Physica A 523 (2019) 476–487

Contents lists available at ScienceDirect

Physica A

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

Structural and functional robustness of networked critical infrastructure systems under different failure scenarios

Shuliang Wang [a,b], Wenzhuo Lv [a], Longfeng Zhao [c,b,*], Sen Nie [d,b], H. Eugene Stanley [b]

[a] School of Electrical Engineering and Automation, Jiangsu Normal University, Xuzhou, 221116, China
[b] Center for Polymer Studies and Department of Physics, Boston University, Boston, MA 02215, USA
[c] School of Management, Xi'an Polytechnic University, No. 19, Jinhua South Road, Xi'an, Shaanxi 710048, China
[d] School of Electrical &, Automation Engineering, East China Jiaotong University-Nanchang, Jiangxi 330013, China

HIGHLIGHTS

- The structural and functional robustness are analyzed.
- The critical areas most likely to be attack targets are identified.
- The fraction of the system after a series of failures occur are determined.
- Overload failures are examined to determine how they propagate.

ARTICLE INFO

Article history:
Received 6 July 2018
Received in revised form 24 October 2018
Available online 6 February 2019

Keywords:
Robustness assessment
Structural characteristic
Functional characteristic
Percolation theory
Vulnerability

ABSTRACT

We analyze the structural and functional robustness of networked critical infrastructure systems (CISs). We propose a structural and functional robustness model of a typical complex network and take into account the corresponding measuring metrics and cascading processes to assess the impact of different hazard modes on robustness. We analyze the robustness of the shanghai subway network and the central China power grid to demonstrate an application of the model. We find that both are strongly robust to random failure but extremely vulnerable to targeted attack. We identify the critical areas most likely to be attack targets and use a functional perspective to identify vulnerabilities. Our proposed method can be applied to other CISs and aid in understanding the mechanisms of network robustness.

1. Introduction

Real-world networks are critical infrastructure systems (CISs) that function collaboratively and synergistically to produce essential services and facilitate human interaction [1]. In recent years researchers have recognized the importance of CIS robustness. System failure reduces the stability and safety of CISs [2]. For example, power networks can fail due to system overload and subway systems can be disrupted by terrorist attacks. While it would be ideal if failures could be prevented entirely, this is unlikely since every system will experience failure at one time or another.

Robustness to failure is an important research hotspot for CISs in general, and our goal here is to find a way to deeply understand CISs so that they can be optimized by the structure and continue functioning when some of their nodes fail.

* Correspondence to: School of Electrical Engineering and Automation, Jiangsu Normal University, Xuzhou, 221116, China.
E-mail address: zlfccnu@bu.edu (L. Zhao).

https://doi.org/10.1016/j.physa.2019.01.134
0378-4371/

We can describe CISs as networks composed of nodes and links through which hazard impacts can spread [3,4]. Complex network methods and theories have been greatly expanded and widely applied to questions associated with CISs [5,6] and other areas, such as disease related genes [7] and miRNAs [8], and we use them here to study CISs robustness.

In studying cascading failure processes and CIS robustness, researchers have focused on robustness [9], the resilience of networks to cascading failure [10], their tolerance to failure [11], failure cascade patterns in coupled network systems [12,13], the control of cascades, and defense strategies [14–16].

There are two traditions in the CIS robustness literature. One tradition studies the robustness based on their structural properties. Here the state of a node depends on the state of its neighbors, i.e., failing nodes cause neighbors to also fail. The second tradition examines the CIS mechanism to assess the consequence of disruptions. The models produced by the se studies demonstrate that when an overloaded node stops traffic flow, the choosing of alternative paths can overload other nodes, and a cascading failure that disables the entire network can result.

Little research has been done that simultaneously considers both structural and functional aspects, and studies of CIS robustness tend to focus on one aspect and ignore the others. To understand CIS robustness we must take into account both structural and functional considerations. That is our goal here. We want to understand CIS robustness and be able to assess both the structural and functional robustness of networked systems.

We structure the rest of our paper as follows. Section 2 describes typical complex network models and a statistical index. Section 3 describes robustness assessment methods. We use percolation theory to assess structural robustness and a local load redistributed model to analyze functional robustness. Section 4 introduces our case study of the Shanghai subway network and central China power network and discusses our results. Section 5 describes our conclusions and some prospects for future research.

2. Network models and statistical index

Most currently-discovered properties of complex networks are related to their structures [17,18]. Complex networks can be hierarchical, scale-free, small world, random graph, and regular and can also take other forms. To study complex network robustness we focus on three network structures, i.e., the Watts–Strogatz (WS) small-world network, the Barabasi–Albert (BA) scale-free network, and the Erdos–Rényi (ER) random network. We also describe several statistical indices, including degree, degree distribution, clustering, characteristic path length, and betweenness centrality.

2.1. Network models

The ER random network has a complex topology in which each vertex has a random number of connecting vertices. Because these connections are assigned randomly they have a Poisson degree distribution when the network size is large [19], and the likelihood that a node has a degree k is given by $P(k) = \langle k \rangle^k e^{-k}/k!$.

The WS small-world network falls midway between a regular and random network [20]. There are only a few links between nodes and most nodes to not have neighbors. To build a WS network we select the nearest coupled network with a node quantity N and connect each node to N nearest nodes. We then cut each edge, reconnect it randomly with a probability q, and disallow self-loops and multiple edges.

The BA scale-free network exhibits the properties of such real-world networks as the Internet, the WWW, citation networks, and some infrastructure networks. Scale-free graphs reveal that their degree distribution often takes the form of a power law, i.e., their degree distribution is $P(k) \sim k^{-\gamma}$ [21]. When $\gamma < 3$ some nodes collect many more connections than the other nodes and the variance moves toward infinity.

