.udg.edu, [4]teresa@deec.uc.pt,
[5]GunkelM@telekom.de, [6]paul.smith@ait.ac.at, [7]tapolcai@tmit.bme.hu
[8]sofie.verbrugge@intec.UGent.be, [9]wosinska@kth.se

ABSTRACT

Disaster-based failures can seriously disrupt any communication network, making its services unavailable. Such disruptions may be caused by natural disasters, technology-related failures, or malicious attacks, and they are observably increasing in number, intensity and scale. When network services that are a part of critical infrastructure become unavailable, commercial and/or societal problems are inevitable. The issue of limiting the impact of disaster-based failures needs to be urgently addressed due to the lack of suitable mechanisms deployed in the current networks.

The COST CA15127 (RECODIS) Action will fill this gap by developing appropriate solutions to provide cost-efficient resilient communications in the presence of disaster-based disruptions considering both existing and emerging communication network architectures. It will be driven by researchers from academia and industry in strong cooperation with governmental bodies.

In this paper, we highlight the objectives of RECODIS, its structure, as well as planned outcomes.

Keywords: end-to-end resilience, disaster-based disruptions

1. INTRODUCTION

Failures of nodes / links in communication networks occur due to a variety of reasons. Apart from being a consequence of single, random failures (e.g., unintentional fibre cuts), node and link failures are more and more a result of *disaster-based massive failures* [1], [2] caused by:

- *natural disasters* including floods, tornadoes, earthquakes, or fires,
- *technology-related disasters* referring to technological issues (e.g., power blackouts),
- *malicious attacks* – intentional human activities aimed to cause severe losses at minimum cost (often resulting in failures of nodes / links serving most of the traffic).

Disaster-based failures have been identified to be far more dynamic and broader in scope than “classical” random failures. They frequently result in the so-called *region failures* denoting simultaneous failures of network elements located in specific geographical areas [3]-[5].

Tens of hurricanes worldwide, also including Europe, have been responsible for power outages implying failures of network nodes on a massive scale for a long time (for about 10 days, on average [2]). Other natural disruptions, such as heavy rain falls, can bring about correlated failures e.g., of high capacity links in Wireless Mesh Networks. Another notable example – the 2014 flooding in Zagreb, Croatia caused a several-hour failure of the entire flight control system in the country (i.e. a disaster-induced breakdown of the critical communication infrastructure) due to power outages (an example of a cascading failure).

Earthquakes and volcano eruptions are the reasons for even greater destructions of communication networks equipment due to long times of manual repair actions. For instance, the 2006 7.1-magnitude earthquake in Taiwan destroyed seven submarine cables disrupting the Internet connectivity between Asia and North America for weeks. The 2011 Greatest Japan Earthquake of 9.0 magnitude impacted about 1500 telecom switching offices due to power outages [1] and damages of undersea cables. In Europe, the 2011 earthquake in the City of Patras, Greece, resulted in the collapse of telecommunication networks.

Fires, resulting e.g., in millions of acres of the EU land being burnt to ashes every year in Greece, Spain, Italy, France, or Portugal, are in turn reported to be frequent reasons for failures of communication infrastructure in Southern Europe. Climatologists confirm that due to global warming, the frequency of weather based disasters occurrence is predicted to increase.

Another important reason for disruptions on a massive scale is related to intentional human activities, referred to as attacks (e.g., bombing or use of weapons of mass destruction attacks, electromagnetic pulse attacks) being actions aimed to cause failures of important equipment (e.g., nodes switching / storing large amount of data; high capacity links). In particular, electromagnetic pulse (EMP) attack (an intense energy field) can immediately result in overloading or disrupting multiple electrical circuits at a large distance (thus affecting electronic components in a large geographic area [6]). Similar to natural disasters, the frequency of attacks (forming a serious threat for any network operator to fulfil the Quality of Service requirements) is predicted to increase.

In this paper, we describe the ideas behind the newly approved COST CA15127 – RECODIS Action ("Resilient Communication Services Protecting End-user Applications from Disaster-based Failures") [7] together with its structure and objectives. In particular, the need to introduce a set of techniques and services providing end-user applications with resilient connectivity even under disaster-based failures (the main aim of RECODIS) is evident due to:

a) increasing threat of disaster-based failures of any kind,

b) lack of built-in mechanisms to assure availability of network services in the presence of disaster-based failures with respect to existing communication networks,

c) severe impact of disaster-based failures on performance of communication networks (nowadays expected to be "always available") that form an important part of the critical infrastructure of everyday life,

d) emerging communication architectures, in particular related to the Future Internet (FI) [8], wireless networking, as well as new networking concepts (including e.g., content-oriented networking [9], cloud computing [10], Software Defined Networking (SDN) [11], or machine-to-machine (M2M) interaction [3]). None of these new technologies has been designed with resilience in mind.

