A multiple perspective method for urban subway network robustness analysis

Shuliang Wang,[1,2,a] Sen Nie,[2,3] Longfeng Zhao,[2,4] and H. Eugene Stanley[2]
[1]*School of Electrical Engineering and Automation, Jiangsu Normal University, Xuzhou 221116, China*
[2]*Center for Polymer Studies and Department of Physics, Boston University, Boston, Massachusetts 02215, USA*
[3]*School of Electrical & Automation Engineering, East China Jiaotong University, Nanchang, Jiangxi 330013, China*
[4]*Key Laboratory of Quark and Lepton Physics (MOE) and Institute of Particle Physics, Central China Normal University, Wuhan 430079, China*

(Received 28 January 2018; accepted 1 July 2018; published online 19 July 2018)

Most network research studying the robustness of critical infrastructure networks focuses on a particular aspect and does not take the entire system into consideration. We develop a general methodological framework for studying network robustness from multiple perspectives, i.e., Robustness assessment based on percolation theory, vulnerability analysis, and controllability analysis. Meanwhile, We use this approach to examine the Shanghai subway network in China. Specifically, (1) the topological properties of the subway network are quantitatively analyzed using network theory; (2) The phase transition process of the subway network under both random and deliberate attacks are acquired (3) Critical dense areas that are most likely to be the target of terrorist attacks are identified, vulnerability values of these critical areas are obtained; (4) The minimum number of driver nodes for controlling the whole network is calculated. Results show that the subway network exhibits characteristics similar to a scale-free network with low robustness to deliberate attacks. Meanwhile, we identify the critical area within which disruptions produce large performance losses. Our proposed method can be applied to other infrastructure networks and can help decision makers develop optimal protection strategies.
https://doi.org/10.1063/1.5023766

While many studies have investigated the robustness of critical infrastructure systems (CISs), most of them focus on a particular aspect, we have not come across a paper on this subject giving a multiple perspective method. We think that it is of great importance to assess robustness from a multiple perspective to deeply understand the CISs. So, this paper introduces a multiple perspective approach to assess the robustness of subway network, where the robustness of a network is characterized as its ability to maintain structural and functional integrity in case that nodes or edges are disturbed under random failures or intentional attacks. We quantitatively analyze the topological properties of the system and determine the phase transition process of the system under different failure scenarios. Then, we identify the critical dense areas that are most likely to be targets of attack and quantify their vulnerability. We calculate the number of minimum driver nodes needed to make the entire system controllable. We find that the subway system exhibits characteristics similar to a scale-free network with low robustness to deliberate attacks. We locate the critical area within which disruptions produce large performance losses. It is argued that the proposed method in this paper enables studying other infrastructure

[a]Corresponding author: Shuliang Wang, Email: shuliang0820@sina.com

networks. Meanwhile, the method is helpful for decision makers to develop optimal protection strategies.

I. INTRODUCTION

Real-world networks are critical infrastructure systems (CISs) that function collaboratively and synergistically to produce essential services and facilitate human interaction.[1] Examples include electrical power systems, telecommunication systems, water supply systems, natural gas supply systems, and transportation systems, all of which are essential in maintaining the economy of a nation and the well-being of its citizens.

Among CISs, subway systems are particularly important. They provide essential public transport services and play a key role in urban economic development. Urban subway networks have been greatly expanded in recent years, and now medium-sized cities are building them, and even some small cities have plans for their construction. Large cities such as New York, Shanghai, and London continue to maintain and expand them, and the result is complex subway networks with high station densities and intricate interstation coupling.[2]

The 2010 bombing in the Moscow subway and the 2008 London subway accident clearly indicate that random failure or deliberate destruction impairs the robustness of a subway network. Because disruptions cause economic loss and strongly affect citizen mobility and quality of life, the modeling and analysis of urban subway network robustness has become a rapidly expanding field in recent years.

The recent expansion and increasing availability of data mining and the use of artificial intelligence have enhanced our understanding of CISs. For the analysis of CISs, Researchers have devised a number of different models for analyzing their robustness, including approaches that are empirical[3] or agent-based,[4] or that focus on system dynamics,[5] economic theory,[6] or complex network theory.[7] Because we need topological and geographical information in the research we describe in this paper, we use complex network theory in this paper.

There has been some prior research that has used complex network theory to model and analyze urban subway networks. Dribble and Kennedy analyzed the vulnerability of 33 subway networks world-wide using complex network theory.[8] Wang et al. studied the vulnerability of urban rail systems in San Francisco and Boston, and identified their most vulnerable segments.[9] Rodríguez-Núñez and García-Palomares presented a methodology and used it to analyze the vulnerability of the Madrid subway network.[10]

In addition, the robustness of controllability for complex networks has also been investigated recently.[11–13] A system is controllable if it can be driven from any initial state to any desired state within finite external inputs in finite time. Controllability of complex networks has attracted a lot of attention.[14–20] Liu et al.[14] introduced an analytical framework to study the structural controllability of directed networks and identified the minimum number of driver nodes than can guide the system's dynamics. Further, Wang et al.[15] proposed the exact controllability to determine the minimum driver nodes for both directed and undirected networks. Based on these research,[11–13] analyzed the robustness of controllability for networks in cascading failure and discussed the results under different attack strategies. However, the controllability of real networks has not been investigated sufficiently.

