Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2013, Article ID 938398, 10 pages
http://dx.doi.org/10.1155/2013/938398

Research Article

Identifying Vulnerable Nodes of Complex Networks in Cascading Failures Induced by Node-Based Attacks

Shudong Li,[1,2] Lixiang Li,[3] Yan Jia,[2] Xinran Liu,[4] and Yixian Yang[3]

[1] *College of Mathematics and Information Science, Shandong Institute of Business and Technology, Shandong, Yantai 264005, China*
[2] *School of Computer Science, National University of Defense Technology, Hunan, Changsha 410073, China*
[3] *Information Security Center, Beijing University of Posts and Telecommunications, P.O. Box 145, Beijing 100876, China*
[4] *National Computer Network Emergency Response Technical Team/Coordination Center, Beijing 100029, China*

Correspondence should be addressed to Lixiang Li; li_lixiang2006@163.com

Received 18 July 2013; Accepted 7 August 2013

Academic Editor: Ming Li

In the research on network security, distinguishing the vulnerable components of networks is very important for protecting infrastructures systems. Here, we probe how to identify the vulnerable nodes of complex networks in cascading failures, which was ignored before. Concerned with random attack (RA) and highest load attack (HL) on nodes, we model cascading dynamics of complex networks. Then, we introduce four kinds of weighting methods to characterize the nodes of networks including Barabási-Albert scale-free networks (SF), Watts-Strogatz small-world networks (WS), Erdos-Renyi random networks (ER), and two real-world networks. The simulations show that, for SF networks under HL attack, the nodes with small value of the fourth kind of weight are the most vulnerable and the ones with small value of the third weight are also vulnerable. Also, the real-world autonomous system with power-law distribution verifies these findings. Moreover, for WS and ER networks under both RA and HL attack, when the nodes have low tolerant ability, the ones with small value of the fourth kind of weight are more vulnerable and also the ones with high degree are easier to break down. The results give us important theoretical basis for digging the potential safety loophole and making protection strategy.

1. Introduction

In modern society, people's life depends on the infrastructure networks more and more, such as the power grid, Internet, transportation networks and the financial networks, and so forth. The overall efficiency of these network systems is being increased, while the internal connections and the dynamical characteristics within the networks are becoming more close and complex, respectively. These behaviours make the networks more vulnerable and increase the possibility of system crash. Especially, with the improvement of netware-based degree, a small incident, through a cascade of reaction, can lead to the collapse of the whole network systems and a great number of economic loss. The typical example is the accident that emerged in the power grid of North America in 2003 [1]. The fault of three extra-high voltage transmission lines leads to a chain reaction in power system, spreads to the eight states in the northeast U.S., affects about 50 million people, and finally results in the economic loss of 4 billion to 10 billion. Another example is the electrical collapse that occurred in Italy [2], which has seriously influenced the operation of the Internet.

These large-scale accidents have threatened the network safety and attracted considerable attentions of scientific researchers [3]. On the one hand, The robustness and vulnerability of topological structure of complex networks are investigated carefully. Some indexes are proposed to measure how robust or vulnerable the complex networks are under different attacks [4–6]. The structural vulnerability of the important real-world networks is also probed, including Italian electrical network [7], the US power grid [8], the European grid [9], and other electrical systems [10] and

the robustness of computer networks under attacks [11], the stability analysis for the uncertain systems [12–14], and the cyber-physical networking systems [15].

