Chaos, Solitons and Fractals 80 (2015) 125–138

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

journal homepage: www.elsevier.com/locate/chaos

Vulnerability and controllability of networks of networks

Xueming Liu [a,b], Hao Peng [c], Jianxi Gao [d,*]

[a] Key Laboratory of Image Information Processing and Intelligent Control, School of Automation, Huazhong University of Science and Technology, Wuhan 430074, Hubei, PR China
[b] Center for Polymer Studies and Department of Physics, Boston University, Boston, MA 02215, USA
[c] Department of Computer Science and Engineering, Zhejiang Normal University, Jinhua 321004, Zhejiang, PR China
[d] Center for Complex Network Research and Department of Physics, Northeastern University, Boston, MA 02115, USA

ARTICLE INFO

Article history:

Keywords:
Networks of networks
Vulnerability
Controllability
Percolation theory

ABSTRACT

Network science is a highly interdisciplinary field ranging from natural science to engineering technology and it has been applied to model complex systems and used to explain their behaviors. Most previous studies have been focus on isolated networks, but many real-world networks do in fact interact with and depend on other networks via dependency connectivities, forming "networks of networks" (NON). The interdependence between networks has been found to largely increase the vulnerability of interacting systems, when a node in one network fails, it usually causes dependent nodes in other networks to fail, which, in turn, may cause further damage on the first network and result in a cascade of failures with sometimes catastrophic consequences, e.g., electrical blackouts caused by the interdependence of power grids and communication networks. The vulnerability of a NON can be analyzed by percolation theory that can be used to predict the critical threshold where a NON collapses. We review here the analytic framework for analyzing the vulnerability of NON, which yields novel percolation laws for n-interdependent networks and also shows that percolation theory of a single network studied extensively in physics and mathematics in the last 50 years is a specific limited case of the more general case of n interacting networks. Understanding the mechanism behind the cascading failure in NON enables us finding methods to decrease the vulnerability of the natural systems and design of more robust infrastructure systems. By examining the vulnerability of NON under targeted attack and studying the real interdependent systems, we find two methods to decrease the systems vulnerability: (1) protect the high-degree nodes, and (2) increase the degree correlation between networks. Furthermore, the ultimate proof of our understanding of natural and technological systems is reflected in our ability to control them. We also review the recent studies and challenges on the controllability of networks and temporal networks.

1. Introduction

Many real-world complex systems can be modeled as complex networks, and it has attracted the attention of scientists and engineers studying such wide-ranging topics as power grid systems, computer science, biology, and social science [1–21]. Plenty of studies have been carried on the structural and dynamic properties of real-world networks, and most networks are found to show a power-law degree distribution and scale-free (SF), e.g. Internet [22], the WWW [3], social networks [23–28], infrastructure networks [29], biological networks [30,31] etc. Comparing to the classical Erdős-Rényi (ER) networks [32], SF networks are significantly more robust than ER networks to random failures but more vulnerable to targeted attack [3–5,33].

* Corresponding author. Tel.: +16178889526.
E-mail address: jianxi.gao@gmail.com (J. Gao).

http://dx.doi.org/10.1016/j.chaos.2015.08.009
0960-0779/

The vulnerability of a network characterizes its inability to withstand the effects of node or link failures. On the opposite direction, the ability of a network to remain functional after initial attack (called robustness) either can be characterized by the integral size of the giant connected component during a whole attacking period [34,35] or defined by the percolation thresholds [4,36,37]. The percolation threshold, p_c, is the critical fraction of remaining nodes (or links) that leads to the collapse of the network [4,38], which is usually predicted by using percolation theory, a method from statistical physics [38,39]. Moreover, using percolation theory one can address some other issues, such as efficient attacks or immunization [5,8,33,40,41], obtaining optimal path [42] and designing robust networks [34,43]. The study of the vulnerability or the robustness of complex systems can help us understand the real-world and enable us to make the infrastructures we use in everyday life more efficient and more robust.

