

Editorial

Risk and Safety of Complex Network Systems

**Xiao-Bing Hu,¹ Adrian V. Gheorghe,² Mark S. Leeson,³ Supeng Leng,⁴
Julien Bourgeois,⁵ and Xiaobo Qu⁶**

¹*Beijing Normal University, Beijing 100875, China*

²*Old Dominion University, Norfolk, VA, USA*

³*University of Warwick, Coventry CV4 7AL, UK*

⁴*University of Electronic Science and Technology of China, Chengdu 611731, China*

⁵*University of Franche-Comte, FEMTO-ST Institute, UMR CNRS 6174, Montbéliard, France*

⁶*Griffith University, Gold Coast, QLD 4222, Australia*

Correspondence should be addressed to Xiao-Bing Hu; huxiaobing@bnu.edu.cn

Received 30 December 2015; Accepted 30 December 2015

Copyright © 2016 Xiao-Bing Hu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Complex network systems cover most aspects of our daily life and are concerned with a wide range of communities, such as transportation, communication and information, energy systems, disaster and risk reduction and mitigation, finance, social networks and perception, and biological and medical systems, as well as academic researchers on theories of reliability, safety, risk, complexity, and networks [1–4]. Despite their enormous benefits to daily life, complex network systems also exhibit disadvantages, and one of the most challenging issues is the risk and safety of complex network systems. In a network system, the impact of a local hazard/fault/disturbance can easily spread out to the whole system due to domino effect, cascading effect, and/or ripple effect and eventually evolves into a large-scale disaster [5, 6]. The finding of “six degrees of separation” may partially illustrate how efficiently the impact of a local event can spread in a network [7]. The speedup of globalization process nowadays just makes the situation even worse [8].

The past two decades has witnessed too many examples of globally networked catastrophes. For instance, in the 2003 Northeast blackout in USA, a software bug in the alarm system at a control room of the FirstEnergy Corporation, located in Ohio, eventually caused a widespread power outage throughout parts of the Northeastern and Midwestern United States and the Canadian province of Ontario, affecting an estimated 10 million people in Ontario and 45 million people in eight U.S. states [9]. In the 2003 SARS plague, the first case of infection was speculated to be a farmer in Foshan County,

Guangzhou Province, China, then modern social network and advanced transportation system boosted the outbreak in 37 countries having claimed 774 lives worldwide [10]. In the 2008 global financial crisis, the bursting of the U.S. housing bubble ended up with the European sovereign-debt crisis and a global recession [11]. In the 2010 Eyjafjallajökull Volcano eruption in Iceland, despite the relatively small intensity and remote location, 20 countries across Western and Northern Europe closed their airspace to commercial jet traffic and it affected about 10 million travelers [12].

Dealing with the risk and safety of complex network systems has long been a common challenging task of concern to researchers and engineers from a wide range of communities. Although substantial relevant results have been reported in the literature, the means to assess the risk and to improve the safety of complex network systems still remains largely unresolved. For example, a most important finding on the structural robustness of networks reveals that a scale-free topology is more vulnerable to intended attacks to hub nodes (i.e., high-degree nodes), which suggests that such nodes are more important than low-degree nodes [1]. However, recent research indicates that, once a node oscillating function is introduced, low-degree nodes are actually more important than hub nodes, no matter what the intended attacks or random failures [13]. These conflicting results clearly remind us of the fact that we are far away from fairly good understanding of complex network systems. What makes things worse is that a real-world complex network system usually keeps changing

and evolving, and therefore studying the past of the system might not necessarily generate a good/feasible solution for the present, but it could even become a source of risk in future [3]. As is pointed out in a contemporary Nature perspective paper [14], the world is currently faced with a diverse range of globally networked risks at a time when we are ill-equipped to understand or handle them.

Researchers and engineers in various communities are eager to see new progress to address the risk and safety of complex network systems. Besides the nature of hazard/fault/disturbance and the topology of system, many other factors such as heterogeneity in components, interaction functions and rules, amplifying effects, self-healing capability, and multiple feedback loops altogether play a crucial role in determining the system performance against hazard/fault/disturbance. The complexity roots in the combination of all these factors, resulting in nonlinear, dynamical, self-adaptive, and self-organizing system behavior, which is far beyond the capability of the existing methodologies. To study the risk and safety of complex network systems, there is an urgent demand for new interdisciplinary theories, models, methods, and experiments. This particularly needs us to fertilize a new thinking of globally networked risks and complex systems science [8, 14].

This special issue aims to serve as a platform for a wide range of communities to share their specialized knowledge and experiences for dealing with the risk and safety of various complex network systems. By bringing together both relevant theoretical works and case studies, the research community can be a source of inspiration and encouragement to promote and enrich research on the risk and safety of complex network systems. In this way, a little more light will hopefully be shed on the challenging task set-up by the perspective paper [14].

The accepted papers in this special issue cover many important topics on the risk and safety of complex network systems, including both theoretical studies and application-oriented researches.

Regarding mathematical theories of complex networks, F. Ren et al. reported a coupled map lattices based approach to analyze the risk of cascading process and recovering strategy in Watts-Strogatz (WS) small-world network and Barabási and Albert (BA) scale-free network, respectively; J. Liu et al. conducted some theoretical analyses on the threshold for the outbreak of the cascading failures in degree-degree uncorrelated networks, which are useful to improve network robustness given the limited capacity resource; H. Han and R. Yang investigated load-induced cascading failures in asymmetrical interdependent networks, discovering that network robustness is positively related to capacity, but negatively related to load.

