2018 IEEE International Conference on Software Quality, Reliability and Security Companion

How does node resilience effect on complex networks?

Qiang Dong, Chong Jin, Ruiying Li*, Rui kang
Science and Technology on Reliability and Environmental Engineering Laboratory
School of Reliability and System Engineering,Beihang University
Beijing 100191, China
liruiying@buaa.edu.cn

***Abstract*—Resilience, the ability of the system to withstand disruption and return to a normal state quickly, is an important and challenging issue in complex networks since both internal failures and external disturbances are inevitable and they may cause complete collapse of network systems. Researchers have analyzed the resilient behavior of complex networks from different points of view. Usually, the resilience of complex networks is measured using network topology related parameters, such as node degree, node betweenness and network clustering coefficient. Using these resilience measures, the resilience of network topology can be evaluated. However, networks are used to transmit data or material, so we focus on the flow transmitted on the network in this paper. The resilience is measured based on the quantity of flow. Different from previous studies, this paper considers that both the system and its nodes have multiple states and have resilience behaviors. To analyze how the resilience of nodes effects on that of the system, both random and three types of intentional attacks are simulated on nodes of both random networks and scale-free networks, respectively. Simulation results show how the network resilience changes along with the number of disturbed nodes and the node attack intensity. The relationship between the resilience of nodes and network is also discussed.**

Keywords—resilience; complex network; tranfic model; random network; scale-free network

I. INTRODUCTION

Complex network is a hot topic in recent years. World-Wide-Web, transport networks and power grids are typical complex networks. The system's behavior is determined by the performance and constitute of its components. Consequently, failures on nodes will influence the network, and some may even lead the whole network to break up. Because failures on nodes are hard to avoid, the 'resilience', which describes the ability of a system to withstand disruption and return to normal state quickly, has gained more and more attention. There are also an increasing number of studies about resilience of complex network.

Resilience is a system performance based measure. According to previous studies on the measurement of complex network resilience, most researchers regarded the topological parameters as the resilience metrics and studied the changing process of these topological metrics after attack. Two kinds of network topological parameter are usually used. One is based on the number of nodes, such as scale of network, the other is based on the path length, such as network efficiency. Zhao et al. [1] used supply availability, the size of the largest functional sub-network and the average supply-path lengths in the largest functional sub-network as resilience metrics to analyze the network's behavior with different network topologies under both random and deliberate attack. Osei-Asamoah and Lownes [2] used global efficiency and the relative size of giant component as the resilience metrics. They studied the topologic resilience of a biological network in bacteria and a transport network in Connecticut and India. Dong et al. [3] analyzed the resilience of power grids in Korea. The network efficiency was regarded as the key performance metric in the process of network cascading failure and recovery. Berche et al. [4] also used the size of the largest giant component as the metric to measure the resilience of complex network. In complex network resilience studies based on topological parameters, nodes are considered to have only two states, either normal or fault.

Considering that topology parameters can only reflect the physical connection of the network and cannot reflect the transmission capability of the network, some researchers have begun to study the resilience from the perspective of network transmission performance. Wang and Ip [5] provided a two-level resilience evolution for supply chain network. They defined the node resilience as the ratio of the available and reliable suppliers over the demand. They also provided a method to calculate the resilience of logistic network with the weighted sum of the node resilience. Based on the same idea, Ip and Wang [6] evaluated the resilience of transport network by calculating the weighted sum of node resilience. Ren et al. [7] considered the influence of recovery strategies to the complex network resilience and used failure rate and the number of recovery nodes to evaluate network resilience. However, these studies only concentrated on the network recovery process, and the ability of network to withstand disturbance were not taken into consideration. Garbin and Shortle [8] used the percent of damaged function path in network to evaluate resilience. Omer et al. [9] compared the ratio of information transfer volume before and after disturbance. They calculated the ratio to evaluate the resilience of network system. Farahmandfar et al. [10] combined the robustness and redundancy of water supply network to evaluate resilience. Studies above used the ability of network to withstand disturbance and the ability to recover after disturbance to define resilience. However, some details about network recovery process is lack. Note that, in the above complex network resilience studies base on transmission performance, nodes are also regarded to have two states. The performance degradation of nodes is not taken into consideration.