The Erdos–Renyi (ER) random network, the Watts–Strogatz (WS) small world network, and the Barabasi–Albert (BA) scale-free network are now considered benchmarks, and they have the following characteristics:

(1) Erdos–Rényi (ER) Random network:

- The nodes are randomly connected to each other.
- Modeled using the Erdö s–Rényi model.

(2) Watts–Strogatz (WS) small-world network:

- Most nodes are not neighbors, but they can connect to any other node through a small number of steps.
- Modeled using the Watts–Strogatz model.

(3) Barabasi–Albert (BA) scale-free network:

- The degree distribution follows a power-law, at least asymptotically.
- Modeled using the Barabasi–Albert (BA) model.

2.2. Network attributes

2.2.1. Degree and degree distribution

The degree of the vertex is defined as the number of edges incident to it. Here $\langle k \rangle$ is the average degree, which indicates the network characteristics. The degree distribution $p(k)$ is defined $p(k) = n_k/N$, where n_k is the number of nodes with degree k, and N is its size.

2.2.2. Characteristic path length

The characteristic path length $\langle d \rangle$ is the average distance among node pairs in a graph, and it can be used to measure network performance.

2.2.3. Clustering coefficient

The average clustering coefficient C describes the correlative degree among a node's neighbors and quantifies the local connectivity of the network.

2.2.4. Betweenness

The betweenness of node ν in complex network G denoted by $B(\upsilon)$ is defined $B(\upsilon) = \sum_{s,t \in V(G) \setminus \{\upsilon\}} \frac{\sigma_{st}(\upsilon)}{\sigma_{st}}$ where $V(G)$ is the node set and $\sigma_{st}(\upsilon)$ is the number of shortest paths passing through node υ.

2.2.5. Giant component

The giant component is the largest connected subgraph in a network. When the giant component changes size, the phase transition that occurs indicates the behavior at or near the critical point. Mathematically the giant component is $P_\infty = G(k)/G(0)$. Here $G(k)$ and $G(0)$ are the largest connected component after and before the attack, respectively.

3. Robustness assessment model

We define robustness of CISs as its ability to maintain integrity in case that components are disturbed under failures. Both the structural and functional aspects are considered to give a deeply understanding of the robustness of CISs. We use percolation theory when considering structural robustness. A local redistributed model is considered When studying functional robustness.

3.1. Structural robustness assessment method

3.1.1. Failure propagation model

We use percolation theory to determine the fraction of the system that remains connected after a series of failures occur. We assume that a fraction $1 - p$ of nodes are removed from the network. The network fragments into clusters. The largest cluster, which is the fraction of nodes remaining in the largest connected component, is the giant connected component P_∞, and only nodes that are part of this largest cluster are considered functional. All others are considered failed.

3.1.2. Parameter measurement

We use the giant connected component P_∞ to quantify network robustness. A larger P_∞ value indicates a larger number of nodes in the giant component and increased system robustness to attack. Figs. 1–3 show the giant connected clusters in three complex networks as a function of the nodes remaining after a random and a targeted attack.

In a single Erdős–Rényi network we find $P_\infty = p\left(1 - e^{-kP_\infty}\right)$. Here p is the fraction of remaining nodes in the network after initial failures and k is the average degree. In addition, because P_∞ appears on both sides of the equation and no additional simplification is possible, the equation is transcendental and can only be solved numerically.

We find that scale-free networks are much more robust to random failure than random networks, but that scale-free networks are extremely vulnerable when the attack is targeted, and the removal of a small fraction of nodes can cause total fragmentation. In contrast, the WS small-world network and the ER random network are both robust to targeted attack.

3.2. Functional robustness assessment method

3.2.1. Cascading model

To model and understand the functional aspects of the failure spreading process, we examine overload failures to determine how they propagate. We define load to be the betweenness centrality that quantifies the number of shortest paths that pass through a given component. Initially the component load is determined by network structure and nodes with a greater number of shortest paths have a higher load. We assume that in the stable state the load of each node is less than its security threshold. Fig. 4 shows that when nodes are removed or fail their load is reassigned to neighboring nodes according to the load redistribution model.

We denote the redistributed load F_i and define the additional load received by node j to be $\Delta F_j = F_i \times \left(W_j / \sum_{a \in \Gamma_i} W_a\right)$. Here Γ_i is the set of neighboring nodes of i, and W_j is the initial load of node j.

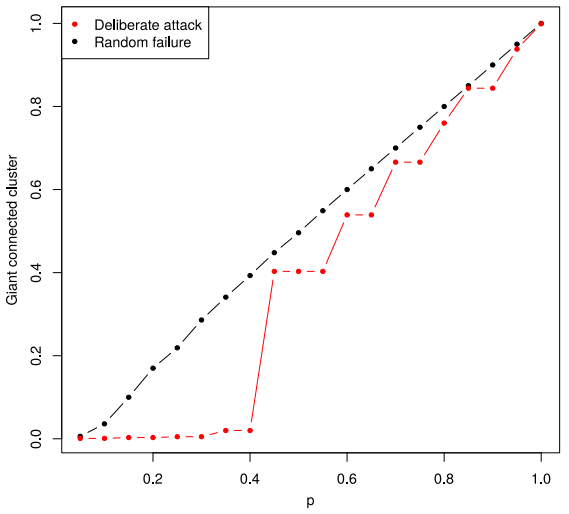


Fig. 1. Ratio of giant clusters of the Erdős–Rényi random network in dependence of the fraction of remaining nodes under random failures and deliberate attacks.

