Infrastructure Network Resilience[i]

Kash Barker[1], Jose E. Ramirez-Marquez[2,3]

[1]School of Industrial and Systems Engineering, University of Oklahoma, USA, [2]Stevens Institute of Technology, Hoboken NJ, USA, [3]Tecnológico de Monterrey, Guadalajara, México

Contact: kashbarker@ou.edu

Keywords: Resilience, Infrastructure networks, Reliability, Vulnerability, Recoverability

Introduction

The US government has increasingly emphasized resilience planning for critical infrastructure. Presidential Policy Directive 21 (White House, 2013) states that critical infrastructure "must be secure and able to withstand and rapidly recover from all hazards," where the combination of 'withstanding' and 'recovering' from disruptions constitutes *resilience*. The resilient operation of critical infrastructures is "essential to the Nation's security, public health and safety, economic vitality, and way of life" (DHS, 2013). DHS planning documents highlight terrorist attacks, natural disasters, and manmade hazards, all of which could exacerbate our aging and vulnerable infrastructure networks, whose general condition was given a grade of D+ (ASCE, 2013).

As *risk* is often viewed as the combination of disruptive scenario, likelihood, and consequence, the study of resilience can be viewed as a special case of risk when 'consequence' is measured in terms of vulnerability to and length of disruption resulting from a disruptive scenario. This is true across many applications, including infrastructure networks. Reducing risk in infrastructure networks, in terms of an ability to withstand a disruptive scenario (reducing vulnerability) and an ability to recover (increasing recoverability), can be achieved as the result of building network resilience. As such, resilience management can be viewed as an important component of risk management depending on how the consequence of a disruptive scenario is defined. And much like the quantification of risk, the quantification of resilience is scenario-specific: a network's resilience is a function of the conditions surrounding the disruption (Haimes, 2009).

Metrics

Resilience has increasingly been seen in the literature, and measures of resilience have seen a recent increase (Hosseini et al., 2016). This paper focuses on a particular paradigm for describing the behavior of a network before, during, and after a disruptive scenario e^j, originally offered by Henry and Ramirez-Marquez (2012) and subsequently refined by Barker et al. (2013), Pant et al. (2014), and Baroud et al. (2014a) and applied with network applications. The network, whose behavior is depicted in Figure 1, operates in state S_0 until a disruption occurs at t_e, and at time t_d the network reaches its maximum disrupted state S_d. Recovery from the disruption commences at time t_s, and

[i] This paper is part of the IRGC Resource Guide on Resilience, available at: https://www.irgc.org/risk-governance/resilience/. Please cite like a book chapter including the following information: IRGC (2016). Resource Guide on Resilience. Lausanne: EPFL International Risk Governance Center. *v29-07-2016*

state S_{f} is attained at time t_{f} and is maintained thereafter. The performance of the network is measured with $\varphi(t)$, which assumes that a larger value of network performance is preferred, therefore a degradation caused by e^j leads to a decrease in $\varphi(t)$. Figure 1 depicts the behavior of $\varphi(t)$ before, during, and after disruption e^j.

Figures 1 and 2 illustrate three dimensions of resilience: reliability, vulnerability, and recoverability. Prior to disruptive scenario e^j, the ability of the network to meet performance expectations is described by its *reliability* (Ebeling, 2010; Modarres et al., 2010). Jonsson et al. (2008) define *vulnerability* as the magnitude of network damage given the occurrence of a particular disruptive scenario, complementary in concept to *robustness* in the “resilience triangle” literature in civil infrastructure (Bruneau et al., 2003). *Recoverability* is related to understanding the ability and speed of networks to recover after a disruptive scenario, similar in concept to *rapidity* in the “resilience triangle” literature in civil infrastructure [Bruneau et al. 2003].