The Action is thus well justified due to lack of appropriate mechanisms deployed in practice within Europe. RECODIS is intended to fill this gap by offering the respective solutions to provide resilient communications for disaster scenarios in existing communication networks (e.g., IPv4/IPv6-based, current Internet), and emerging architectures of the global communications infrastructure (viz., the Future Internet). Apart from development of the respective mechanisms of, e.g., resilient routing, the purpose of this Action is also to prepare the respective recommendations for network operators (following from topological characteristics of networks) on how to design / update the networks to improve their resistance to disaster-based failures.

Therefore, the Action is to address research problems strategically important for Europe being not only of a scientific and technological nature, but at the same time also related to important socio-economic issues, since practically in any disaster-based scenario, availability of communication and emergency services is critical for people in need for the fast information exchange.

2. PROGRESS BEYOND THE STATE OF THE ART

The progress beyond the state-of-the-art and the Action aims to be achieved include:

a) measures to evaluate vulnerability of communication networks to disaster-based disruptions (with the main focus on developing simple and fast algorithms for network characteristics evaluation). Measures available in the literature have been proposed with many remarkable restrictions (e.g., in terms of the shape of the failure regions – commonly assumed to be circular). Available proposals thus commonly refer to rather artificial scenarios with little probability of occurrence in the real life. Innovative aspect of RECODIS will be in new network vulnerability measures tailored to characteristics of real disruptions and worked out in cooperation with Action industrial stakeholders (to get the most benefit from their practical experience),

b) rules and techniques to update the topological characteristics of existing network architectures for network operators (e.g., by techniques for the "controlled" network growth) to make them less vulnerable to disaster-based failures. Based on recent discussions with network operators, network growth (i.e. adding new nodes / links in time) is inevitable for every network. However, network operators are not fully aware of the risks the uncontrolled growth of a network topology may bring in terms of network vulnerability to disaster-based disruptions (in particular to malicious attacks). Also, there is not much knowledge among operators on changes that should be applied to the topology of a network to improve its resistance to disruptions,

c) algorithms for resilient routing together with metrics for establishing resistant-to-disaster communication paths. Special attention is also put on development of methods for fast localization of the disaster-based failures. There are almost no solutions related to disaster-resistant routing currently applied in practice,

d) mechanisms to utilize predictions on disaster-based threats (e.g., following from radar rain maps – as for Wireless Mesh Networks) to achieve proactive preparedness of the network to incoming disruptions. Routing algorithms, and networks themselves can be automatically prepared in advance to incoming disruptions (based e.g. on predictions referring to heavy rain falls, or symptoms of earthquakes). By using such information, routing paths could be updated to prevent from disruptions.

e) techniques of resilient routing for emerging network architectures and networking schemes to achieve disaster-resistant global communications infrastructure, including resiliency in particular related to:
   - Elastic Optical Networks (EONs) [2] being a promising solution of future optical transport (core) networks improving spectral efficiency and line rate elasticity, compared to the existing optical architectures based on fixed-grid Dense Wavelength Division Multiplexing,
   - Wireless Mesh Networks (WMNs) [3] formed by stationary nodes and high-capacity wireless links using directional antennas, but experiencing problems related e.g., to weather-based threats,
   - Future Internet schemes built around content with end-users serving as sources of the content, since primary utilization of the current Internet gradually evolves into data/content distribution,
   - Software Defined Networking with network control being decoupled from forwarding and directly programmable,
   - cloud computing / communications being an efficient solution to provide the global-scale resource and computation capabilities by placing data centres and computation units into the cloud to form a "computing utility" available over the Internet,
   - energy efficiency issues following from increased use of energy resources due to utilization of alternate paths in failure scenarios [12].

f) proposals of concepts for the spare equipment placing on a continental scale in order to be able to deliver this equipment to the disaster-affected region in relatively short term (i.e. one or two days).

3. ACTION WORKING GROUPS AND THEIR OBJECTIVES

RECODIS is structured into five following Working Groups (WGs):

WG1: ***Large-scale natural disasters*** with the objective to provide methodology to improve the resilience of networks to the negative effects of natural disasters resulting in multiple correlated failures (with special focus on earthquakes, volcano eruptions, hurricanes, tornadoes, floods, fires, or electromagnetic storms) occurring relatively rarely but covering large areas and causing non-temporary significant negative effects such as collapse of buildings with network nodes located inside them). Outcomes of WG1 will be of particular importance for the core (international / national) communications infrastructure (e.g. those based on optical communications).