It is increasingly clear that diverse critical infrastructures are not isolated but coupled together or depend on each other, such as water and food supply, communications, fuel, financial transactions, and power stations [44–50]. Take a coupled system for example, as shown in Fig. 1, the electric power network provides power for pumping and for controlling systems of water network, the water network provides water for cooling and emissions reduction of power network, the fuel network provides fuel for generators for the electric power network and the electric power network provides power to pump oil for fuel network, etc [51,52]. The interdependence between networks can highly increase the vulnerability of the system, since failure of nodes in one network may lead to the failure of dependent nodes in other networks and this may happen recursively and lead to a cascade of failures and system collapse. For example, electrical blackouts that affect large regions are cascading failures caused by the interdependence between two systems: communication network and power grid [49,53].

The interactions between systems have led to an emerging new field in network science that focuses on what are variously called interdependent networks [54–64], interconnected networks [65–67], multi-layered networks [68–72], multiplex networks [73], and in general a network of networks [37,50,74,75], In these systems, networks interact with each other and exhibit structural and dynamical features that differ from those observed in isolated networks. For example, Buldyrev et al. [54] developed an analytical framework based on the generating function formalism [76,77], describing the cascading failures in two interdependent networks, and finding a first order discontinuous phase transition, and this is dramatically different from the second order continuous phase transition found in isolated networks; Parshani et al. [55] studied a model more close to real systems, two partial interdependent networks, finding that the percolation transition changes from a first order to a second order at a certain critical coupling as the coupling strength decreases; Gao et al. developed an analytical framework to study the percolation of a tree-like network formed by n interdependent networks (tree-like NON) [37,78,79], discovering that while for $n = 1$ the percolation transition is a second order, and for any $n > 1$ where cascading failures occur, it is a first order (abrupt) transition. The tree-like NON has some other extensions, such as the multiplex networks [73] considered as n interdependent networks without feedback condition, and the interdependent networks based on epidemic spreading [80]. More recently, Gao et al. [81] developed a general framework to study the percolation of any "network of networks".

The process of cascading failures in network of networks is caused by the initial attack on nodes. Most of the studies above are focused on random initial failure. While in real scenarios, initial failures are mostly not random but due to targeted attack on important hubs (nodes with high degree) or occur to low degree nodes since important hubs are purposely protected [82], which triggers another branch of the studies of networks of networks. Huang et al. [82] proposed a mathematical framework for understanding the robustness of fully interdependent networks under targeted attacks, which was later extended to targeted attacks on partially interdependent networks by Dong et al. [83]. Huang et al. [82] and Dong et al. [83] developed a general technique that uses the random attack solution to map the targeted attack problem in interdependent networks. Furthermore, Dong et al. [74] extended the study of targeted attacks on high degree nodes in a pair of interdependent networks to the study of network of networks, and find that the robustness of networks of networks can be improved by protecting important hubs.

The analytic tools of the robustness of interdependent networks have been applied to various real systems, such as financial systems [84], airline systems [85], brain [86] and social systems [87], which helps us understand the catastrophic failure and crisis in complex systems in real scenarios. The applications to real systems show that the correlations between networks are common in interacting systems, and it decreases the vulnerability of the coupled systems. Parshani et al. [60] proposed an "intersimilarity" measure between the interdependent networks. They studied a system composed of the interdependent world-wide seaport and the world-wide airport networks, and found that as the interdependent networks become more intersimilar the system becomes more robust. The case in which all pairs of interdependent nodes in both networks have the same degree was solved analytically by Buldyrev et al. [88]. The effect of intersimilarity between the coupled networks on percolation was further studied analytically by Cellai et al. [89] and Hu et al. [90]. Very recently, Reis et al. [86] shows that the stability of a system of networks relies on the relation between internal structure of a network and its pattern of connections to other networks. Hu et al. [87] applied the percolation of interdependent networks with in- and out- degree correlations between two networks to coupled social networks, showing that the in- and out degree correlations between networks benefit the robustness of the coupled social systems. Thus, increasing the correlations between different coupled infrastructure systems is another method to increase the robustness of the entire systems and avoid catastrophic failures.

The studies of the vulnerability and other structural and dynamical properties of networks of networks help us understand natural and technological systems, and the ultimate proof of our understanding of them is reflected in our ability to control them [91]. Due to the large-scales and complexities, controlling complex networks still remains a huge