978-1-5386-7839-8/18/$31.00 ©2018 IEEE
DOI 10.1109/QRS-C.2018.00057

The current research on the resilience of complex networks has the following characteristics:

1) Most studies used topological parameters based resilience metrics, and a few research applied transmission performance based ones. The latter can better reflect the complex network transmission capabilities, and related research has received more and more attention.

2) Most studies only analyzed the resilience behavior of the network system, neglecting the resilience behavior of the node (regard that the node has only two states), and did not analyze the impact of component resilience on the system resilience.

To solve these problems, this paper analyzes the relationship between the resilience of the complex network system and that of the network node. The ratio of the system performance integral before and after the attack are used to calculate the resilience of both network and node [11]. This metric considers the network's ability to resist interference or attacks and the ability to recover from interference or attacks.

Using simulation, the relationship between node resilience and system resilience are analyzed for two types of networks (random network and scale-free network) under four types of attacks (random attack, degree-based attack, betweenness-based attack, and traffic-based attack). Result show that networks with different topologies behave differently under the different attack strategy.

II. Problem Description

A. Network Topology

The topology form is the foundation of the network. This paper studies two typical complex network topological models—ER random network [12] and BA scale-free network [13]. Among them, the ER random network is a completely random network model, the probability of edge connection between any two nodes is the same, and its degree distribution function can be represented by Poisson distribution. The BA scale-free network is a structure where only a few nodes have a large number of connections and the degree graduations conform to the power law distribution. Compared with the random network, the BA scale-free network reflects that the complex network has a high degree of heterogeneity, and the connection status (degrees) between nodes has a serious uneven distribution.

B. Traffic Model

We assume that the transmission capacity of the network link is infinite, and each node in the network has a fixed transmission capacity C. A node can transmit a fixed number of data packets in a certain time interval. In this model, all nodes can both generate and forward data packets. The network transmission process follows the traffic model in [14-15], which is popular in network related studies. At each moment, data packets are randomly generated in the network at a fixed rate R. Both the new generated data packets and those already existed on the network are transmitted according to the network routing policy. The packet are deleted after it reaches the destination node. The data packet obeys the first-in, first-out rule on the node. In this paper, we use the shortest path routing strategy that is widely used in actual networks.

C. Network Performance Measure

Resilience is calculated based on the performance of the system. In this paper, node traffic load and network traffic load are regarded as the key performance index. The attacks will reduce the transmission capacity of nodes, and the performance changes are used to calculate the resilience of nodes and networks. The traffic load is defined as the number of data packets at node and the whole network at each time point. The traffic load of nodes can be obtained as $W_i(t)\left(i=1,2,\cdots,\mathrm{N}\right)$, and that of network can be computed as

$$W_n(t)=\sum_{i=1}^{N}W_i(t) \tag{1}$$

These two kinds of traffic load are small-the-better performance parameter, and we use their inverses to normalize the performance as follows:

$$Q_i\left(\mathrm{t}\right)=\frac{1}{W_i\left(t\right)},\quad (i=1,2,\cdots,\mathrm{N}) \tag{2}$$

$$Q_n\left(\mathrm{t}\right)=\frac{1}{W_n\left(t\right)}=\frac{1}{\sum_{i=1}^{N}W_i(t)} \tag{3}$$

III. Method

A. Resilience Measurement

The resilience measures the ability of the system to withstand the disruption and recovery quickly. Li et.al. [11] proposed a resilience evaluation method based on performance integrals. This method introduced the maximum allowable recovery time determined by users, and used the integral of normalized performance to evaluate resilience within such time interval. Considering that the network performance may also change under normal conditions, this paper uses the following resilience measurement:

$$\mathbb{R}_D=\frac{\int_{t_0}^{t_0+T^*}Q(t)dt}{\int_{t_0}^{t_0+T^*}Q_0(t)dt} \tag{4}$$

Where $Q_0(t)$ is the normalized performance of the system at time t under normal state (without disturbance), and $Q(t)$ is the normalized performance at time t after the disruption occurs, t_0 is the start time of the disturbance, and T^* is the maximum allowable recovery time determined by users. By adding the

parameter T^*, the resilience of different systems are comparable as the time scales measured in resilience are consistent. The area of residual performance also reflects the system's ability to absorb, adapt, and recover from disruption.