On the other hand, there exist the physical flows (also defined as load) in real-world networks, such as the electric stream in power grids, the data transmitted in communication networks, and the cars in transportation networks. Also, the physical load is dynamical. The fault of some local components (nodes or edges) always leads to the redistribution of load over the whole networks. Then, the overloaded components will fail as the new load on them exceeds their capacity (the maximum load). Therefore, the new redistribution of load over the whole networks will begin and lead to the cascade over the networks. This evolving procedure is called "cascading failure" which emerged locally and always resulted in the whole collapse of networks. Therefore, the cascading failures of complex networks have been one of the hottest topics in network safety. Induced by random breakdown and intentional attack, Motter explored the condition of cascading failures occurring in complex networks [16]. The similar procedure of load redistribution included the works [17–20]. For the local redistribution of load on nodes or edges, the cascading dynamics due to node overloaded breakdown in US power grid [21] and the edge overloaded breakdown in scale-free networks [22] are investigated, respectively. Also, the condition of cascading failures in weighted networks under edge-based attack is analyzed carefully [23], where the redistribution of load on edges is similar to the process [22]. Then, the influence of different definitions of load on cascading failures in weighted complex networks is probed to reduce the possibility of cascading failures [24]. The features and time characteristics shown in cascading failures are revealed [25]. In addition, recently, considering that the networks in real world are interdependent and internally connected, the cascading propagation in the interdependent networks is investigated [26–29] and the robustness and critical effect of networks are also explored carefully [30, 31].

All the previous researches mainly focus on the structural vulnerability or the cascading dynamics of the integral complex networks. However, in the cascading failures caused by overloaded breakdown, the following important problems have not been considered. What features do the nodes easy to break down or crash have? How should we describe the characteristics of the congested node in complex networks? These problems are the correlations between the vulnerability of nodes and the cascading failures in complex networks. We argue that, by exploring this problem, we are able to identify the vulnerable nodes, analyze the potential safety hazard in networks, and find the bottlenecks in the dynamical change of network "flows". Finally, it can provide the important theoretical basis for protecting complex networks and improving the robustness of real-world networks.

Here, this paper explores the correlations between the vulnerability of nodes and the cascading failures in complex networks. Firstly, by assigning the load on nodes, we model the cascading dynamics of complex networks induced by random attack and intentional attack on nodes. Secondly, we introduce four kinds of weighting methods to describe the characteristics of the nodes in complex networks including BA scale-free networks (SF), WS small-world networks (WS), ER random networks (ER), and two real-world networks (autonomous system network and US airport network). Finally, in order to identify the features of the vulnerable nodes in complex networks, we numerically computed the ratio of the failed nodes with four kinds of weights less than their respective average weights to the total failed ones in networks. As a result, we find that, for SF network under intentional attack, the ratio of the failed nodes with small value of the fourth kind of weight defined here is the highest. The autonomous system network with power-law distribution also shows similarity to SF network. It reveals that the nodes with small value of the fourth kind of weight defined in this work are more vulnerable. Moreover, for the WS small-world network and ER random network, under both random and intentional attack, when the tolerance ability of nodes is low, the ratio of the failed nodes with small value of the fourth kind of weight is higher, and, at the same time, the ratio of the failed ones with high degree is also higher. It means that the nodes with smaller value of the fourth kind of weight and large degree are vulnerable and the nodes with large degree are also vulnerable.

The rest of this paper is organized as follows. Section 2 develops the model of cascading dynamics of complex networks induced by random attack (RA) and highest load attack (HL) on node. In Section 3, we introduce four kinds of weighting methods to characterize the nodes in complex networks in order to distinguish them. In Section 4, we describe the studied complex networks including BA scale-free network, WS small-world networks, ER random network, and two real-world networks. In Section 5, we simulate and analyze the characteristics of the failed nodes of complex networks in cascading failures. Section 6 summarizes the most important contribution of this paper and points out the meaning of this work.

2. Modelling the Cascading Failures in Complex Networks

In this section, we will model the cascading dynamics of complex networks under node-based attacks. For a general undirected network comprising of N nodes, its adjacent matrix is defined as $A = (a_{ij})_{N\times N}$, where $a_{ij} = 1$ if the node i links to node j; otherwise, $a_{ij} = 0$. Usually, modelling cascading dynamics of complex networks is based on the following three key points [19–23]: the definition of load on node, the relationship between the load and the capacity, and the evolving procedure of cascading failures.