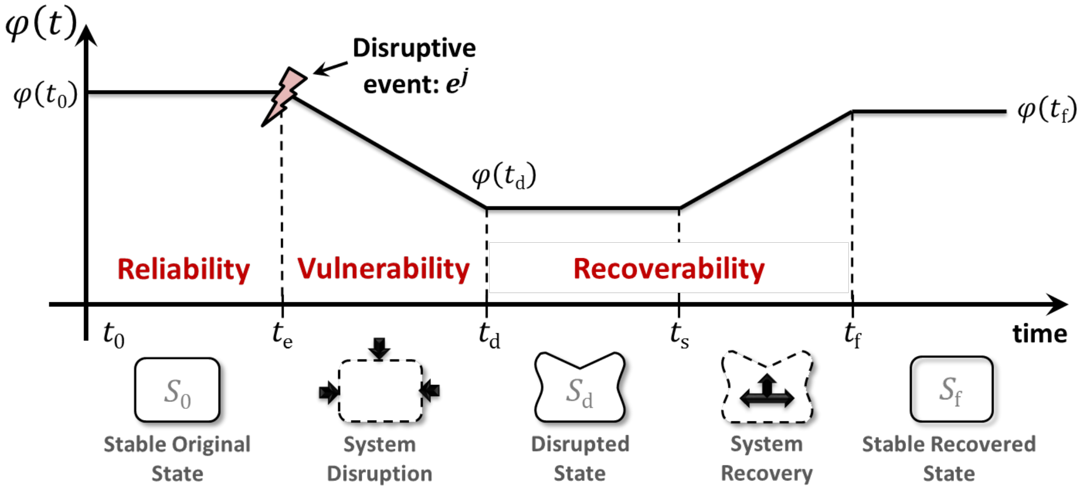

Figure 1. Graphical depiction of decreasing network performance, φ(t), across several state transitions over time.

Resilience is defined here as the time dependent ratio of recovery over loss, or $Я(t) = \mathrm{Recovery}(t)/\mathrm{Loss}(t)$, noting the notation for resilience, *Я* (Whitson & Ramirez-Marquez 2009) as *R* is commonly reserved for *reliability*. Eq. (1) formalizes this measure, where $\varphi(t_0)$ refers to the ‘as-planned’ performance level of the network, t_{d} is the point in time after the disruption where network performance is at its most disrupted level, recovery of the network occurs between times t_{s} and t_{f}, and any quantification of resilience requires the occurrence of disruptive scenario e^j. Eq. (1) is used for networks whose performance is reflected in Figure 1.

$$Я_{\varphi}(t|e^j) = \frac{\varphi(t|e^j) - \varphi(t_{\mathrm{d}}|e^j)}{\varphi(t_0) - \varphi(t_{\mathrm{d}}|e^j)} \tag{1}$$

Hosseini et al. (2016) provide a recent review of several definitions and quantitative measures of resilience, particularly from the perspective of engineering systems and networks. Another common measure is the normalized area below the $\varphi(t)$ curve in Figure 1 (Bruneau et al., 2003; Zobel 2011). This idea was applied particularly to networks by Ganin et al. (2016), who define a network $G(N, L)$ with set of nodes N and links L. In the context of Figure 1, the performance of a network at time t is

$\varphi(t; N, L, C)$, where C is the set of temporal decision rules and strategies to improve network resilience, noting explicitly that resilience is not only a function of the disruptive scenario but also of the actions taken to improve it. Similar to Bruneau et al. (2003), Ganin et al. (2016) measure resilience with Eq. (2), where resilience is measured between time 0 and a control time T_C, E is the set of disruptions (e.g., possible node attacks), and $\varphi^{nominal}$ is the undisrupted network performance level (similar to $\varphi(t_0)$).

$$Я_{\varphi}(E, [0, T_C]) = \frac{\frac{1}{|E|} \sum_E \int_{t=0}^{T_C} \varphi(t; N, L, C)}{\int_{t=0}^{T_C} \varphi^{nominal}(t; N, L, C)} \qquad (2)$$