In the simulation, we can only obtain the discrete performance values, and the trapezoidal method is used to compute the resilience

$$\mathbb{R}_D \approx \frac{\sum_{k=1}^{m}[Q(t_k)+Q(t_{k-1})]}{\sum_{k=1}^{m}[Q_0(t_k)+Q_0(t_{k-1})]},\ m=\frac{T^*}{\Delta t} \tag{5}$$

Where t_k is the kth time point in time period, $T^*$and $Q(t_k)$ are the normalized performance of system after and before the disruption respectively at time t_k.

B. Disruption Generation and Simulation

In order to measure the resilience of nodes and networks under different disturbances of ER network and BA network, the following two types of attack strategies are defined: random attacks and deliberate attacks [3], where three types of deliberate attack are considered, including degree-based attack, betweenness-based attack and traffic-based attack.

Random-attack: the nodes are attacked randomly in the network during the disturbance.

Degree-based attack: the probability that nodes are attacked is determined by their degree, and nodes with higher degree have larger probability to be attacked.

Betweenness-based attack: similar to the degree-based attack, only the attack probability of nodes is determined by their betweenness.

Traffic-Based Attack: similar to both degree-based and betweenness-based attack, the attack probability of nodes is determined by the average traffic load on them.

In the simulation, we first operate the network normally, and record the traffic loads of all nodes within the user determined maximum allowable recovery time. Then, we use the above attack strategies to attack the nodes in the network and reduce the node's transmission rate. After a few moments, recover those attacked nodes back to the normal state. We record the traffic load of all nodes within time T^*, and then evaluate the resilience. The simulation process is as follows:

- Create an ER random network or BA scale-free network with a specified network size;
- Determine the initial packet generation rate R and node forwarding rate C, implement the traffic load model mentioned in section II, and then perform the simulation;
- Record the traffic loads of all nodes under normal state;
- Generating attack using strategies mentioned above, and the transmission rate of these attacked nodes will be reduced. Then, recover the attacked nodes after a few time steps, and the transmission rate will return back. Record the traffic load of all nodes after attack until T^* is achieved;
- Evaluate the resilience. With the traffic flow of all nodes before and after the attacks, compute the network resilience using Eqs. (1-3,5).

IV. Result and Discussion

For ER random network and BA scale-free network with node number N=100, the resilience of them are evaluated under the traffic load model described in section II and attack strategies and the simulation process described in section III. To make the transmission density similar, we set different data packet generation rates, i.e., R_{ER}=20, R_{BA}=40, and the same node forwarding rate C=4. Under such packet generation rate, the network traffic is maximized in those which will not make the network congested at the initial state. After that, using different attack strengths (the node's transmission rate drops to C=1,1.25,1.5,...,3.75 after the attack) and different attack scales (the number of attacked nodes M=1,2,3,...,10), we analyze the resilience of ER and BA networks under four attack strategies.

A. ER Network

We studied the resilience of ER networks with connection probability p=0.08. The network resilience evaluation results are shown in Fig. 1, and we can see that the network resilience under different attack strategies vary greatly. The network is more sensitive to traffic-based attacks and less sensitive to random attacks.