Although these studies have improved our ability to analyze the robustness of urban subway networks, most of them focus on a particular aspect and lack an integrating mechanism that allows a full consideration of the system. This approach is no longer adequate because subway networks are growing in complexity and heterogeneity, and it particularly in adequate when redesigning a system and strengthening it robustness.

We thus propose a multiple perspective approach to the analysis of urban subway network robustness that uses percolation theory, vulnerability theory, and controllability theory, and we closely examine the Shanghai subway system. In Sec. II we introduce the case study of the Shanghai subway. In Sec. III we describe the methodology used in our multiple perspective robustness analysis. In Sec. IV we discuss our results, and in Sec. V we present our conclusions and suggest possible avenues for future research.

II. A REAL MODEL

A. The Shanghai subway network

Shanghai is the economic, financial, cultural, educational and transportation center of China, with a population of 24 million and a land area of 6340 square kilometers. To expand its public transportation system, the government of Shanghai has constructed a 617 km subway network with 14 interconnected lines (Fig. 1). There are plans to extend five of these lines and to add four new ones, which will make it the largest subway network in the world. It has proven to be a highly convenient and effective transportation system, and on some holidays it carries in excess of 10 million people. Maintaining its robustness is thus highly important.

B. Topological properties

We here use complex network theory to study subway network robustness in which stations are nodes and lines are edges. The subway stations are presented by nodes while lines are presented by edges. The function network has 277 edges and 252 nodes. The average shortest distance, i.e., the mean number of stops between origin and destination, is 14. Here $G = <V, E, A>$ is an annotated, simple, undirected graph, where $V = \{v_i | i \in I = \{1,2,\ldots,N\}\}$ is the set of nodes and $E = \left\{e_{ij} = \left(v_i, v_j\right) | i,j \in I\right\} \subseteq V \times V$ the set of edges, and $A = \left(a_{ij}\right)_{N \times N}$ is the adjacent matrix of the graph, with entries equal to 1 if there is an edge joining node i to node j and to 0 otherwise. Figure 2

FIG. 1. Network-based structure of the Shanghai subway network.

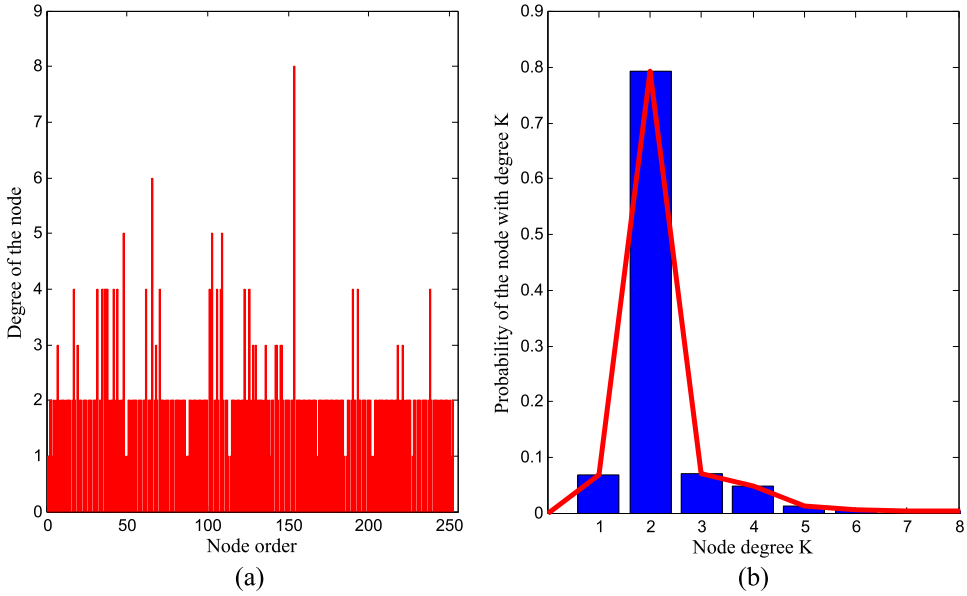

FIG. 2. Degree and degree distribution of the Shanghai subway network. (a) Node degree distribution of the subway network (b) Probability distribution of node degree.

shows the degree distribution. Most network nodes have a degree of two, suggesting that any expansion of the network will be linear. In addition, its degree distribution is approximately power-law, and thus the Shanghai subway system is approximately scale-free.

The size of a subway network is really smaller than the typical huge complex network. Thus, certain gaps between the features of the subway network and the huge scale-free complex network are inevitable. However, Yang et al.[21] indicate (i) the similarity in evolution pattern (the new nodes are prone to link to nodes with highest connections in the original network), (ii) conventional applications of complex network to various infrastructures (It is proved that the complex network theory has a potential to be applied to networks in different scales), and (iii) that the fact of traffic congestion and system failure caused by hub station incidents make the use of complex network theory to analyze subway network robustness reasonable and advantageous.

III. METHODOLOGY

The robustness of a network is characterized as its ability to maintain structural and functional integrity in case that nodes or edges are disturbed under random failures or intentional attacks. This paper gives a multiple perspective method to analyze the robustness of the subway network based on three aspects, (i) percolation, (ii) vulnerability, (iii) controllability. Figure 3 shows our methodological framework for analyzing robustness.