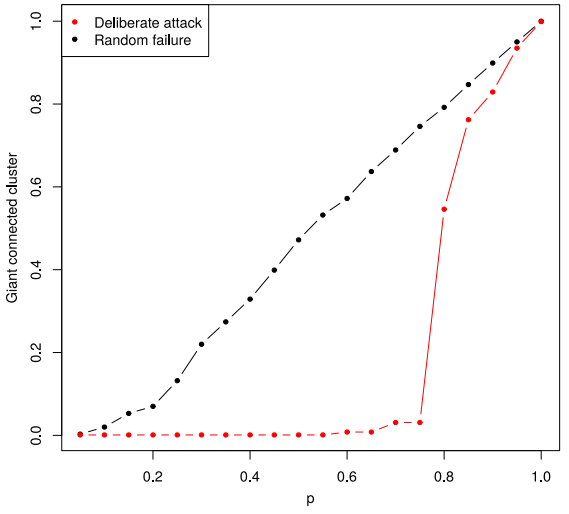


Fig. 2. Ratio of giant clusters of the BA scale-free network in dependence of the fraction of remaining nodes under random failures and deliberate attacks.

3.2.2. Capacity of the node

The maximum load that a node can handle is its capacity. A node ability to process its load is determined by the technology used and the economic conditions of its construction. We assume that the capacity C_j of node j is proportional to its initial load L_j. Here $C_j = (1+\alpha)L_j$, where the constant α is the tolerance parameter. After an initial set of localized failures, the paths between nodes change and the load is redistributed. This load redistribution may push other nodes beyond their capacity limit and cause them to fail. When the loads of the remaining nodes in the network fall below their safety thresholds, the cascading failure stops and the network is in a new stable state.

3.2.3. System robustness measurement

We denote the performance value under normal operating conditions and after a damage event to be P_{norm} and P_{damg}, respectively. We quantify network vulnerability to be its drop in performance following a disruptive event and use it as a metric to measure robustness. Here

$$V_P = \frac{P_{norm} - P_{damg}}{P_{norm}}. \tag{1}$$

The characteristic path length is defined to be the average number of steps along the shortest paths for all possible pairs of network nodes. It measures both network size and overall connectivity, and we use it as a performance index. To avoid

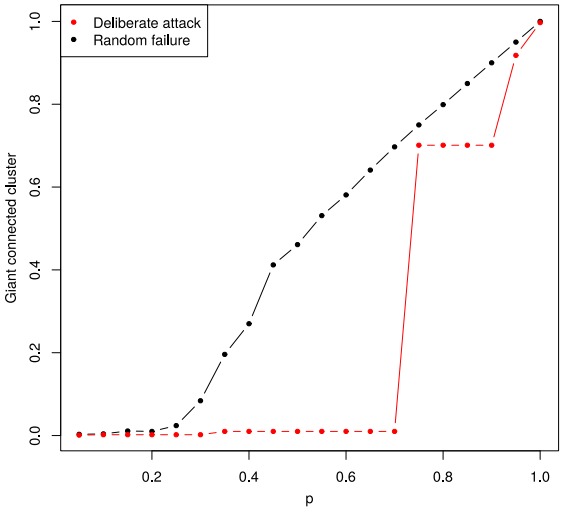


Fig. 3. Ratio of giant clusters of the WS small world network in dependence of the fraction of remaining nodes under random failures and deliberate attacks.

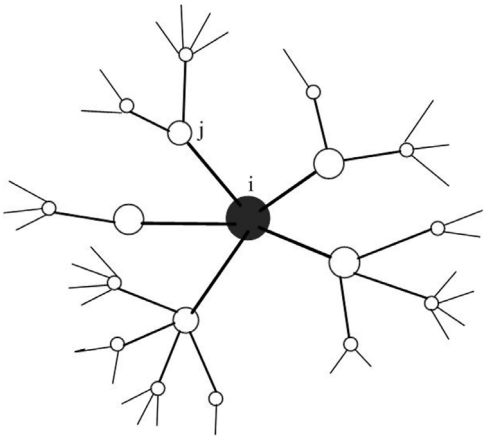


Fig. 4. The schematic diagram of load redistribution after the breakdown of node.

invalid values caused by disconnections, we used the reciprocal characteristic path lengths to measure network performance and define it

$$P = \frac{1}{N\,(N-1)} \sum_{i \neq j} d_{ij}. \tag{2}$$

Here d_{ij} is the shortest distance between two nodes i and j. When we know the level of network performance we can calculate its vulnerability. A higher vulnerability value indicates that the network is less robust to attack, and a lower vulnerability value indicates that the network is more robust to attack.

3.3. Failure modes

Random failure is the most common threat to real-world complex networks. For example, an electric power network inevitably experiences different types of equipment and node failure.

Targeted attack is an attack on important, high-degree network nodes. Thus we need a way of evaluating node importance to determine which nodes are key and play crucial roles in maintaining network robustness.

Spatially localized attack is another real-world phenomenon we must understand in order to understand network robustness. We need a way of identifying the critical areas that are potential targets for intelligent attackers. We also need to understand the systemic failure spreading process that occurs when this attack takes place.

Table 1
Comparing analysis of topological properties of different power networks.