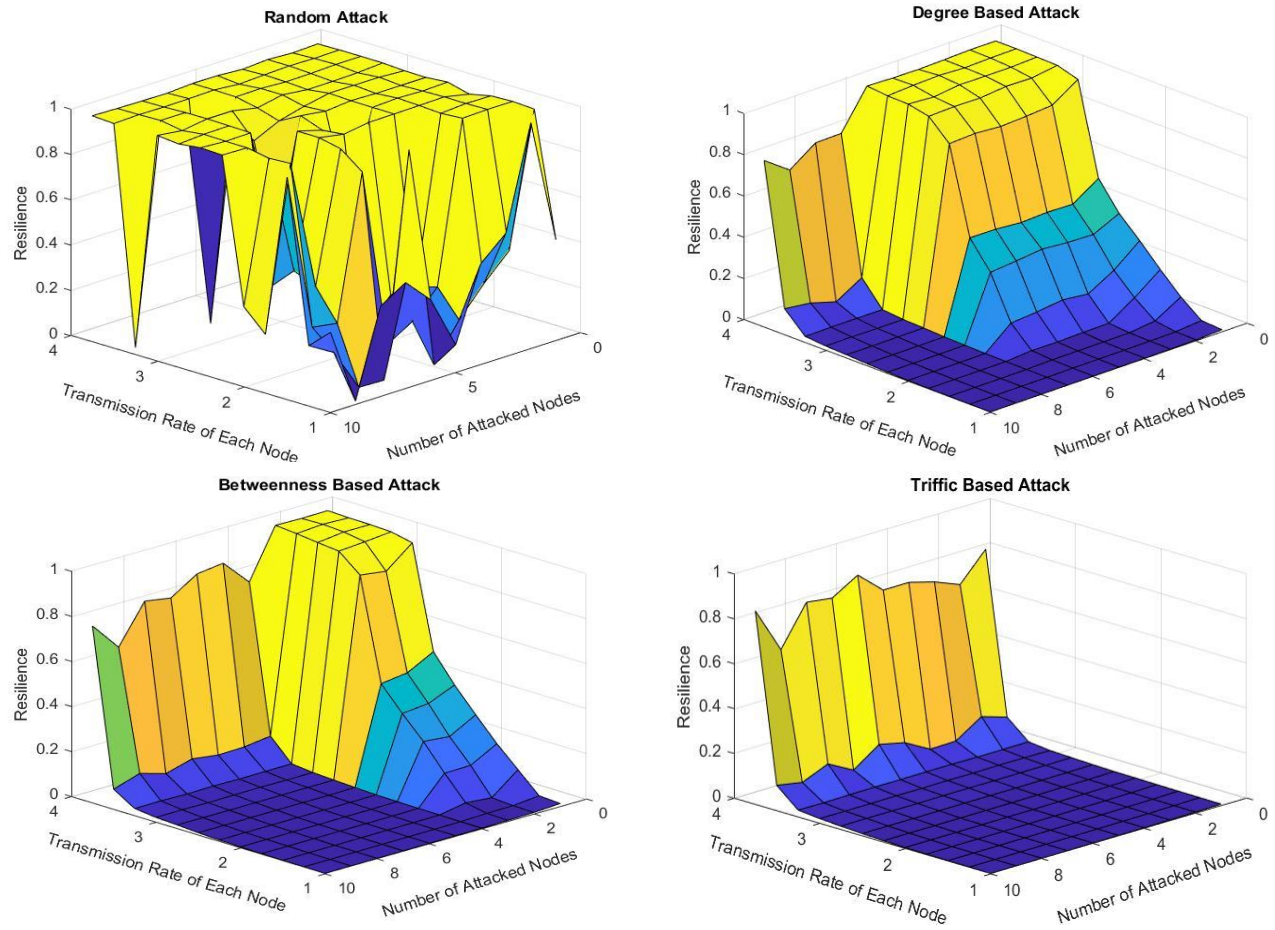

Fig. 1. Resilience evaluation result of ER random network

Under random attack, the resilience of ER networks behaves randomly. This is because each node in the network has a different influence on network resilience. If the important nodes are attacked, small performance degradation of them can lead a great impact to the network. If those unimportant nodes are attacked, even large performance degradation on them has negligible impact on the network. From Fig. 1, we can also see that with the increasing number of attacked nodes and/or performance degradation of attacked nodes, the probability that the network resilience is low gradually increases. This phenomenon shows that the attack strength and scale have a direct impact on network resilience.

Under the three types of deliberate attack, when the network node's transmission rate drops below 2.75, the network resilience changes significantly. For the degree-based attack, the betweenness-based attacks, and the traffic-based attack, when the number of attacked nodes is greater than 6, 3, 0 respectively, the network resilience is nearly 0. It shows that, it is not accurate to use degree of nodes to describe their influence to network resilience. In contrast, the nodes with high traffic are with larger importance to the network resilience. Attacking these nodes can effectively reduces the network resilience.