Network performance, $\varphi(t)$, can be defined in a number of ways. For example, Almoghathawi et al. (2016) describe network performance as the extent to which demand is being met at the demand nodes of a network, an important consideration in electric power or water networks. In transportation network applications (e.g., Jenelius & Mattson (2015)), origin/destination travel times or network flow may appropriately measure network performance. Ganin et al. (2016) propose the proportion of active nodes in a network as a measure of performance. Gao et al. (2016) also use a graph theoretic measure of network performance,

Several related measures can be derived from Eqs. (1) and (2) (Pant et al. 2014), including: (i) time to complete restoration, or the total time spent from the point t_s when recovery activities commence up to the time when all recovery activities are finalized, (ii) time to full network resilience, or the time spent from t_s up to the time when $Я_{\varphi}(t|e^l) = 1$ (note that for network applications, flow can be at its maximum when links are still disrupted, thus the distinction between (i) and (ii)), and (iii) time to α ×100% resilience, or the time spent from t_s up to when $Я_{\varphi}(t|e^l) = \alpha$.

As one might imagine, there is a dependence relationship among the three dimensions of resilience from Figures 1 and 2. Strengthening reliability through network protection and hardening may reduce the impact experienced after e^j, thus investments in reliability may assist in reducing vulnerability. Likewise, a less vulnerable network (or a network that is more capable of withstanding a disruptive scenario) is more easily restored. Thus, an investment in reducing vulnerability can pay dividends in improving recoverability, even though these risk management options are very different from each other. There exists a tradeoff among reliability, vulnerability, and recoverability, where pre-disruption investments may be less expensive than post-disruption investments to achieve and maintain similar levels of network performance before and after a disruptive scenario. And naturally, there exists a likelihood that the scenario occurs (and thus recoverability is necessary).

Annotated bibliography

Bursztein and Goubault-Larreq (2007) proposed a logic-based framework to assess the resilience of computers networks against disruptions such as malicious intruders as well as random faults. Their proposed model uses two-layered presentation of dependencies between files and services and also quick response to the incidents. Sterbenz et al. (2013) described a comprehensive methodology to assess network resilience through a combination of topology generation, simulation, and experimental emulation techniques with the goal of improving the resilience and solvability of the future internet. Trivedi et al. (2009) reviewed the definitions and metrics for network resilience.

Individual dimensions of network resilience (reliability, vulnerability, recoverability) have been well studied. Reliability typically quantifies the likelihood of connectivity of a network (Mandaltsis & Kontoleon, 1987; Jan, 1993; Ramirez-Marquez & Rocco, 2008, 2009).

Numerous works study network vulnerability, noting that vulnerability is highly dependent upon the type and extent of disruption e^j (Crucitti et al., 2005; Zio et al., 2008; Zhang et al., 2011). In particular, Nicholson et al. (2016) propose measures of network vulnerability based on network flow, as opposed to most studies that emphasize topology (Holme et al., 2002; Holmgren, 2006; Wu et al., 2011; Johansson et al., 2011; Johansson et al., 2013).

The work on optimizing recovery typically involves the order and scheduling of links to restore (Gong et al., 2009; Matisziw et al., 2010; Aksu & Ozdamar, 2014; Nurre et al., 2012; Cavdaroglu et al., 2013).

To identify the important components (nodes/links) contributing to the resilience of a network, Barker et al. (2013) offer some resilience-based component importance measures derived from Eqs. (1) and (2). Fang et al. (2016) extend this approach with some new measures.

References

Aksu, D.T. & Ozdamar, L. (2014). A Mathematical Model for Post-disaster Road Restoration: Enabling Accessibility and Evacuation. *Transportation Research Part E: Logistics and Transportation*, 61(1): 56-67.

Almoghathawi, Y., Barker, K., & McLay, L.A. (2016). Resilience-Driven Restoration Model for Interdependent Infrastructure Networks. In submission.

American Society of Civil Engineers (2013). *Report Card for America's Infrastructure 2013*.