A. Failure types

There are three general types of failure. The first involves such natural hazards as earthquakes, hurricanes, and storms, but because subway networks are underground and thus natural disasters can cause rapid systemic destruction we are not considering them in this study. The second type is random failure in which network dysfunction is caused by the random failure of one or several nodes. The third type is the targeted attack on important nodes defined by node degree. We use a family of functions[22] in which a value $W_\alpha(k_i)$

$$W_\alpha(k_i) = \frac{k_i^\alpha}{\sum_{i=1}^{N} k_i^\alpha}, \quad -\infty < \alpha < \infty \tag{1}$$

is assigned to each node, which represents the probability that node i with degree k_i is initially attacked and removed. When $\alpha > 0$, high-degree nodes are more vulnerable to deliberate attack.

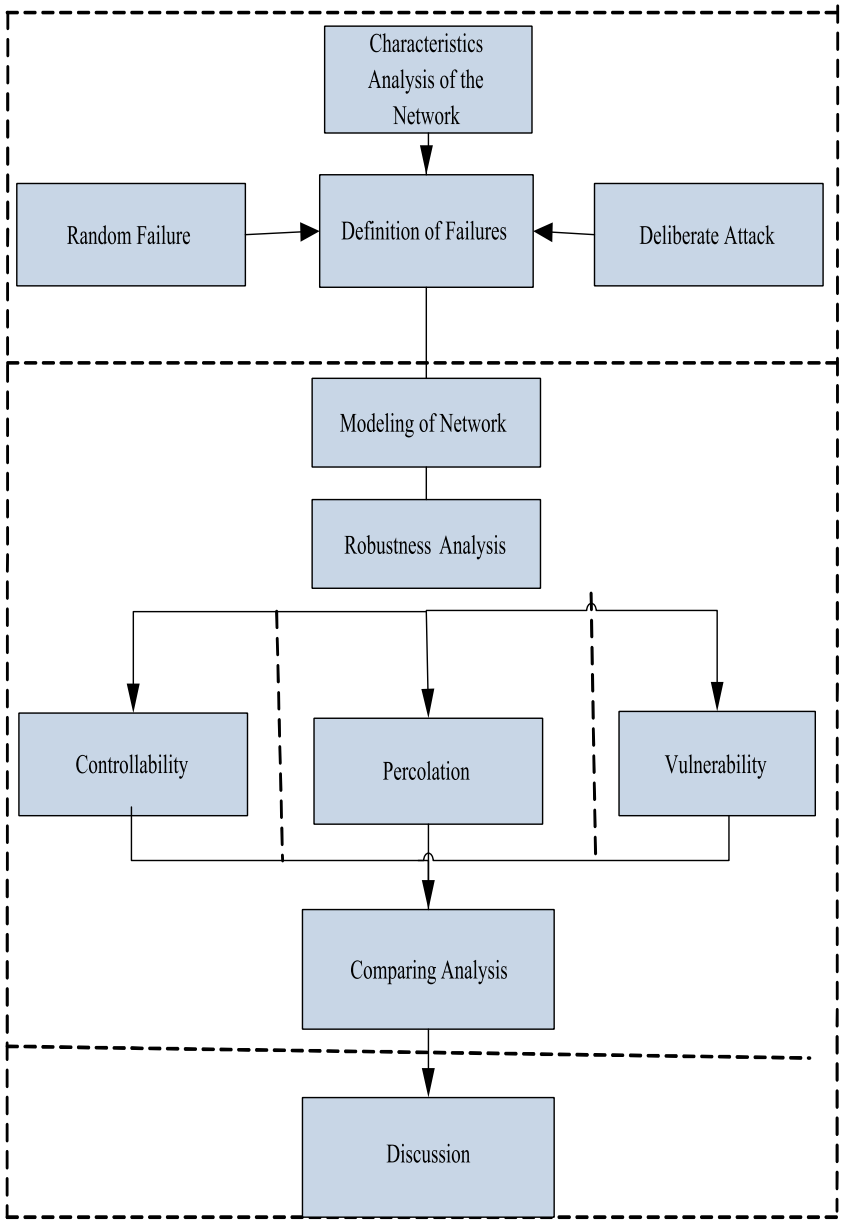

FIG. 3. Methodological framework of subway network robustness analysis.

When $\alpha < 0$, high-degree nodes are protected and have a lower probability of being attacked. When $\alpha = 0$ the removal of nodes is random, but when $\alpha \to \infty$ the removal of nodes is targeted in strict order from high degree to low degree. We also will examine spatially localized attacks, a factor that reflects terrorist intelligence, and we will devise a method of identifying the critical attack areas that require a higher level of protection.