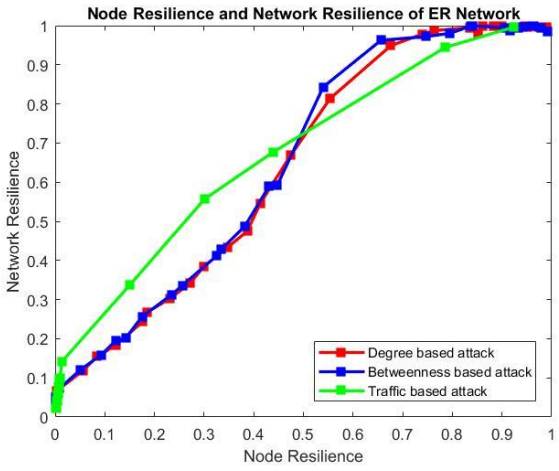

Fig. 2. Network resilience and node resilience of ER network

Base on the results above, we analyze the influence of resilience of nodes to that of network. As the network resilience under random attack is unstable, we only analyze the resilience of network and nodes under deliberate attack. Fig. 2

shows how the network resilience changes along with the node resilience when only one node is attacked. We can see that the two curves of network resilience under the degree-based and betweenness-based attack strategies are similar. When the node resilience is low, the curves are nearly a straight line. After that, with the increasing of node resilience, the network resilience rises quickly. Besides, when the node resilience rises to 0.7, the network resilience is close to 1.0, and the increasing rate of network resilience becomes low again. On the other hand, the curve of ER network under traffic-based attack is very different. When the node resilience is low, the resilience of network increasing quickly with that of node. After that, the increasing rate of the network resilience continues coming down. When the resilience of nodes approaches 0.9, the resilience of network is almost 1.0.

B. BA network

For the BA scale-free network in this study, the number of initial nodes is 4, and the number of added nodes in each step is 2. The results of network resilience under the 4 types of attacks are shown in Fig.3.

As same as the ER network, the BA network is highly sensitive to deliberate attacks. Under random attacks, resilience of network is also relevant to attack intensity and attack scale, and the value of resilience is random. The following part mainly analyzes the differences between the resilience behaviors of two networks.

Under degree-based attack and/or betweenness-based attack, the resilience of BA network performs the same pattern as the ER network. When the node's transmission rate drops below 2.75, the resilience of network declines sharply. Different from the random network, when the number of attacked nodes is greater than 2, the resilience of BA network becomes very low. In a ER network, more nodes needs to be attacked to cause a rapidly decrease of the network resilience. These rules show that, degree-based attack and betweenness-based attack are highly effective in a scale-free network compared with a random one. Combining the heterogeneity of the BA network, it can be concluded that the degree, betweenness, and traffic load importance of BA network nodes are highly consistent. A node with high structural importance in a BA network has high probability to be a performance critical node, which is highly different from ER network.