WG2: ***Weather-based disruptions*** focusing on the end-to-end transmission continuity solutions in the presence of those weather-based disruptions that lead to temporary (but frequent) degradation of network performance characteristics (with special focus on negative effects of heavy rain fall, fog, etc.), resulting e.g., in remarkable reduction of available capacity of wireless links due to signal attenuation e.g., in the presence of heavy rain. Time periods of a negative factor influence to be considered by WG2 are thus typically shorter than those to be investigated by WG1. However, even such short time periods of disruptions (measured in terms of minutes / hours) are often critical due to their high frequency of occurrence. Problems considered by WG2 are mostly related to access networks (local and metropolitan), which form an important part of the global communications infrastructure.

WG3: ***Technology-related disasters*** having a direct impact on communication networks performance degradation after failures of network nodes and links with duration measured in terms of hours or even days (e.g., as a direct consequence of power blackouts). Solutions to be proposed by WG3 also include techniques for utilization of alternate communication technologies, as well as ability to use alternate power supplies to mitigate the occurrence of such cascading failures.

WG4: ***Malicious human activities*** with the aim to provide the appropriate means to protect the networks against malicious human activities (e.g., cyber and physical attacks) that lead to the failure (usually multiple and correlated) of important network elements (for instance high-capacity links, nodes of high processing capability, or being important forwarders of the content due to their localization in the network topology). Therefore, one of the objectives of WG4 will be thus to provide, e.g., new routing algorithms and link cost metrics (with the objective to decrease the vulnerability of important flows to attack-based disruptions), as well as methodologies of network topology update to decrease the topological vulnerability of networks to attacks.

WG5: ***Oversight across WGs*** with the objective to identify possible intersecting and overlapping activities (with respect to WG1-WG4), and to provide general principles, challenges, definitions, as well as architecture and mechanisms of disaster-resistant communication systems [13].

4. ACKNOWLEDGEMENTS

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).

cost
EUROPEAN COOPERATION IN SCIENCE AND TECHNOLOGY

RECODIS
Resilient communication services
protecting end-user applications
from disaster-based failures

REFERENCES

[1] F. Dikbiyik, M. Tornatore, B. Mukherjee: Minimizing the risk from disaster failures in optical backbone networks, IEEE/OSA Journal of Lightwave Technology, vol. 32, no. 18, pp. 3175-3183, 2014.

[2] R. Goścień, K. Walkowiak, M. Klinkowski, J. Rak: Protection in Elastic Optical Networks. IEEE Network. vol. 29, no. 6, pp. 88-96 (2015)

[3] J. Rak: *Resilient routing in communication networks*, Springer (2015)

[4] M. Farhan Habib, M. Tornatore, F. Dikbiyik, B. Mukherjee, Disaster survivability in optical communication networks, Computer Communications, vol. 36, no. 6, 630-644 (2013)

[5] X. Long, D. Tipper, T. Gomes: Measuring the survivability of networks to geographic correlated failures. Optical Switching and Networking, vol. 14, no. 2, pp. 117-133 (2014)

[6] J.S. Foster *et al.*: Report of the commission to assess the threat to the United States from electromagnetic pulse (EMP) attack, vol. I: Executive report (Apr. 2008)

[7] Webpage of COST CA15127 - RECODIS: *http://www.cost-recodis.eu*

[8] J. Pan, S. Paul, R. Jain: A survey of the research on future Internet architectures. IEEE Communications Magazine, vol. 49, no. 7, pp. 26-36 (2011)

[9] G. Xylomenos, C.N. Ververidis, V.A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K.V. Katsaros, G.C. Polyzos: A survey of Information-Centric Networking research. IEEE Communications Surveys & Tutorials, vol. 16, no. 2, pp. 1024-1049 (2014)

[10] M. Fouquet, H. Niedermayer, G. Carle: Cloud computing for the masses, Proc. 1st ACM workshop on User-provided networking: challenges and opportunities, pp. 31-36, ACM (2009)

[11] D. Kreutz, F.M.V. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky, S. Uhlig: Software-Defined Networking: a comprehensive survey. IEEE Network, vol. 103, no. 1, pp. 14-76 (2015)

[12] Y. Ye, F. Jiménez Arribas, J. Elmirghani, F. Idzikowski, J. López Vizcaíno, P. Monti, F. Musumeci, A. Pattavina, W. Van Heddeghem: Energy-efficient resilient optical networks: challenges and trade-offs. IEEE Communications Magazine, vol. 53, no. 2, pp. 144-150 (2015)

[13] J.P.G. Sterbenz, D. Hutchison, E.K. Çetinkaya, A. Jabbar, J.P. Rohrer, M. Schöller, P. Smith: Resilience and survivability in communication networks: strategies, principles, and survey of disciplines. Computer Networks, Elsevier, vol. 54, no. 8, pp.1245-1265 (2010)