B. Robustness assessment method of subway network

1. Robustness assessment based on percolation theory

Here we develop a method of assessing robustness using percolation theory, a method from statistical physics[23,24] that allows us to better understand real-world systems and improve their infrastructure. We assume a fraction $1 - p$ of nodes are removed from the network due to either random

failure or deliberate attack. The network begins to fragment into connected components called "clusters." We define only giant connected clusters to be functional, and we denote P_∞ the fraction of nodes belonging to the giant component. To illustrate P_∞ as a function of $1 - p$ under both random failure and deliberate failure scenarios and further identify the critical P_c, we define the generating function $G_0(x)$ for the probability distribution of vertex degree k to be

$$G_0(x) = \sum_{k=0}^{\infty} P_k x^k \tag{2}$$

where P_k is the probability that a randomly chosen vertex on the graph has degree k, and x is a random variable. The generating function of the branching process is

$$H_0(x) = \frac{\sum_{k=0}^{\infty} P_k k x^{k-1}}{\overline{k}} = \frac{G_0{}'(x)}{G_0{}'(1)}, \tag{3}$$

We define f to be the probability that a randomly chosen edge does not connect to the giant component, i.e.,

$$f = H_0(f) \tag{4}$$

and hence the probability that a randomly selected node g belongs to the giant component is

$$g = G_0(f). \tag{5}$$

When a fraction $1 - p$ of nodes are removed from the network due to random failure, the generating function remains the same, but with a new argument z that satisfies $z = p \times f + 1 - p$.[25] Thus using f and g the probability that a randomly chosen surviving node belongs to the giant component is

$$g(p) = 1 - G(pf(p) + 1 - p), \tag{6}$$

where $f(p)$ satisfies

$$f(p) = 1 - H(pf(p) + 1 - p). \tag{7}$$

Thus the percentage of remaining nodes belonging to giant connected clusters P_∞ is

$$P_\infty = pg(p) \tag{8}$$

When targeted attacks remove a fraction $1 - p$ of nodes from the network, using Eq. (1) the generating function of degree distribution $P_p(k)$ of the remaining nodes satisfies $G_{Ab}(x) = \sum_k P_p(k)x^k = \frac{1}{p}\sum_k P_p(k)t^{k^\alpha}x^k$. The generating function of the remaining nodes after a targeted attack satisfies $G_{Ac}(x) = G_{Ab}(1 - \widetilde{p} + \widetilde{p}x)$. As pointed by Huang et al.,[26] the difference between the cascading process under a targeted attack and a random attack occurs in the first stage. Network A' has a generating function $\widetilde{G}_{A0}(x)$ such that the generating function of its remaining nodes is the same as $G_{Ac}(x)$ after a random removal $1 - p$ fraction of nodes where $\widetilde{G}_{A0}(x)$ satisfies $\widetilde{G}_{A0}(1 - p + px) = G_{Ac}(x)$. Then the targeted-attack problem can be solved as a random-attack problem.

2. Robustness assessment based on vulnerability analysis

We here assume that system vulnerability can be measured by quantifying its performance drop during a disruptive event. Therefore, in order to measure the vulnerability, performance metric should be determined first. Characteristic path length, which is defined as the average number of steps along the shortest paths for all possible pairs of network nodes and indicates the overall connectivity as well as the size of a network, is chosen as the performance index. It is important to assess robustness by evaluating the error tolerance and attack vulnerability. To avoid invalid values due to potential disconnections, in this paper the reciprocal characteristic path lengths adopted are used to measure network performance. It is defined as follows

$$P = \frac{1}{N(N-1)} \sum_{i \neq j} d_{ij} \tag{9}$$

Where d_{ij} is the shortest distance between two nodes i and j. If the performance value under normal operating conditions is P_{norm}, and P_{damg} after a damage event, then the vulnerability can be given as follows:

$$V_P = \frac{P_{norm} - P_{damg}}{P_{norm}} \tag{10}$$

When the performances under random and deliberate attacks are calculated, the vulnerability of the shanghai subway network can be analyzed.

We also identify critical areas and determine their vulnerability. Research has found that many networks have community structures, defined as a group of elements that are "densely connected to each other but sparsely connected to other dense groups in the network".[27] The communities are related to dense areas in the subway network and those with high vulnerability are most likely to be the target of attacks. So, the community related critical areas will be identified first and the corresponding vulnerability of these areas will be calculated latter.

We apply the fast modularity algorithm[28,29] devised by Newman et al. They use modularity to quantify the community robustness. Associated to a set of k communities, the modularity Q is defined as:

$$Q = \sum_{i=1}^{k} \left(\frac{e_i}{m} - \left(\frac{d_i}{2m} \right)^2 \right). \tag{11}$$

Here k and e_i define the number of communities and the number of links in community i, respectively. d_i is the degree sum of all nodes in community i, and m is the total number of links in the network. In this community detection strategy we (i) designate each node in the subway network a single community, (ii) calculate the change in modularity ΔQ_{ij} when creating a new community from communities i and j, (iii) merge the two communities with the highest ΔQ_{ij} value, and (iv) repeat steps (ii) and (iii) until $\Delta Q_{ij} \leq 0$.

When the communities of the network are acquired, the critical attack area will be identified. This paper considers elements with max degree in the community as the attack center. Meanwhile, it is assumed that all components connecting to the attack center are directly affected by the attacks. The attack strength of the i$^{\text{th}}$ node connecting to the attack center is denoted as:

$$Attack_{node_i}^{strength} = Attack_{\text{center}}^{strength} * (I_i / I_{center}) \tag{12}$$

Where I_{center} and I_i represent the importance degree of the attack center and the i$^{\text{th}}$ node connecting to the attack center. Based on the attack model, the dynamical processes and the performance response can be simulated, the vulnerability of the critical areas can be calculated.