Network	N	E	$\langle k \rangle$	$\langle d \rangle$	D	C
CCPG	295	413	2.800	7.922	20	0.096

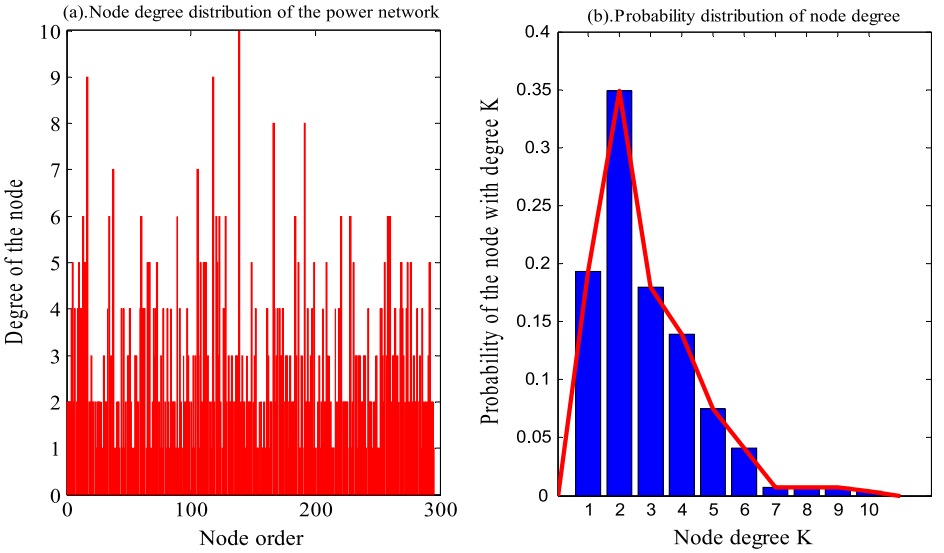


Fig. 5. Degree and degree distribution of the central China power network.

4. Real network model

Many real CISs such as power grids and subway systems can be modeled as complex networks. What constitutes a node and link depends on the system being analyzed. For example, in power grids the nodes are power stations and substations and the links are powerlines connecting the stations. In a subway network, stations are nodes and subway tracks are edges. Many empirical studies have found that real-world complex networks have characteristics that are similar to scale-free, small world, or random networks.

4.1. Central china power network

We first study the transmission system of the central China power network. Table 1 uses basic statistical metrics to describe the topological properties of this power network. Most of the nodes in the central China power network are low-degree, but the network is heterogeneous and some nodes are high-degree hubs. In addition, the degree distribution this network follows an approximate power-law distribution and thus exhibits characteristics found in a scale-free network (see Fig. 5).

4.1.1. Structural robustness results of the power network

The structural robustness of a network quantifies its ability to retain its structural integrity when its components are disrupted. Fig. 6 shows the giant connected clusters of the power network as a function of the nodes remaining following random and targeted attacks. Note the comparison with a scale free network. Unlike most power networks, this transmission network resembles a theoretical BA scale-free network in that it is relatively robust to random failure but vulnerable to targeted attack. When 10% of the nodes are destroyed by random failure the value of the giant connected clusters decreases slightly, but when the giant connected clusters are targeted failure occurs after the removal of only a small fraction of nodes.

4.1.2. Functional robustness results of the power network

We use the local load redistribution model introduced above to study power network robustness in terms of function and overload failure. Fig. 7 shows the vulnerability of the central China power network under random failure and targeted attack. Note that a random failure of nodes causes less network damage than a targeted attack. This supports our assumption that deliberate attacks focus on high-degree nodes, the failure of which can trigger cascading failures and systemic shutdown.

To analyze power network robustness to localized attacks, we must identify the critical areas most likely to be attacked and analyze their vulnerability. Intelligent attackers usually select most intensive areas. Research has found that many

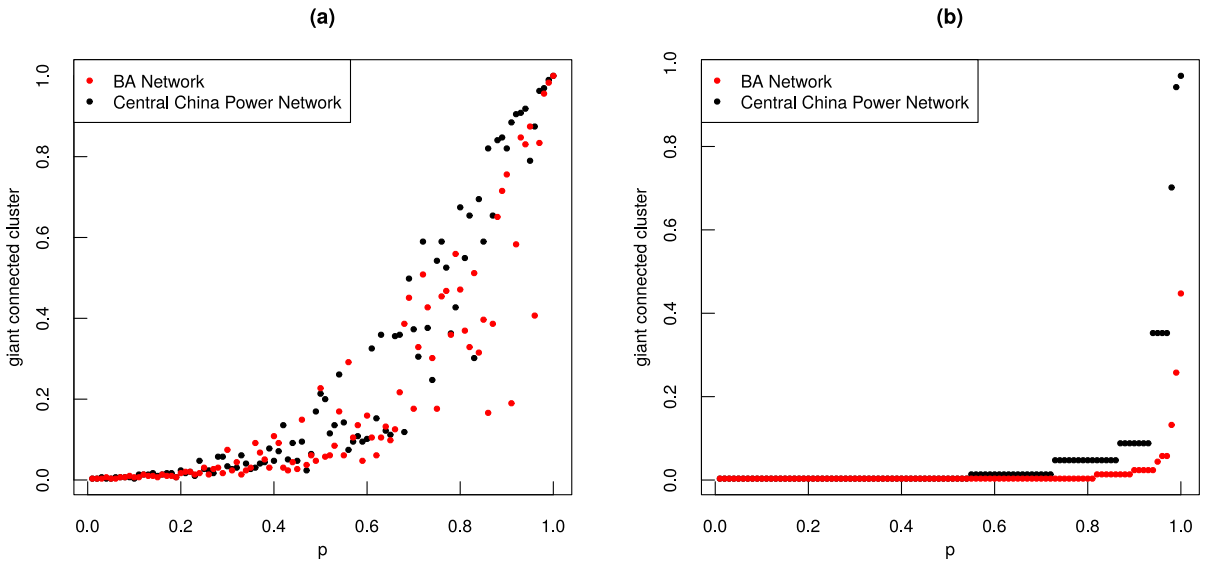


Fig. 6. Ratio of giant connected clusters in dependence of the fraction of removed nodes Comparing with BA Network, (a) Random failures, (b) Deliberate failures.