In the area of transportation systems and civil engineering, C. Xu et al. developed some artificial neural network models to predict the free flow speed of bicycle traffic and then to analyze the associated crash risk, which are important for the evaluation, planning, and management of bicycle traffic safety; H. Ju and M. Fu focused on the vibration control of structures and conducted a deep investigation on the in-plane vibration response of periodic viaduct on saturated soil under Rayleigh surface wave.

In the area of communication networks and information systems, R. He et al. proposed an efficient top-k query processing scheme with result integrity verification, named as ETQ-RIV, in two-tiered sensor networks, and the proposed scheme exhibits better performance than the relevant existing works in terms of both communication cost and query result redundancy rate; T. A. Nguyen et al. targeted at sensitivity assessment of availability for data center networks (DCNs), which plays a crucial role in design and management of cloud computing based businesses, and they presented a comprehensive availability modeling and sensitivity analysis of a DCell-based DCN with server virtualization for business continuity using stochastic reward nets.

In the area of cyber world security, T. Yang et al., based on the attribute-based encryption (ABE) and the distributed hash table (DHT) technologies, reported a secure ciphertext self-destruction scheme in order to improve the cloud storage security for handling expired data.

In the area of disaster reduction and emergence management, X. Zhai et al. proposed a robust satellite scheduling model to address a sequence of emergency tasks, in which both the benefit and robustness of schedule are simultaneously maximized in each stage; Y. F. Wang et al., based on hybrid causal logic model techniques, developed a quantitative risk analysis framework to assess the risk of offshore fire and explosion.

In the area of biological and medical systems, X. Zhang et al. studied epidemic spreading characteristics and immunity measures based on complex network with contact strength and community structure.

In the area of financial systems, C. Cheng et al. presented a heuristic multikernel growth approach based on constrained Delaunay triangulation in order to address a special zone design problem for economic census investigators; Y. Xiang et al. analyzed the production stability of process routes for complex parts based on weighted network, where a brittleness risk entropy, as an indicator of the vulnerability of nodes in a weighted network, was introduced to predict those easily failed subsystems in the entire network.

Acknowledgments

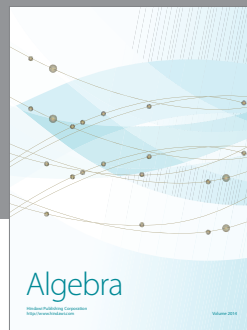
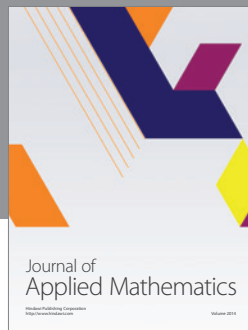
Being the guest editors, we would like to express our gratitude to all the authors who have contributed their work to this special issue.

Xiao-Bing Hu
Adrian V. Gheorghe
Mark S. Leeson
Supeng Leng
Julien Bourgeois
Xiaobo Qu

References

- [1] R. Albert and A.-L. Barabasi, "Statistical mechanics of complex networks," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 47–97, 2002.

- [2] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, "Complex networks: structure and dynamics," *Physics Reports*, vol. 424, no. 4-5, pp. 175–308, 2006.
- [3] A. V. Gheorghe, *System of Systems*, InTech, 2012.
- [4] P. Ball, *Why Society is a Complex Matter*, Springer, Berlin, Germany, 2012.
- [5] X. Q. Huang, I. Vodenska, S. Havlin, and H. E. Stanley, "Cascading failures in bi-partite graphs: model for systemic risk propagation," *Scientific Reports*, vol. 3, article 1219, 2013.
- [6] X.-B. Hu, M. Wang, M. S. Leeson, E. L. Hines, and E. Di Paolo, "Deterministic ripple-spreading model for complex networks," *Physical Review E*, vol. 83, no. 4, Article ID 046123, 2011.
- [7] S. Milgram, "The small-world problem," *Psychology Today*, vol. 1, no. 1, pp. 61–67, 1967.
- [8] OECD, "Future global shocks—improving risk governance," OECD Reviews of Risk Management Policies, OECD, 2011.
- [9] E. J. Lerner, "What's wrong with the electric grid?" *The Industrial Physicist*, vol. 9, no. 5, pp. 8–13, 2003.
- [10] World Health Organization (WHO), Summary of probable SARS cases with onset of illness from 1 November 2002 to 31 July 2003.
- [11] J. Crotty, "Structural causes of the global financial crisis: a critical assessment of the 'new financial architecture,'" *Cambridge Journal of Economics*, vol. 33, no. 4, pp. 563–580, 2009.
- [12] S. M. Wilkinson, S. Dunn, and S. Ma, "The vulnerability of the European air traffic network to spatial hazards," *Natural Hazards*, vol. 60, no. 3, pp. 1027–1036, 2012.
- [13] K. Morino, G. Tanaka, and K. Aihara, "Dynamical robustness in complex networks: the crucial role of low-degree nodes," *Scientific Reports*, vol. 2, article 232, pp. 1–6, 2012.
- [14] D. Helbing, "Globally networked risks and how to respond," *Nature*, vol. 497, no. 7447, pp. 51–59, 2013.



Hindawi

Submit your manuscripts at
<http://www.hindawi.com>