(1) The definition of load on node: usually, the physical flows (data packets, energy, etc.) are transmitted in many networks according to the shortest path routing strategy [1, 3, 16, 17]. For a given pair of nodes (a, b), the physical flows are exchanged and transmitted along the shortest paths connecting them; maybe there exist some shortest paths through node i. In this case, it is natural to regard the total number of shortest paths passing through the node i between any pair of nodes in a network as the load on node i. Therefore,

we define $L_i(t)$ as the load on node i, where $L_i(t)$ is the number of the shortest paths passing through node i at some time t after attacks ($t = 0$ means the initial load $L_i(0)$ before attack).

(2) The relationship between the load and the capacity: usually, there is some maximum load (the maximum capacity) that node i can handle. So, we assume that the maximum load C_i on node i is proportional to its initial load $L_i(0)$; namely,

$$C_i = (1 + \alpha) L_i(0), \quad \forall i, \tag{1}$$

where the constant $0 \leq \alpha \leq 1$ is the tolerance parameter. The bigger α means the higher capacity of node i and then the higher ability against failures. It is a rational definition in the design of real-world networks including power grids and Internet because the capacity of the components (nodes or links) in these networks is always limited by the cost.

(3) The evolving procedure of cascading failures: beginning with the removal of some nodes in networks, the load on other nodes will change and be redistributed over the whole networks. At some time t, the node j will fail if the new load $L_j(t)$ on j exceeds its capacity C_j. This will cause the new redistribution of load over the networks. This process is iterated until there is no node exceeding their capacity. At this time, the iterative process can be regarded as being completed. This iterative process is called "cascading failures" in complex networks, which is described in Figure 1.

Here, we consider two kinds of attack strategies.

(1) Random attack (RA): we choose some proportion of nodes randomly and then remove them from the networks; here we assume the proportion $\rho = 0.01$. This attack mainly simulates the case of complex networks subject to some random breakdown, such as the natural disasters, misoperations and random disturbances, and so forth.

(2) Highest load attack (HL): first, we descend the order of nodes according to the initial load $L_i(0)$ and then remove some proportion of nodes with the highest initial load; here, the proportion $\rho = 0.01$. This attack simulates the case of the intentional attack.

3. The Weighting Methods of Nodes in Complex Networks

In order to identify the vulnerable nodes of complex networks in cascading failures, in this paper, we introduce four kinds of weighting methods $w_i^{(1)}$, $w_i^{(2)}$, $w_i^{(3)}$, and $w_i^{(4)}$ to describe the characteristics of nodes in complex networks. These quantities can distinguish the failed nodes in cascading failures.

(1) The Weighing Method $w_i^{(1)}$. Considering that we assume the load (physical flows) is transmitted according to the shortest path strategy, while the initial load $L_i(0)$ of node i is the number of the shortest paths, thus the initial load can describe the characteristic of node. Here, we define the first weighting method $w_i^{(1)}$ as

$$w_i^{(1)} = L_i(0). \tag{2}$$

(2) The Weighing Method $w_i^{(2)}$. In the research of complex networks, the degree k_i of node i is always used to describe its feature, which can measure the importance of node in complex networks. Usually, the node with higher degree means higher importance, and it will become the hubs in networks. Thus, we use it to describe the characteristic of node i; namely,

$$w_i^{(2)} = k_i = \sum_{j \in \Gamma_i} a_{ij}, \tag{3}$$

where Γ_i is the set of the neighbors of node i.

(3) The Weighing Method $w_i^{(3)}$. In the investigation of cascading dynamics, the product $(k_i k_j)^\theta$ of the degrees k_i and k_j of the two end nodes of an edge e_{ij} can measure the weight of an edge e_{ij}. Wang shows that the networks with $\theta = 1$ have the strongest robustness against cascading failures [23]. Thus, in this paper, we define the third weighting method as:

$$w_i^{(3)} = \sum_{j \in \Gamma_i} \left(k_i k_j\right)^\theta = k_i^\theta \sum_{j \in \Gamma_i} k_j^\theta, \tag{4}$$

where Γ_i is the set of the neighbors of node i, and here we assume the parameter $\theta = 1$.