Barker, K., Ramirez-Marquez, J.E. & Rocco, C.M. 2013. Resilience-Based Network Component Importance Measures. *Reliability Engineering and System Safety*, 117(1): 89-97.

Baroud, H., J.E. Ramirez-Marquez, J.E., Barker, K. & Rocco, C.M. (2014a). Stochastic Measures of Network Resilience: Applications to Waterway Commodity Flows. *Risk Analysis*, 34(7): 1317-1335.

Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O'Rourke, T.D., Reinhorn, A.M., Shinozuka, M., Tierney, K., Wallace, W.A. & von Winterfeldt, D. (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra*, 19(4): 733-752.

Bursztein, E. & Goubault-Larrecq, G. (2007). A Logical Framework for Evaluating Network Resilience Against Faults and Attacks. Springer-Verlag Berlin Heidelberg I. Cervesato (Ed.): ASIAN 2007, LNCS 4846: 212-227.

Cavdaroglu, B., Hammel, E., Mitchell, J.E., Sharkey, T.C. & Wallace, W.A. (2013). Integrating Restoration and Scheduling Decisions for Disrupted Interdependent Infrastructure Systems. *Annals of Operations Research*, 203(1): 279-294.

Crucitti, P., Latora, V. & Marchiori, M. (2005). Locating Critical Lines in High-Voltage Electric Power Grids. *Fluctuation and Noise Letters*, 5(2): L201-L208.

Department of Homeland Security (2013). *National Infrastructure Protection Plan*. Washington, DC: Office of the Secretary of Homeland Security.

Ebeling, C.E. 2010. *An Introduction to Reliability and Maintainability Engineering*. 2nd edition. Long Grove, IL: Waveland Press, Inc.

Fang, Y.P., Pedroni, N. & Zio, E. (2016). Resilience-Based Component Importance Measures for Critical Infrastructure Network Systems. *IEEE Transactions on Reliability*, 65(2): 502-512.

Ganin, A.A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J.M., Kott, A., Mangoubi, R. & Linkov, I. (2016). Operational Resilience: Concepts, Design and Analysis. *Scientific Reports*, 6: 19540

Gao, J., Barzel, B., & Barabási, A.-L. (2016). Universal Resilience Patterns in Complex Networks. *Nature*, 530: 307-312.

Gong, J., Lee, E.E., Mitchell, J.E. & Wallace, W.A. (2009). Logic-based Multi-objective Optimization for Restoration Planning. Optimization and Logistics Challenges in the Enterprise. W. Chaovalitwongse, K.C. Furman, P.M. Pardalos (eds.). New York: Springer.

Haimes, Y.Y. (2009). On the Definition of Resilience in Systems. *Risk Analysis*, 29(4): 498-501.

Henry, D. & Ramirez-Marquez, J.E. (2012). Generic Metrics and Quantitative Approaches for System Resilience as a Function of Time. *Reliability Engineering and System Safety*, 99: 114-122.

Holme, P., Kim, B.J., Yoon, C.N. & Han, S.K. (2002). Attack Vulnerability of Complex Networks. *Physical Review E*, 65(5): 056109.

Holmgren, A.J. (2006). Using Graph Models to Analyze the Vulnerability of Electric Power Networks. *Risk Analysis*, 26(4): 955-969.

Hosseini, S., Barker, K. & Ramirez-Marquez, J.E. (2016). A Review of Definitions and Measures of System Resilience. *Reliability Engineering and System Safety*, 145: 47-61.

Jan, R.-H. (1993). Design of Reliable Networks. *Computers and Operations Research*, 20(1): 25-34.

Jenelius, E. & Mattsson, L.G. (2015). Road Network Vulnerability Analysis: Conceptualization, Implementation and Application. *Computers, Environment and Urban Systems*, 49: 136-147.

Johansson, J., Hassel, H. & Cedergren, A. (2011). Vulnerability Analysis of Interdependent Critical Infrastructures: Case Study of the Swedish Railway System. *Journal of Critical Infrastructures*, 7(4): 289-316.