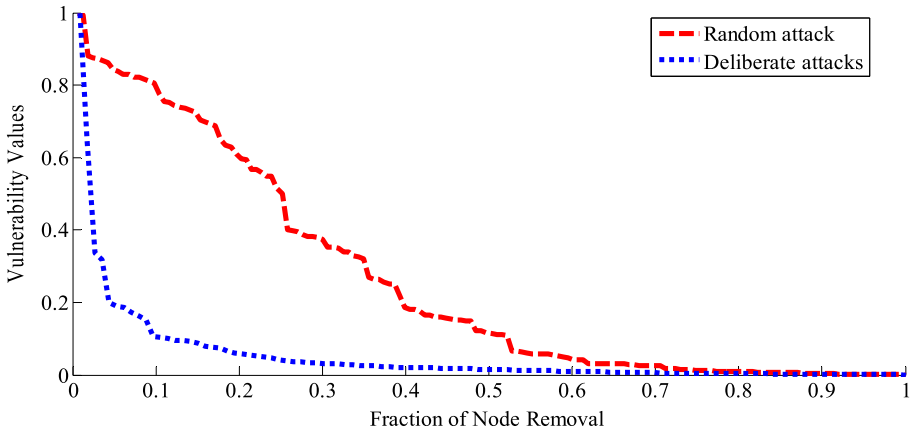


Fig. 7. Vulnerability of central China power network in dependence of the fraction of removed nodes under random and deliberate attacks.

networks have community structures that are relatively dense in their internal connections but sparsely connected to other dense network groups [22,23]. We use the fast modularity algorithm [24,25], which determines the shortest distance between node pairs by selecting the link mostly used, to detect communities.

Fig. 8 shows the power network partitioned into 15 communities. These intensive community based areas reflect their regional importance, and show their likelihood of being targets for attack. Although a hazard can be spatially local in a network system, its impact can spread through network topology and become global. Fig. 9 shows that the variation in the vulnerability values of different community areas is extremely large. The disruption of a dense area has a greater negative impact on performance. For example, attacks on Area-5 and Area-6 located in the interior of the power network produces large vulnerabilities of 0.5189 and 0.6443, respectively, and thus should be given prioritized protection.

4.2. Shanghai subway network

Fig. 10 shows the large Shanghai Metro subway network. It has 14 different lines and extends over 617 km, and future plans include five extensions and four completely new lines, which will make it the largest subway network in the world.