Furthermore, according to the theory of the degree of networks and probability [32], as $\theta = 1$, the second term on the right hand side of (4) will become

$$\sum_{j \in \Gamma_i} k_j = k_i \sum_{k' = k_{\min}}^{k_{\max}} P\left(k' \mid k_i\right) k', \tag{5}$$

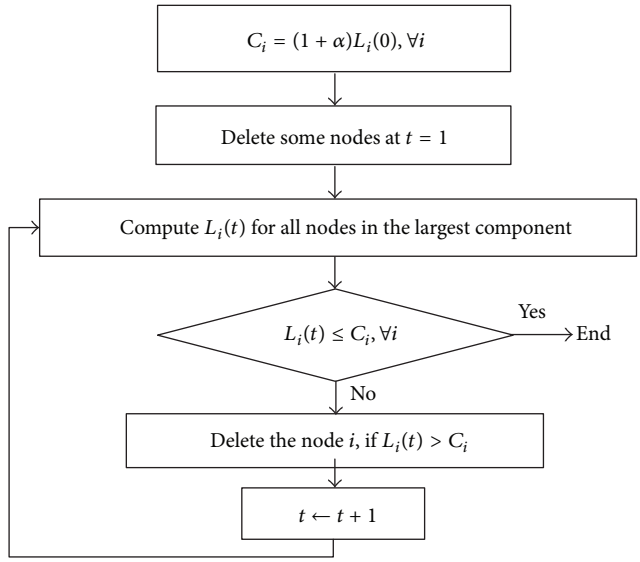

Figure 1: The iterative process of cascading failures in complex networks.

where $k_{\min}$ and $k_{\max}$ are the minimum degree and the maximum degree in a network, respectively. $P(k' \mid k_i)$ is the conditional probability that the node with degree k_i links to a neighbouring node with degree k', and this conditional probability satisfies the normalized and equilibrium conditions:

$$\sum_{k'} P\left(k' \mid k_i\right) = 1,$$
$$k_i P\left(k' \mid k_i\right) P\left(k_i\right) = k' P\left(k_i \mid k'\right) P\left(k'\right). \tag{6}$$

Since the BA scale-free networks, WS small-world networks, and ER random networks have no degree-degree correlation [33], according to the conditions in (6), one can get

$$P\left(k' \mid k_i\right) = \frac{k' P\left(k'\right)}{\langle k \rangle}, \tag{7}$$

where $\langle k \rangle$ is the average degree of networks. Therefore, inserting (7) back into (5), we get

$$\sum_{j \in \Gamma_i} k_j = k_i \sum_{k'=k_{\min}}^{k_{\max}} \frac{k' P\left(k'\right) k'}{\langle k \rangle} = \frac{k_i \left\langle k^2 \right\rangle}{\langle k \rangle}. \tag{8}$$

Now, finally (4) is simplified as

$$w_i^{(3)} = \frac{k_i^2 \left\langle k^2 \right\rangle}{\langle k \rangle}. \tag{9}$$

One can see that the weighting method $w_i^{(3)}$ is different with $w_i^{(2)}$ obviously.

(4) The Weighing Method $w_i^{(4)}$. Here, we introduce the fourth kind of weighting method based on node centrality betweenness. The link is always important as the two nodes of its end are important in many real-world networks. For example, the packet has always been transmitted along the links with the important chosen nodes, while the node betweenness centrality is used to describe the importance of nodes in networks [34]. Considering this intuition, usually, the product $(B_i B_j)^\theta$ is used to measure the weight of the edge e_{ij} [24], where B_i and B_j are the node betweenness of node i and j, respectively. The node betweenness of node i is defined as

$$B_i = \sum_{a \neq b} \frac{\sigma_{ab}(i)}{\sigma_{ab}}, \tag{10}$$

where σ_{ab} is the number of the shortest paths between node a and b. $\sigma_{ab}(i)$ is the number of the shortest paths passing through the node i in the shortest paths σ_{ab}.