Johansson, J., Hassel, H. & Zio, E. (2013). Reliability and Vulnerability Analyses of Critical Infrastructures: Comparing Two Approaches in the Context of Power Systems. *Reliability Engineering and System Safety*, 120: 27-38.

Jonsson, H., Johansson, J. & Johansson, H. (2008). Identifying Critical Components in Technical Infrastructure Networks. *Journal of Risk and Reliability*, 222(2): 235-243.

Mandaltsis, D. & Kontoleon, J.M. (1987). Overall Reliability Determination of Computer Networks with Hierarchical Routing Strategies. *Microelectronic Reliability*, 27(1): 129-143.

Matisziw, T.C., Murray, A.T. & Grubesic, T.H. (2010). Strategic Network Restoration. *Networks and Spatial Economics*, 10(3): 345-361.

Modarres, M., Kaminskiy, M. & Krivtsov, V. (2010). *Reliability Modeling and Risk Analysis: A Practical Guide*. 2nd edition. Boca Raton, FL: CRC Press.

Nicholson, C.D., Barker, K. & Ramirez-Marquez, J.E. (2016). Flow-Based Vulnerability Measures for Network Component Importance: Experimentation with Preparedness Planning. *Reliability Engineering and System Safety*, 145: 62-73.

Nurre, S.G., Cavdaroglu, B., Mitchell, J.E., Sharkey, T.C. & Wallace, W.A. (2012). Restoring Infrastructure Systems: An Integrated Network Design and Scheduling Problem. *European Journal of Operational Research*, 223(3): 794-806.

Pant, R., Barker, K., Ramirez-Marquez, J.E. & Rocco, C.M. (2014). Stochastic Measures of Resilience and their Application to Container Terminals. *Computers and Industrial Engineering*, 70(1): 183-194.

Ramirez-Marquez, J.E. & Rocco, C.M. (2008). All-terminal Network Reliability Optimization via Probabilistic Solution Discovery. *Reliability Engineering and System Safety*, 93(11): 1689-1697.

Ramirez-Marquez, J.E. & Rocco, C.M. (2009). Stochastic Network Interdiction Optimization via Capacitated Network Reliability Modeling and Probabilistic Solution Discovery. *Reliability Engineering and System Safety*, 94(5): 913-921.

Sterbenz, J.P.G., Cetinkaya, E.K., Hameed, M.A., Jabbar, A., Qian, S., & Rohrer, J.P. (2013). Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation. *Telecommunication Systems*, 52: 705-736.

Trivedi, K.S., Seong Kim, D., & Ghosh, R. (2009). Resilience in Computer Systems and Networks. *International Conference on Computer-Aided Design* (ICCAD) 2009, San Jose, CA.

White House (2013). *Presidential Policy Directive 21 -- Critical Infrastructure Security and Resilience*. Office of the Press Secretary: Washington, DC.

Whitson, J.C. & Ramirez-Marquez, J.E. (2009). Resiliency as a Component Importance Measure in Network Reliability. *Reliability Engineering and System Safety*, 94(10): 1685-1693.

Wu, J., Barahona, M., Tan, Y.-J. & Deng, H.Z. (2011). Spectral Measure of Structural Robustness in Complex Networks. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 41(6): 1244-1252.

Zhang, C., Ramirez-Marquez, J.E. & Rocco, C.M. (2011). A New Holistic Method for Reliability Performance Assessment and Critical Components Detection in Complex Networks. *IIE Transactions*, 43(9): 661-675.

Zio, E., Sansavini, G., Maja, R. & Marchionni, G. (2008). An Analytical Approach to the Safety of Road Networks. *International Journal of Reliability, Quality and Safety Engineering*, 15(1): 67-76.

Zobel, C.W. (2011). Representing Perceived Tradeoffs in Defining Disaster Resilience. *Decision Support Systems*, 50(2): 394-403.