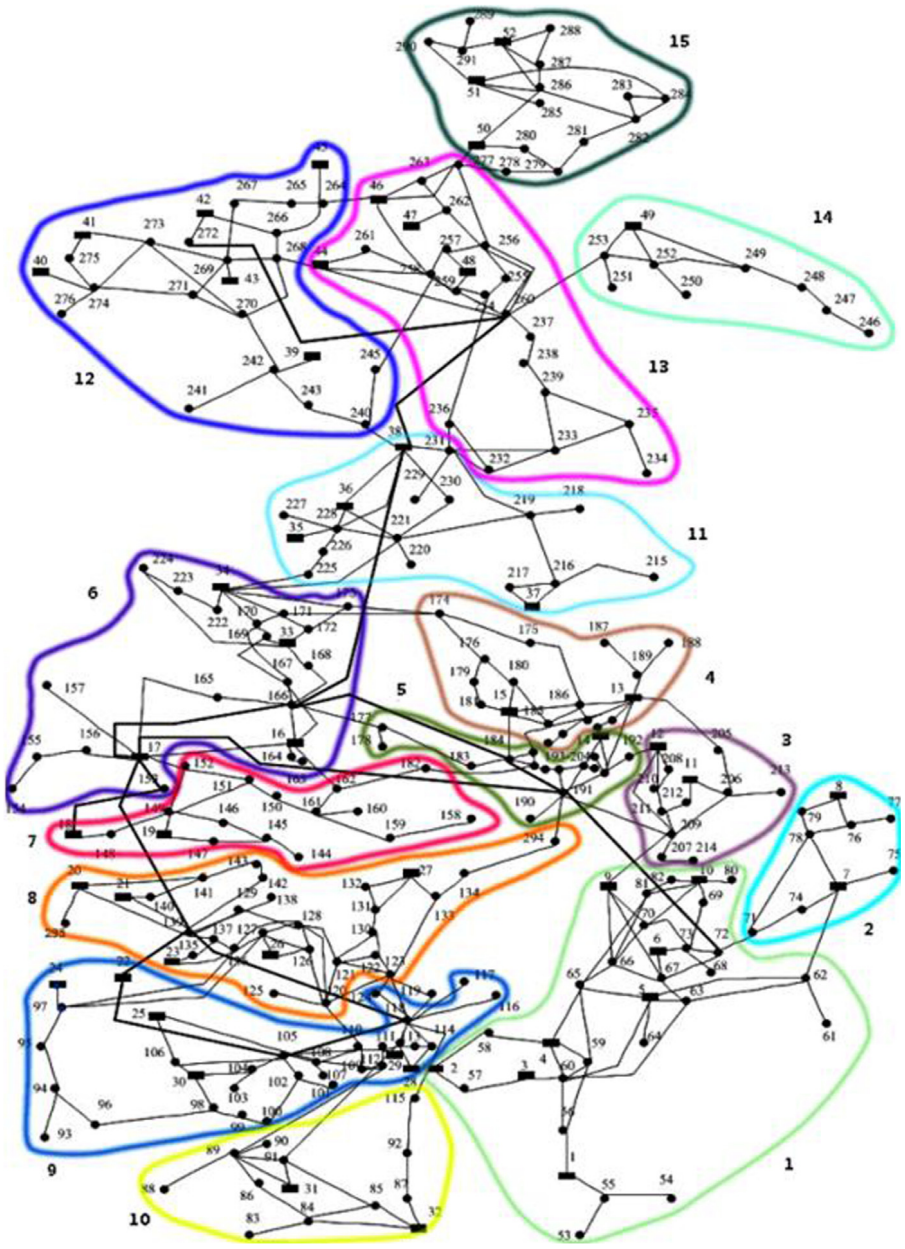


Fig. 8. Community structures of central China power network.

4.2.1. Structural robustness results of the subway network

Although the size of the Shanghai subway system is smaller than a true complex network, it is similar to a BA scale-free network (see Fig. 11) and exhibits a second-order phase transition under random failure and a first-order phase transition under targeted attack.

4.2.2. Functional robustness results of the subway network

We next analyze the functional robustness of the subway network under random failure, targeted attack, and spatially localized attack. Fig. 12 shows the vulnerability of the Shanghai subway network in terms of the fraction of removed nodes under random failure and targeted attack. When the subway network is attacked, the performance decreases. Then, the vulnerability values can be easily observed from the figure. The results shown in Fig. 12 reveals that the random removal of nodes will cause less damage to the network than the deliberate attack, it is similar with the results of the power network.

We next identify the critical areas of the Shanghai subway network and analyze their vulnerability. We partition the subway network into 16 communities. Fig. 13 shows the vulnerability curves of these critical areas as a function of attack

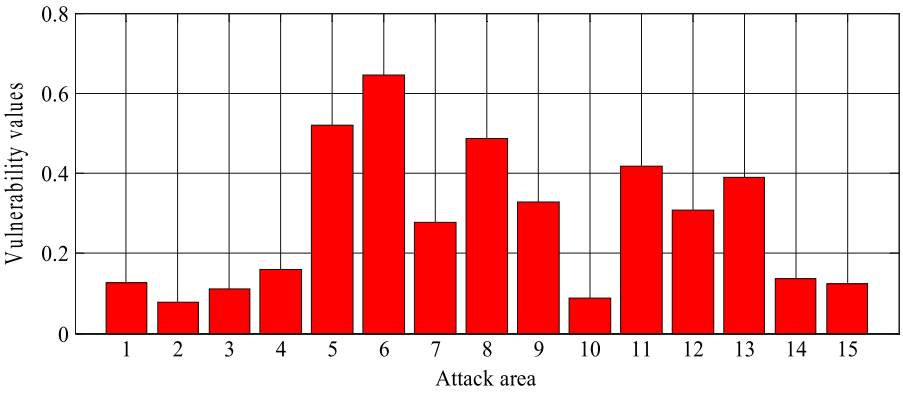


Fig. 9. Vulnerability values of different community areas.

Fig. 10. Network-based structure of the Shanghai subway network.

times. Note that when the number of attacks increases in critical community areas, more vertices are removed from the network, decreasing the performance and increasing the vulnerability values. In addition, only a small number of node disruptions are needed to cause some areas to collapse. For example, Area-12 and Area-15 are destroyed completely after being attacked only five times. These results indicate that some critical areas exhibit higher attack susceptibilities.

5. Conclusion

We have presented a comprehensive description of CIS robustness and have proposed methods of assessing the structural and functional robustness of networked systems. We analyze the central China power network and the Shanghai subway

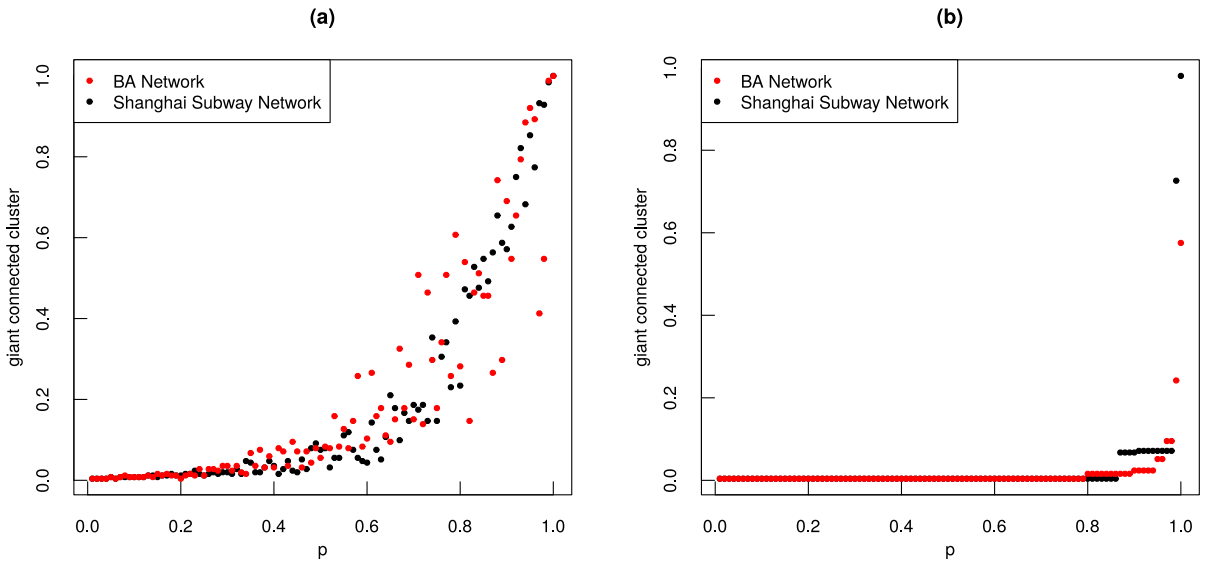


Fig. 11. Ratio of giant connected clusters of the Shanghai subway network in dependence of the fraction of removed nodes, (a) Random failures, (b) Deliberate failures.