Therefore, we define the fourth kind of weighting method $w_i^{(4)}$ as the follows:

$$w_i^{(4)} = \sum_{j \in \Gamma_i} \left(B_i B_j\right)^\theta = B_i^\theta \sum_{j \in \Gamma_i} B_j^\theta, \tag{11}$$

where Γ_i is the set of the neighbors of node i, and here we assume the parameter $\theta = 1$.

Using Bayes' rules [32], (11) can become

$$w_i^{(4)} = B_i \sum_{B'=B_{\min}}^{B_{\max}} k_i P\left(B' \mid B_i\right) B', \tag{12}$$

where $B_{\min}$ and $B_{\max}$ are the minimum and the maximum node betweenness in networks, respectively. $P(B' \mid B_i)$ is the conditional probability that a node with node betweenness centrality B_i links to the node with node betweenness centrality B'.

Considering that it has been shown that small-world networks do not show betweenness-betweenness correlations [24], therefore, we can assume $P(\mathrm{B}' \mid B_i) = P(B')$. Then, (12) can be simplified as

$$w_i^{(4)} = B_i k_i \sum_{B'=B_{\min}}^{B_{\max}} P\left(B'\right) B' = B_i k_i \langle B \rangle, \tag{13}$$

where $\langle B \rangle$ is the average node betweenness in networks.

Now, it is obvious that the four kinds of weighting methods of node introduced here can describe the characteristics of nodes and distinguish the nodes in network.

4. The Studied Complex Networks

In this paper, to investigate the vulnerable nodes in networks subject to cascading failures, we mainly take the following typical complex networks into account: Barabasi-Albert scale-free networks (SF), Watts-Strogatz small-world networks (WS), and ER random networks (ER).

(1) Scale-free networks (SF): SF network model in this paper is generated according to the two rules: growth and preferential attachment [35]. The degree distribution of the generated SF network obeys the power law distribution $P(k) \sim k^{-\gamma}$ ($\gamma = 3$) and the mean degree $\langle k \rangle \approx 4$.

(2) WS small-world networks (WS): here, according to Watts-Strogatz model [36], we generate the small-world network by changing the rewiring probability p. We mainly consider the two cases with the rewiring probability $P = 0.1$ and $P = 0.5$. It should be noticed that the rewiring probability $P = 1$ means that the WS network will become a completely random network.

(3) ER random networks (ER): the random network model studied is generated according to the rules in [37], where we control the average degree $\langle k \rangle \approx 4$.

Also, in order to compare with the network models, we consider two real-world networks: the autonomous system network (AS) and US airport network (US airport).

(4) The autonomous system network (AS): from the AS level topology of Internet, the Internet can be seen as a network comprising of routers. Usually, the data is transmitted between routers according