3. Robustness assessment based on controllability

To further understand network robustness, we also analyze the controllability of the Shanghai subway system. Although the structure and dynamics of complex networked systems have received much study over the past decade,[30–33] we still cannot adequately control them. For example, selecting an appropriate target gene in a social network means determining which gene node will produce the desired final outcome. To achieve a desired publicity outcome in a social network means selecting the informational publishing node that can produce the effect.

Consider a network with N nodes described as follows:

$$\frac{dx(t)}{dt} = Ax(t) + Bu(t) \tag{13}$$

Where the vector $x(t) = (x_1(t), x_2(t), \ldots x_N(t))^T$ describes the state of nodes. $A \in R^{N \times N}$ is the adjacent matrix which captures the systems wiring diagram and the interaction strength between individuals. $u = (u_1, u_2, \ldots, u_m)^T$ is the vector of m controllers, and B is the $N \times m$ control matrix that identifies how the external inputs imposed into driver nodes.

The minimal number of driver nodes N_D is used to evaluate the controllability of network, which is calculated by exact controllability as follows:[25]

$$N_D = \max_i \{\mu(\lambda_i)\} \tag{14}$$

where $\mu(\lambda_i)=N-rank(\lambda_i I_N-A)$ is the geometric multiplicity of distinct eigenvalues λ_i of the matrix A. If the network can be controlled with less driver nodes, then the controllability is better.

IV. RESULTS

According to the method proposed above, the integral size of the giant connected component during a whole attacking period and the percolation thresholds are characterized. We also deals more particularly with the performance changing process of the subway network under failures scenarios. Minimum controllable nodes will be identified and applied to assess the controllability, further to analyse the subway network robustness.

A. Robustness results based on percolation theory

Using percolation theory to measure robustness allows us to determine a system's ability to remain functional when its components are disrupted, and this approach can be applied to both random failure and targeted attack scenarios. We assume that a fraction 1 - p of the nodes are removed from the network. Figures 4 and 5 show the giant connected clusters of remaining nodes in a subway network after random and targeted attacks, respectively. When 10% of the nodes are randomly destroyed, the value of the giant connected clusters decreases slightly. When the attack is targeted, after the removal of only a small fraction of nodes the ratio of giant connected clusters rapidly decreases from 1 to less than 0.1. Thus the decrease under targeted disruption is much greater than under random failure, which means the Shanghai subway system is robust to random failure but vulnerable to targeted attack.

Note that the transition process of the Shanghai subway network is similar to the theoretical results of the BA scale-free network model. Most nodes have a small degree of 2, but there are some high-degree nodes ("hubs"). Although the degree distribution of the Shanghai subway system is approximately power-law and it exhibits the general characteristics of a scale-free network, its size is too small to be a true example of a complex network. Nevertheless we see similarities between the subway system and a BA scale-free network in that under random failure both exhibit a second-order phase transition.

B. Robustness results based on vulnerability analysis

We focus on two aspects when we use a vulnerability analysis to quantify the robustness of the Shanghai subway system. Figure 6 shows its vulnerability in terms of the fraction of removed

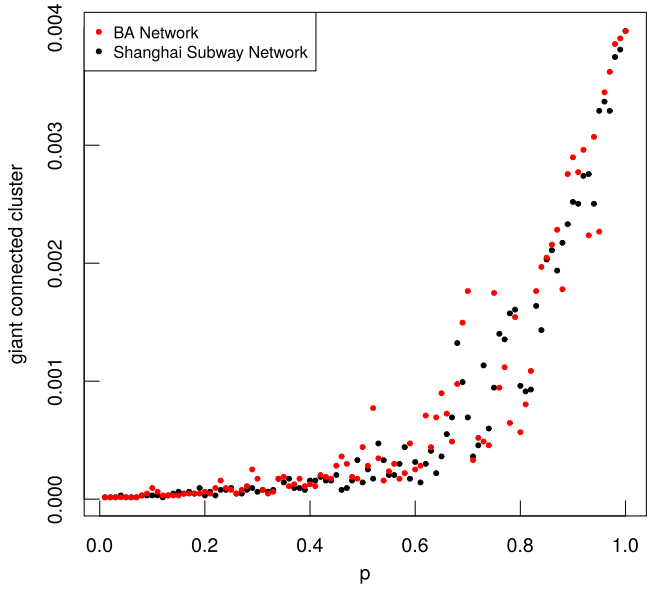

FIG. 4. Ratio of giant connected clusters in dependence of the fraction of removed nodes under random failures.

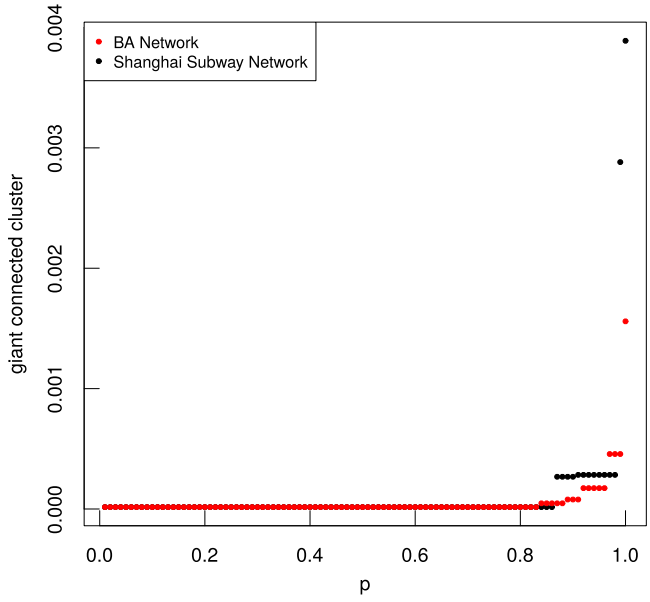

FIG. 5. Ratio of giant connected clusters in dependence of the fraction of removed nodes under deliberate attack.