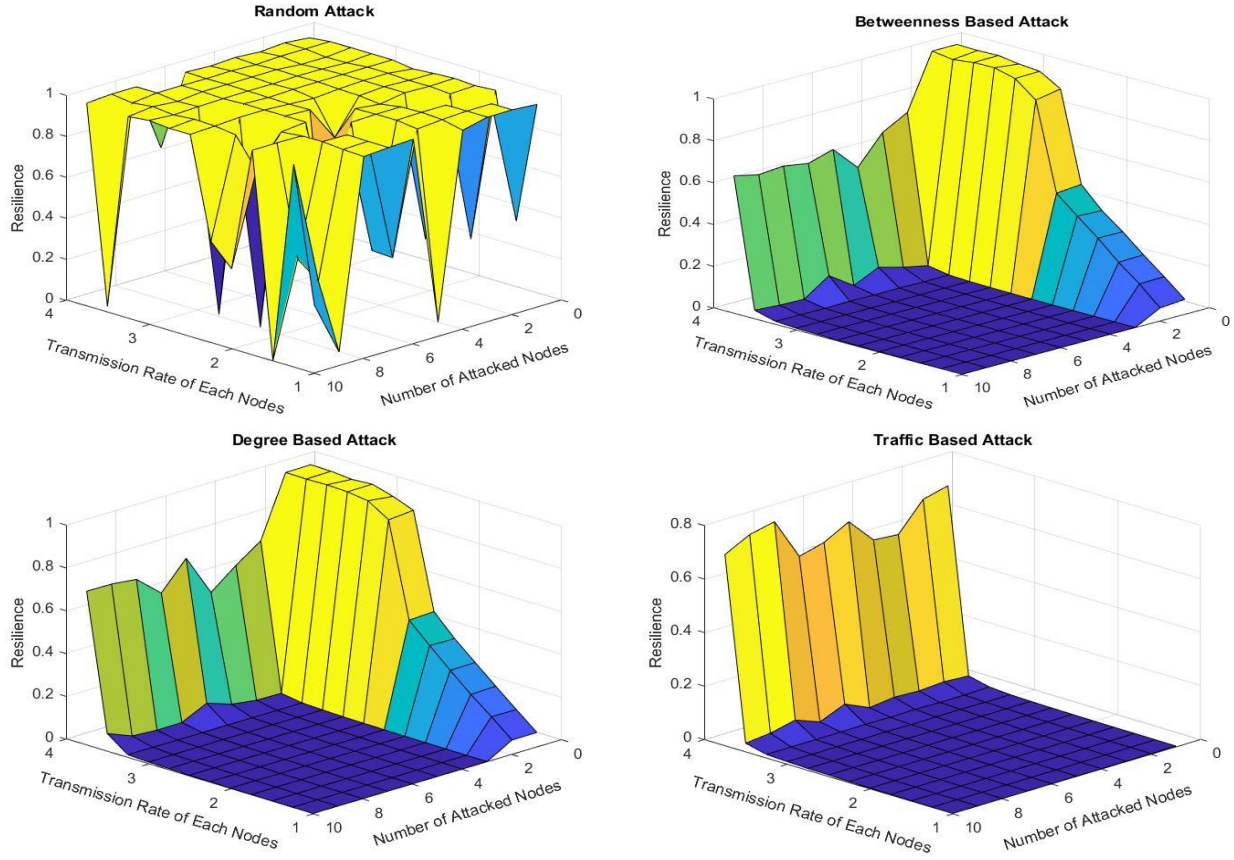

Fig. 3. Resilience evaluation result of ER random network

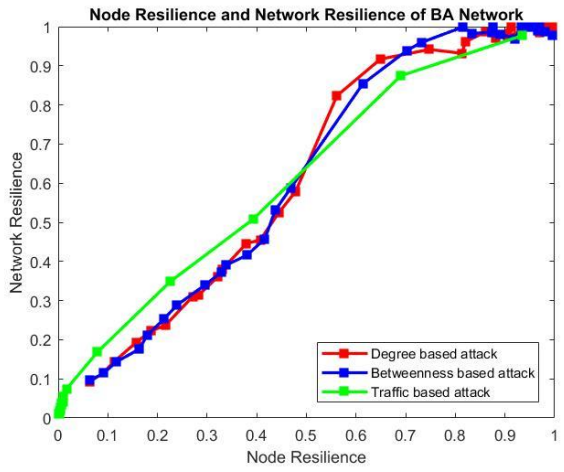

Fig. 4. Node resilience and network resilience of BA network

Base on the results above, the influence of nodes resilience on network resilience in BA network is also analyzed. Based on the same reason as ER network, random attack is neglected in this part. The results are shown in Fig. 4.

From Fig. 4, we can see that the trends of three curves are similar to those in Fig.2. It means that the rules of how the resilience of node influence on that of the network in the two different networks are same. The only difference is, the curve which shows the relationship between network resilience and node resilience is nearly a straight line under the traffic-based attack. Some possible explanations about the curves in Fig.2 and Fig.4 are as follow. There are some redundancies in ER and BA network under degree-based attack and betweenness-based attack. Therefore, when the resilience of node starts declining, the resilience of network still keeps on a high level. However, the redundancies are limited. When the resilience of node continues declining, the resilience of network declines sharply and remains a same trend as the resilience of node. Two networks are both sensitive to traffic-based attacks, therefore, the change rate of network resilience is similar to that of node resilience. The BA network is more sensitive to traffic-based attack, because the curve of BA network under traffic-based attack is nearly a straight line which means network resilience is approximately equal to node resilience all the time.