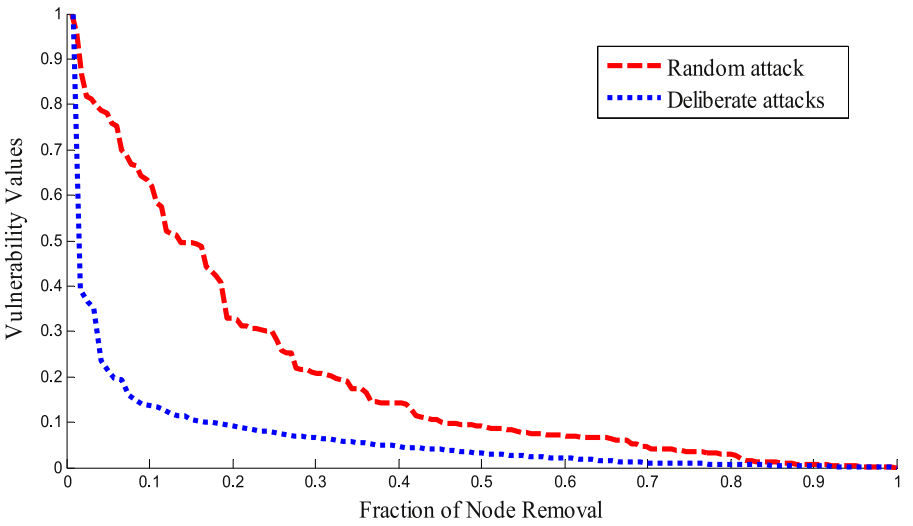
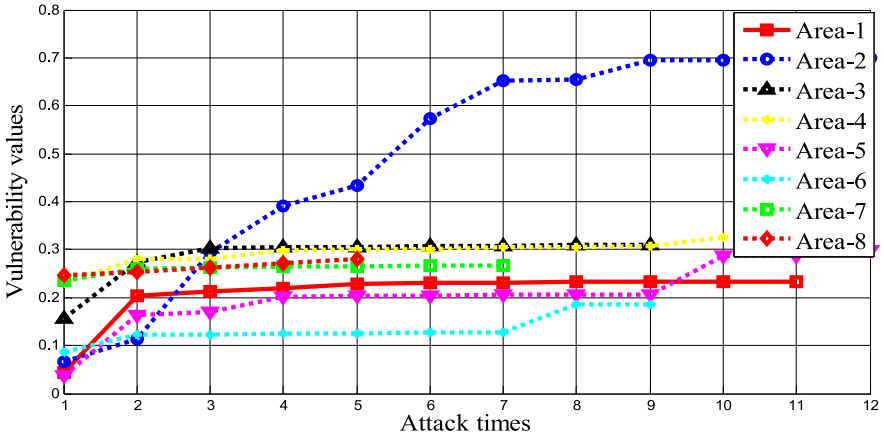


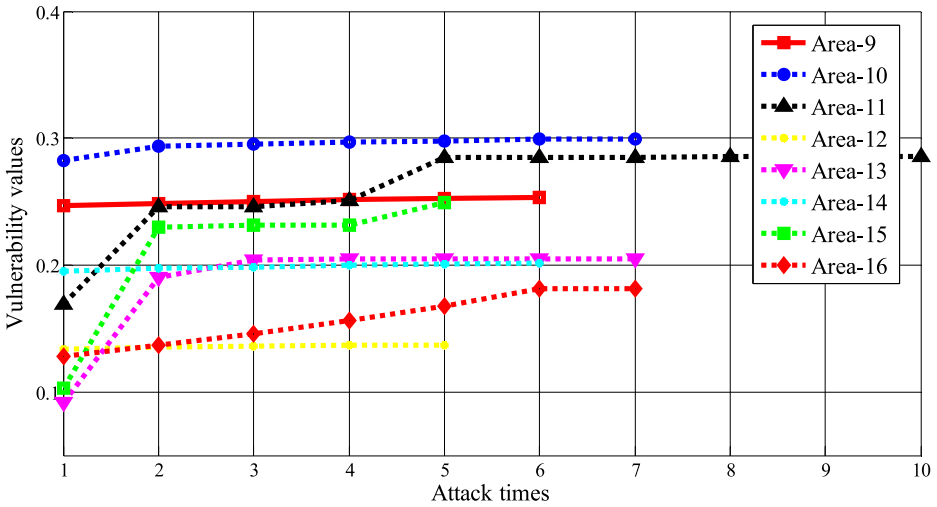
Fig. 12. Vulnerability of Shanghai subway network in dependence of the fraction of removed nodes under random and deliberate attacks.

network, and analyzed the giant connected clusters as a function of the nodes remaining following random failure and targeted attack. We also identify the critical areas that most likely to be attacked and analyze their vulnerability. We find that they exhibit characteristics similar to those of a scale-free network.