nodes under random failure and targeted attack. We use the average reciprocal shortest path lengths to measure its performance and calculate its vulnerability. Under both random and targeted failure its performance decreases, but the figure shows that a random removal of nodes causes less damage to the system than a targeted attack. This is case because deliberate attacks target high-degree nodes and thus cause a higher level of destruction.

We now identify the critical areas in the Shanghai subway system and analyze their vulnerability. We use the Modularity algorithm introduced above and generate 16 dense communities in the network that reflect their density and regional importance. These hubs are highly vulnerable, highly susceptible to targeted attack, and—when made to fail—cause widespread damage to the system. Figure 7 shows the vulnerability curves of these critical areas as a function of attack times.

The vulnerability curves produced by different attack areas increase as the attack times increase. Note that with the increase in the number of attacks to critical community areas an increasing number of vertices fail and are removed from the network. System performance decreases and vulnerability values increase, and only a small number of node disruptions can cause area to collapse. For example,

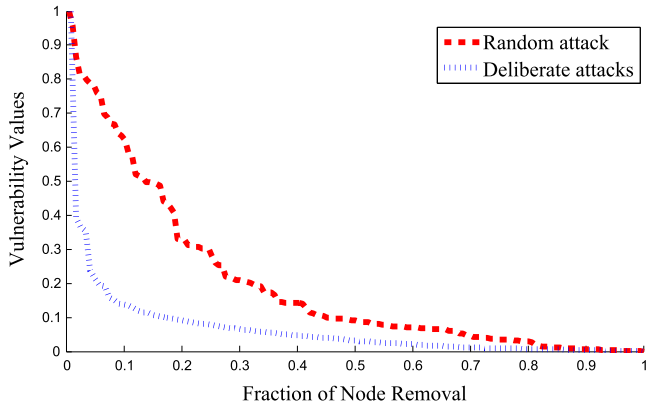

FIG. 6. Vulnerability of Shanghai subway network in dependence of the fraction of removed nodes under random and deliberate attacks.

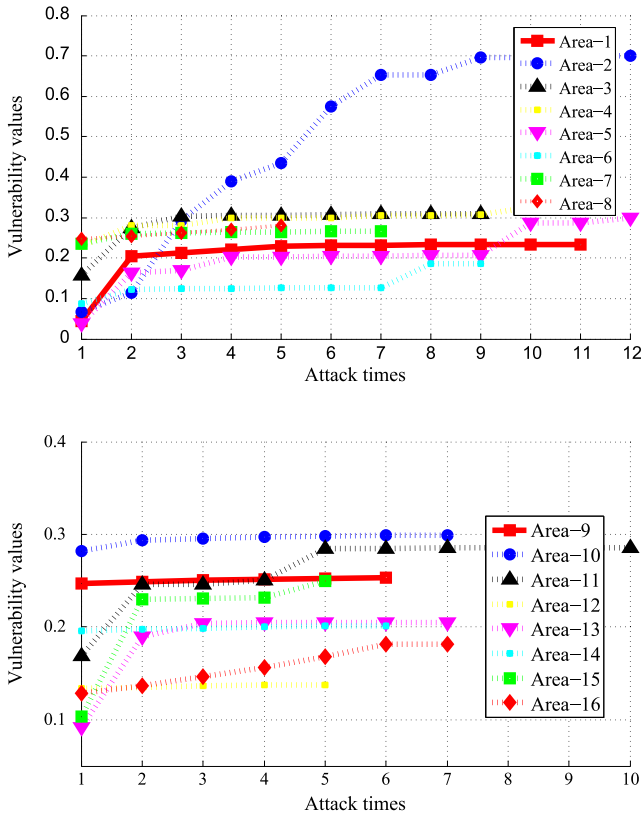

FIG. 7. Vulnerability values produced by different critical areas as a function of attack times.

Area 12 and Area 15 are destroyed completely after only five attacks. Note that some identified critical areas exhibit a higher susceptibility under attack than others.

Figure 8 shows the vulnerability values of different critical areas. Note that these values differ greatly from community to community. Area 16 is located at the periphery of the subway network and generates a relatively small vulnerability value of 0.1813, but Area 2 is located in the interior of the network and generates a very large vulnerability value of 0.7000. Thus disruptions to some of areas cause larger performance disruptions to the network than others. These critical areas, which can cause greater damage, need enhanced protection strategies to reduce their vulnerability.