V. CONCLUSION

In this paper, we analyze how the resilience of nodes effects on that of complex networks. Traffic load is determined as the key performance parameter to evaluate both network and node resilience. Network behaviors are simulated using traffic flow model on both ER random network and BA scale-free network of the same scale, and four types of attacks, random attack, degree based attack, betweenness based attack and traffic based attack, are analyzed. The contributions of this study are as follows: (1) the nodes in network are regarded as multi-status components, which are usually considered as components with only two status (i.e., failed and normal) before; and (2) Simulation results show that the resilience of BA network is more sensitive to degree based attack and betweenness based attack than ER network. More details about this topic will be analyzed in our further studies.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (61773044) and Graduate Innovation Practice Foundation of Beihang University (YCSJ-02-2017-08).

REFERENCES

[1] K. Zhao, A. Kumar, T.P. Harrison, and J. Yen, "Analyzing the Resilience of Complex Supply Network Topologies Against Random and Targeted Disruptions," IEEE Systems Journal, vol. 5, pp. 28-39, January 2011.

[2] A. Osei-Asamoah and N. Lownes, "Complex Network Method of Evaluating Resilience in Surface Transportation Networks," Transportation Research Record: Journal of the Transportation Research Board, vol. 2467, pp. 120-128, December 2014.

[3] D.H. Kim, D.A. Eisenberg, Y.H. Chun and J. Park, "Network topology and resilience analysis of South Korean power grid," Physica A: Statistical Mechanics and its Applications, vol. 465, pp. 13-24, January 2017.

[4] B. Berche and C. von Ferber, "Resilience of public transport networks against attacks," The European Physical Journal B, vol. 71, pp. 125-137, September 2009.

[5] D. Wang and W.H. Ip, "Evaluation and analysis of logistic network resilience with application to aircraft servicing," IEEE Systems Journal, vol 3, pp. 166-173, June 2009.

[6] W.H. Ip and D. Wang, "Resilience and friability of transportation networks: evaluation, analysis and optimization," IEEE Systems Journal, vol 5, pp. 189-198, June 2011.

[7] F. Ren, T. Zhao, and H. Wang, "Risk and resilience analysis of complex network systems considering cascading failure and recovery strategy based on coupled map lattices," Mathematical Problems in Engineering, vol. 2015, July 2015.

[8] D.A. Garbin and J. F. Shortle, "Measuring resilience in network-based infrastructures," Critical Thinking: Moving from infrastructure protection to infrastructure resilience, 2007.

[9] M. Omer, R. Nilchiani and A. Mostashari. "Measuring the Resilience of the Trans-Oceanic Telecommunication Cable System," IEEE Systems Journal, vol. 3, pp. 295-303, September 2009.

[10] Z. Farahmandfar, K.R. Piratla and R.D. Andrus. "Resilience Evaluation of Water Supply Networks against Seismic Hazards," Journal of Pipeline Systems Engineering and Practice, vol. 8, July 2016

[11] R. Li, Q. Dong, C. Jin and R. Kang, "A New Resilience Measure for Supply Chain Networksm," Sustainability, vol. 9, July 2016.

[12] P. Erds, and A. Rényi, "On the evolution of random graphs," Publ. Math. Inst. Hung. Acad. Sci, vol. 5, pp. 17-61, 1960.

[13] A.L. Barabási and R. Albert, "mergence of scaling in random networks," science, vol. 286, pp. 509-512, October 1999.

[14] B. Tadić, S. Thurner and G.J. Rodgers, "Traffic on complex networks: Towards understanding global statistical properties from microscopic density fluctuations," Physical Review E, vol. 69, March 2004.

[15] G. Mukherjee and S.S. Manna, "Phase transition in a directed traffic flow network," Physical Review E, vol. 71, June 2005.