A Quantitative Resilience Framework for Interdependent Networks

D. Hutchison, *Lancaster University, U.K.*
P. Smith, *AIT, Austria*
P. Van Mieghem, *Delft University of Technology, the Netherlands*
R.E. Kooij, *Delft University of Technology, the Netherlands*
Giorgio Ventre*, University of Napoli Federico II, Italy*

Summary

Resilience evidently cuts through several thematic areas, such as information and network security, fault-tolerance, dependability, and network survivability. Significant research efforts have been devoted to these themes, typically by confining to specific mechanisms for resilience and to subsets of the challenge space. We refer to Sterbenz et al [1] for a discussion on the relation of various resilience disciplines, and to a survey on network resilience by Cholda et al [2]. A shortcoming of existing research and deployed systems is the lack of a systematic view on resilience, to engineer networks that are resilient to challenges that transcend those considered by a single thematic area. A non-systematic resilience approach that does not cover thematic areas, leads to an impoverished view on resilience objectives, potentially resulting in ill-suited solutions. Additionally, a patchwork of resilience mechanisms, incoherently devised and deployed, can result in undesirable behaviour and an increased management complexity, encumbering the overall network management task [3]. Smith et al [4] argue for resilience as a critical and integral property of networks. They adopted a systematic approach to resilience, which takes into account the wide-variety of challenges that may occur. The core of this approach consists of a coherent resilience framework, which includes implementation guidelines, processes, and toolsets to underpin the design of resilience mechanisms at various levels in the network. Central to the framework is a control loop, which defines necessary conceptual components to ensure network resilience. The other elements – a risk assessment process, metrics definitions, policy-based network management, and information sensing mechanisms – emerge from the control loop as necessary elements to realise this systematic approach.

Although the framework from [4] is very useful to deal with resilience engineering of networks operating in isolation, in the last few years an increasing awareness penetrates the research community that the critical infrastructures of a nation are closely coupled: the proper functioning of one infrastructure depends heavily on the proper functioning of another [5]. A case in point is the interdependency between the electric power grid and the communication network. The aim of our paper is to sketch how the resilience framework proposed in [4] can be extended to interdependent networks. Besides robustness envelopes [8] and coupling strengths between interdependent networks, an important part of this extended framework will be to incorporate a generic resilience metric, referred to as the R-value in [6], which is a linear combination of several graph metrics that quantify resilience in networks, such as average shortest path length, diameter and assortativity, but also more advanced metrics such as algebraic connectivity or spectral radius. Recently, the R-value concept has been extended, see [7], in order to solve two open issues, namely how to dimension several metrics to allow their summation and how to weight each of the metrics.

The (enhanced) R-value will be used to define a number of resilience classes. A resilience class specifies, for a certain service, a subinterval of [0, 1] since $R \in [0, 1]$. For example, class C1 contains all graphs whose R-values lie between [0, r1], class C2 contains all graphs in [r1, r2], and so on. The rationale behind resilience classes is that a small number of classes is more manageable than a

continuous range of R, and they ease interpretations by mapping the R-values to a few ranges such as red, orange, green with their usual meaning.

[1] J.P.G. Sterbenz, D. Hutchison, E.K. Çetinkaya, Abdul Jabbar. J.P. Rohrer. M. Schöller, P. Smith, "Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines," Elsevier Computer Networks, Special Issue on Resilient and Survivable Networks, vol. 54, no. 8, June 2010, pp. 1243–42.
[2] P. Cholda, A. Mykkeltveit, B.E. Helvik, O. Wittner, "A Survey of Resilience Differentiation Frameworks in Communication Networks," IEEE Communications Surveys & Tutorials, vol. 9, no. 4, 2007, pp. 32–55.
[3] ENISA Virtual Working Group on Network Providers' Resilience Measures, "Network Resilience and Security: Challenges and Measures," tech. rep. v1.0, Dec. 2009.
[4] P. Smith, D. Hutchison, J.P.G. Sterbenz, M. Schöller, A. Fessi, M. Karaliopoulos, C. Lac, B. Plattner, "Network Resilience: A Systematic Approach", Communications Magazine, IEEE, Volume 49, Issue 7, pp. 88-97, July 2011.
[5] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, S. Havlin, "Catastrophic cascade of failures in interdependent networks," Nature, vol. 464, no. 7291, pp. 1025–1028, 2010.
[6] P. Van Mieghem, C. Doerr, H. Wang, J. Martin Hernandez, D. Hutchison, M. Karaliopoulos, R. E. Kooij, "A Framework for Computing Topological Network Robustness", Delft University of Technology, report 20101218, 2010.
[7] M. Manzano, F. Sahneh, C. Scoglio, E. Calle, J. L. Marzo, "Robustness surfaces of complex networks", Nature Scientific Reports, Volume, 4, Article number: 6133, doi:10.1038/srep06133, 2014.
[8] S. Trajanovski, J. Martin-Hernandez, W. Winterbach and P. Van Mieghem, "Robustness Envelopes of Networks", Journal of Complex Networks, Vol. 1, pp. 44-62, 2013.

Relevance to "Managing resilience, learning to be adaptable and proactive in an unpredictable world"

A variety of networks, such as transportation, traffic, communication and energy networks, form the backbone of our modern society. Such networks are vulnerable to a wide range of challenges, such as random failures of their elements, malicious attacks, human mistakes (e.g. misconfigurations) and large-scale natural disasters. These challenges threaten the normal operation. Resilience, the ability of a network to defend against and maintain an acceptable level of service in the presence of such challenges, is viewed today, more than ever before, as a major requirement and design objective. Given the dependence of our society on interdependent network infrastructures, we take the position that resilience should be an integral property of current and future interdependent networks. In this paper we suggest a systematic approach to resilience for interdependent networks. The control loop, which is at the core of our systematic approach, allows for adaptability and proactivity, two properties that are needed in order to deal with the high amount of uncertainty our network infrastructures are facing today.

Significance/takeaway: How does the proposal advance our ability to create and sustain resilience?

Our resilience framework for interdependent networks builds on work by Sterbenz et al [1], whereby a number of resilience principles are defined, including a resilience strategy, called D^2R^2 + DR: Defend, Detect, Remediate, Recover, and Diagnose and Refine. The strategy describes a real-time control loop to allow dynamic adaptation of the coupled networks in response to challenges, and a non-real time control loop that aims to improve the design of the coupled networks, which includes

the real-time loop operation, by observing and reflecting on past operational experience. Although we are targeting interdependent network infrastructures, focussing on specific examples such as the electric power grid, we intend to produce results that are generalizable to any critical infrastructure coupled with the (critical) services that it supports. These results will advance know-how in creating resilient systems, where desired levels of resilience can be specified from the start, and subsequently sustained through our resilience management approach.