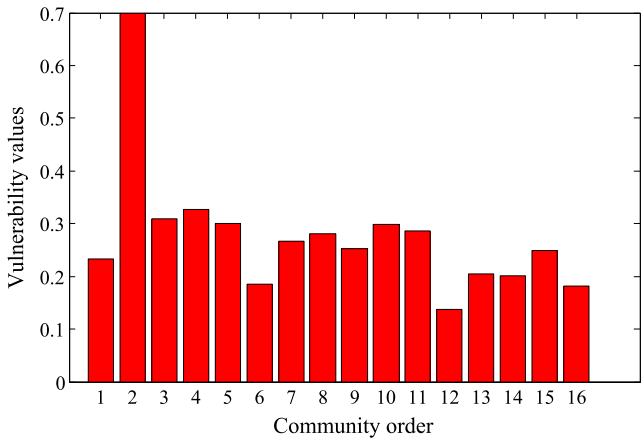

FIG. 8. Vulnerability values of different critical areas.

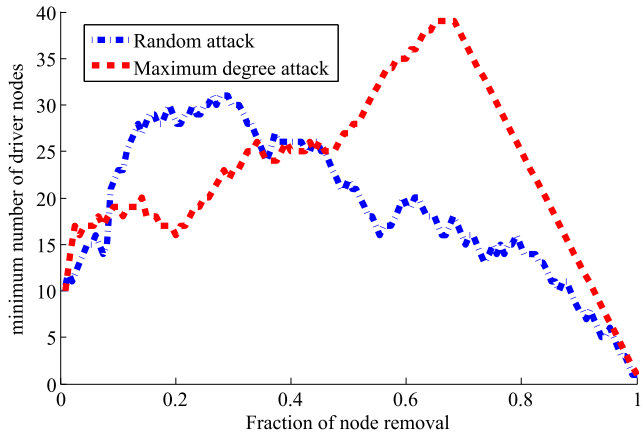

FIG. 9. Minimum number of driver nodes of Shanghai subway network as the function of node removal fraction under random and intentional attacks.

C. Robustness results based on controllability

As the networks are usually confronted with attacks in practice, we investigate the controllability of network under random attack and deliberate attack. We suppose that each node i is assigned with a capacity H_i, and the load L_i is the total number of shortest paths in network passing through the node i. The capacity H_i is identified as follows:

$$H_i = (1 + \alpha)L_i \tag{15}$$

where α is a tolerant parameter. As we remove a fraction of nodes in network, the distribution of shortest paths changes and the loads on some nodes may exceed their capacity. The overloaded node will then fail and there will be a redistribution of loads among the nodes. Finally the cascading stops when there are no more overloaded nodes. We remove all the failed nodes and their connected edges. The topological structure of network is changed after the cascade, and the controllability also changes.

Figure 9 shows that under both random failure and targeted attack the minimum number of driver nodes first increases with the fraction of node removal and then drops to zero. With a small fraction of node removal, an increase in failed nodes requires an increase in driver nodes to maintain full control, but with a large fraction of node removal both the network size and the minimum number of driver nodes decrease. When the fraction of node removal increases to 1, there are no active networks nodes and N_D reduces to 0.

However, the tendency of driver nodes with removal fraction are different under the two attack strategies. The N_D arrives at peak as $f = 0.3$ under random attack, while it arrives at peak as $f = 0.7$ under intentional attack. That is because the driver nodes intend to avoid the high-degree nodes in network, thus the intentional attack removes more non-driver nodes from network. In addition, the cascading failure spreads widely under intentional attack, which leads to more driver nodes to achieve full control than that under random attack.

V. CONCLUSION

Most prior research on network robustness has focused on particular aspects and lacks any integrated approach to network analysis. We examine the Shanghai subway system and propose a multiple perspective method for analyzing network robustness. We consider topological properties and fundamental indices, as well as modes of failure, and we study aspects of network robustness using percolation theory and by analyzing network vulnerability and controllability.

We use percolation theory and carry out a robustness analysis to locate giant connected network clusters and identify phase transition processes. We find that the Shanghai subway system exhibits some scale-free characteristics, including robustness to random failures but vulnerability to targeted

attacks. We analyze network vulnerability and its dependence on the fraction of removed nodes under both random failure and targeted attack. We locate the dense community areas and find they are both the most likely targets for deliberate attack and, when attacked, the strongest propagators of systemic failure cascades. We quantify robustness using controllability analysis and calculate the minimum number of driver nodes, the minimum number of driver nodes presents different tendency with attack strategies and removal fraction after cascades.

Our approach to robustness analysis can be applied to other infrastructure networks and can help decision makers develop optimal protection strategies and infrastructure design. Thus far we have only studied one example of an independent subway system, but because real-world infrastructure systems are interconnected and interdependent, not isolated, in the future we will expand our research and assess the robustness of interdependent infrastructure systems.

ACKNOWLEDGMENTS

This work is jointly supported by National Natural Science Foundations of China (No. 61503166, No. 61763013, No. 11647139), and the Scientific Research Foundation of Chongqing Education Commission (KJ1400329). The science and technology project of Xuzhou (KC16SG253).