Although our proposed methods can be applied to other CISs, we only analyze the structural and functional robustness and future research could include ways of improving CIS robustness and developing repair strategies. For example, common methods of increasing CIS robustness to random failure could include random addition, low-degree node addition, low-betweenness node addition, and additions based on algebraic connectivity. Methods of analyzing key CIS nodes based on the idea of protecting key nodes to improve robustness to targeted attack are also important. A further challenge would include how to repair and recover a CIS after it has experienced failure. It may be ineffective to repair failed components if failure again spreads to the repaired components. Other approaches will be suggested and explored in future research.



(a). Vulnerability values produced by different critical areas as a function of attack times



(b). Vulnerability values produced by different critical areas as a function of attack times

Fig. 13. Vulnerability values produced by different critical areas as a function of attack times.

Acknowledgments

This work is jointly supported by National Natural Science Foundations of China (No. 61503166), the Scientific Research Foundation of Chongqing Education Commission (KJ1400329, KJ1600509), the Foundation and Frontier Projects of Chongqing Science and Technology Commission (cstc2016jcyjA0561), and the science and technology project of Xuzhou (KC16SG253). The Boston University Center for Polymer Studies is supported by NSF Grants PHY-1505000, CMMI-1125290, and CHE-1213217, and by DTRA Grant HDTRA1-14-1-0017.

References

[1] Cen Nan, Irene Eusgeld, Adopting HLA standard for interdependency study, Reliab. Eng. Syst. Saf. 96 (2011) 149–159.
[2] H. Zhang, M. Yuan, Y. Liang, et al., A risk assessment based optimization method for route selection of hazardous liquid railway network, Saf. Sci. (2018) http://dx.doi.org/10.1016/j.ssci.2018.04.003.
[3] X.B. Hu, H. Li, X.M. Guo, et al., Spatial vulnerability of network systems under spatially local hazards, Risk Anal. (2018).
[4] C. Fu, Y. Gao, S. Cai, et al., Center of mass in complex networks, Sci. Rep. 7 (2017) 40982.
[5] H. Wang, M. Li, L. Deng, et al., Robustness of networks with assortative dependence groups, Physica A 502 (2018) 195–200.
[6] D. Zhang, F. Du, H. Huang, et al., Resiliency assessment of urban rail transit networks: Shanghai metro as an example, Saf. Sci. 106 (2018) 230–243.

[7] Xiangxiang Zeng, Yuanlu Liao, Yuansheng Liu, Quan Zou, Prediction and validation of disease genes using HeteSim scores, IEEE/ACM Trans. Comput. Biol. Bioinform. 14 (3) (2017) 687–695.
[8] Quan Zou, Jinjin Li, Li Song, Xiangxiang Zeng, Guohua Wang, Similarity computation strategies in the microRNA-disease network: a survey, Brief. Funct. Genomics 15 (1) (2016) 55–64.
[9] A. Shen, J. Guo, Z. Wang, Research on methods for improving robustness of Cascading failures of interdependent networks, Wirel. Pers. Commun. 95 (3) (2017) 2111–2126.
[10] D. Zhou, A. Elmokashfi, Overload-based cascades on multiplex networks and effects of inter-similarity, PLoS One 12 (12) (2017) e0189624.
[11] B. Mirzasoleiman, G. Hamed, M. Jalili, CaScading failure tolerance of modular small-world networks, IEEE Trans. Circuits Syst. II-Express Briefs 58 (8) (2011) 527–531.
[12] Xueming Liu, H. Eugene Stanley, Jianxi Gao, Breakdown of interdependent directed networks, Proc. Natl. Acad. Sci. 113 (5) (2016) 1138–1143.
[13] Baichao Wu, Aiping Tang, Jie Wu, Modeling cascading failures in interdependent infrastructures under terrorist attacks, Reliab. Eng. Syst. Saf. 147 (2016) 1–8.
[14] Enrico Zio, Challenges in the vulnerability and risk analysis of critical infrastructures, Reliab. Eng. Syst. Saf. 152 (2016) 137–150.
[15] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature 464 (2010) 1025–1028.
[16] S. Wang, L. Hong, M. Ouyang, et al., Vulnerability analysis of interdependent infrastructure systems under edge attack strategies, Saf. Sci. 51 (1) (2013) 328–337.
[17] L.M. Shekhtman, M.M. Danziger, S. Havlin, Spreading of Failures in Interdependent Networks. Diffusive Spreading in Nature, Technology and Society, Springer, Cham, 2018, pp. 397–410.
[18] Y.C. Gao, Y. Zeng, S.M. Cai, Influence network in the chinese stock market, J. Stat. Mech. Theory Exp. 2015 (3) (2015) P03017.
[19] P. Erdös, A. Rényi, On random graphs, I, Publ. Math. (Debrecen) 6 (1959) 290–297.
[20] D.J. Watts, S.H. Strogatz, Collective dynamics of 'small-world'networks, Nature 393 (6684) (1998) 440.
[21] A.L. Barabási, R. Albert, Emergence of scaling in random networks, science 286 (5439) (1999) 509–512.
[22] R.J. Mondragon, J. Iacovacci, G. Bianconi, Multilink communities of multiplex networks, PLoS One 13 (3) (2018) e0193821.
[23] Z. Lu, J. Wahlström, A. Nehorai, Community detection in complex networks via clique conductance, Sci. Rep. 8 (1) (2018) 5982.
[24] A. Clauset, M.E.J. Newman, C. Moore, Finding community structure in very large networks, Phys. Rev. E 70 (6) (2004) 066111.
[25] M. Girvan, M.E.J. Newman, Community structure in social and biological networks, Proc. Natl. Acad. Sci. 99 (12) (2002) 7821–7826.