[1] C. Nan and I. Eusgeld, "Adopting HLA standard for interdependency study," Reliability Engineering and System Safety **96**, 149–159 (2011).
[2] Y. Yang, Y. Liu, M. Zhou *et al.*, "Robustness assessment of urban rail transit based on complex network theory: A case study of the Beijing Subway[J]," Safety science **79**, 149–162 (2015).
[3] I. B. Utne *et al.*, "A method for risk modeling of interdependencies in critical infrastructures," Reliab. Eng. Syst. Saf. **96**(6), 671–678 (2011).
[4] E. Bompard *et al.*, "Assessment of information impacts in power system security against malicious attacks in a general framework," Reliab. Eng. Syst. Saf. **94**(6), 1087–1094 (2009).
[5] N. Santella *et al.*, "Decision making for extreme events: modeling critical infrastructure interdependencies to aid mitigation and response planning," Rev. Policy Res. **26**(4), 409–422 (2009).
[6] Y. Y. Haimes and P. Jiang, "Leontief-based model of risk in complex interconnected infrastructures," J. Infrastruct. Syst. **7**(1), 1–12 (2001).
[7] L. Hong *et al.*, "Vulnerability assessment and mitigation for the Chinese railway system under floods," Reliab. Eng. Syst. Saf. **137**, 58–68 (2015).
[8] S. Derrible and C. Kennedy, "The complexity and robustness of metro networks," Phys. A: Stat. Mech. Appl. **389**(17), 3678–3691 (2010).
[9] J. Wang *et al.*, "Vulnerability analysis and passenger source prediction in urban rail transit networks," PLoS One **8**(11), e80178 (2013).
[10] E. Rodríguez-Núñez and J. C. García-Palomares, "Measuring the vulnerability of public transport networks," J. Transp. Geogr. **35**, 50–63 (2014).
[11] S. Nie, X. Wang, H. Zhang *et al.*, "Robustness of controllability for networks based on edge-attack[J]," PloS One **9**(2), e89066 (2014).
[12] C. L. Pu, W. J. Pei, and A. Michaelson, "Robustness analysis of network controllability[J]," Physica A: Statistical Mechanics and Its Applications **391**, 4420–4425 (2012).
[13] J. C. Nacher and T. Akutsu, "Structurally robust control of complex networks[J]," Physical Review E **91**(1), 012826 (2015).
[14] Y.-Y. Liu, J.-J. Slotine, and A.-L. Barabási, "Controllability of complex networks[J]," Nature **473**, 167–173 (2011).
[15] X. W. Wang, S. Nie, W. X. Wang *et al.*, "Controlling complex networks with conformity behavior[J]," EPL (Europhysics Letters) **111**(6), 68004 (2015).
[16] T. Jia and A. L. Barabási, "Control capacity and a random sampling method in exploring controllability of complex networks[J]," Scientific Reports 3 (2013).
[17] T. Nepusz and T. Vicsek, "Controlling edge dynamics in complex networks[J]," Nature Physics **8**(7), 568–573 (2012).
[18] J. Ruths and D. Ruths, "Control profiles of complex networks[J]," Science **343**(6177), 1373–1376 (2014).
[19] N. J. Cowan, E. J. Chastain, D. A. Vilhena *et al.*, "Nodal dynamics, not degree distributions, determine the structural controllability of complex networks[J]," PloS One **7**(6), e38398 (2012).
[20] G. Yan, G. Tsekenis, B. Barzel *et al.*, "Spectrum of controlling and observing complex networks[J]," Nature Physics **11**(9), 779–786 (2015).
[21] Y. Yang, Y. Liu, M. Zhou *et al.*, "Robustness assessment of urban rail transit based on complex network theory: A case study of the Beijing Subway[J]," Safety science **79**, 149–162 (2015).
[22] L. K. Gallos, R. Cohen, P. Argyrakis *et al.*, "Stability and topology of scale-free networks under attack and defense strategies[J]," Physical Review Letters **94**(18), 188701 (2005).
[23] X. Chen, R. Wang, M. Tang *et al.*, "Suppressing epidemic spreading in multiplex networks with social-support[J]," arXiv preprint arXiv:1708.02507, 2017.
[24] X. Chen, C. Yang, L. Zhong *et al.*, "Crossover phenomena of percolation transition in evolution networks with hybrid attachment[J]," Chaos: An Interdisciplinary Journal of Nonlinear Science **26**(8), 083114 (2016).
[25] J. Shao, S. V. Buldyrev, L. A. Braunstein *et al.*, "Structure of shells in complex networks[J]," Physical Review E **80**(3), 036105 (2009).

[26] X. Huang, J. Gao, S. V. Buldyrev *et al.*, "Robustness of interdependent networks under targeted attack[J]," Physical Review E **83**(6), 065101 (2011).
[27] S. Wang, J. Zhang, M. Zhao *et al.*, "Vulnerability analysis and critical areas identification of the power systems under terrorist attacks[J]," Physica A: Statistical Mechanics and Its Applications **473**, 156–165 (2017).
[28] A. Clauset, M. E. J. Newman, and C. Moore, "Finding community structure in very large networks[J]," Physical Review E **70**(6), 066111 (2004).
[29] M. Girvan and M. E. J. Newman, "Community structure in social and biological networks[J]," Proceedings of the National Academy of Sciences **99**(12), 7821–7826 (2002).
[30] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," Nature **464**(7291), 1025–1028 (2010).
[31] A.-L. Barabási, "The network takeover," Nat. Phys. **8**, 14–16 (2011).
[32] S. H. Strogatz, "Exploring complex networks," Nature **410**, 268–76 (2001).
[33] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," Rev. Mod. Phys. **74**(1), 47–97 (2002).