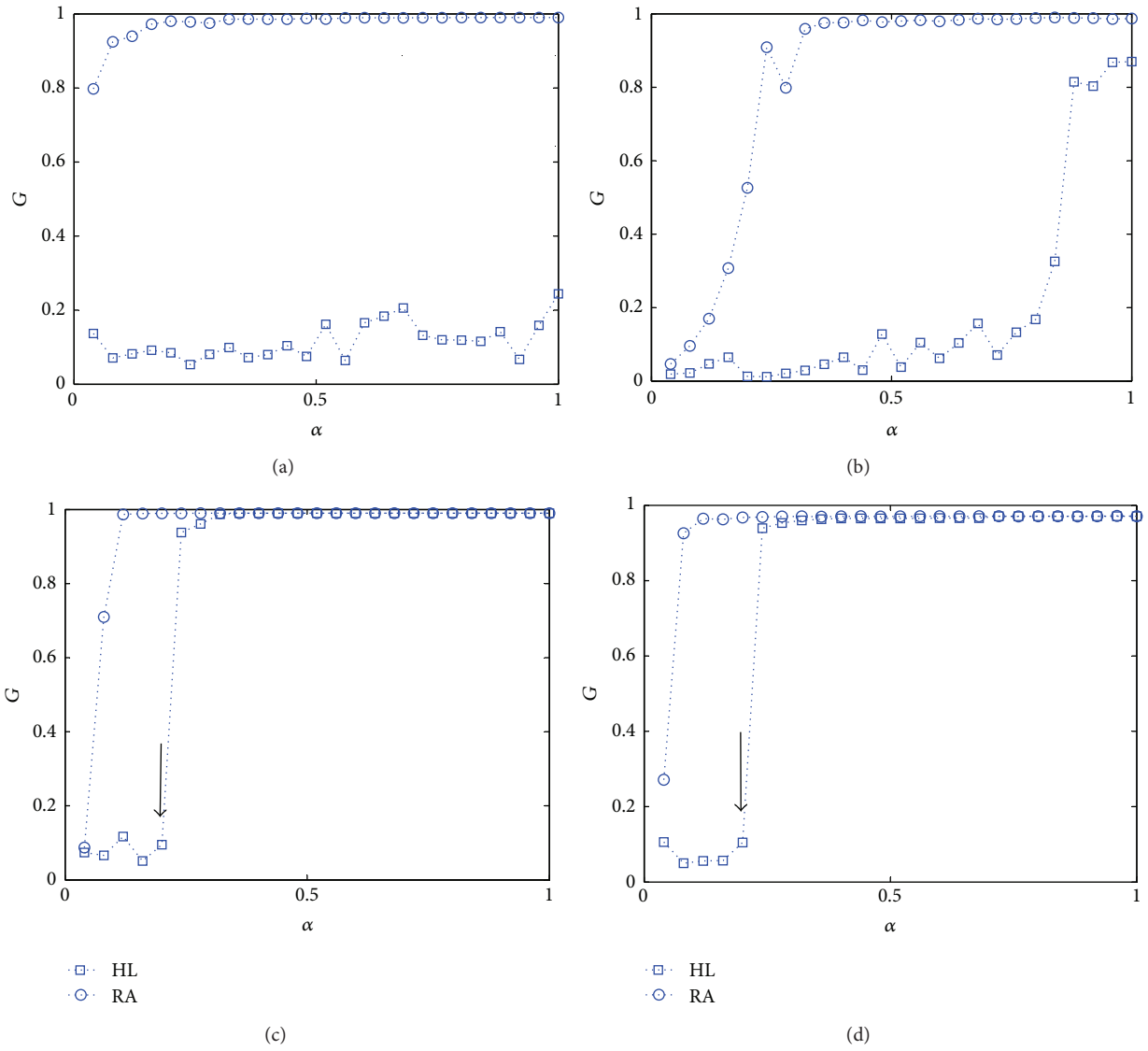

FIGURE 2: Under RA and HL attacks, the relative size of nodes in the largest component G as a function of α for (a) SF network, (b) WS small-world network with the rewiring probability $P = 0.1$, (c) WS network with $P = 0.5$, and (d) ER random network. The simulations under RA attack are averaged over 20 times.

to BGP protocols. Thus, the routers (as nodes) and links construct the autonomous system network (AS) [38]. Here, we take the AS network with 1470 nodes, for example, and the mean degree $\langle k \rangle \approx 4.3$. By computation, we find that the degree of distribution of AS network clearly obeys power-law distribution: $P(k) \sim k^{-\gamma}$, where the index $\gamma \approx 0.005$.

(5) US airport network: as an example of transportation networks, we study the famous USA airport network with 500 airports and 2980 links [39]. The mean degree $\langle k \rangle \approx 11.9$.

5. The Simulation and Analysis

Now, in this section, concerned with two kinds of node-based attacks, we will investigate how to identify the vulnerable nodes of complex networks subject to cascading failures. The studied networks include SF, WS, and ER complex networks models and two real-world networks.

Firstly, we use the relative size of nodes in the largest component of network (G) to quantify the integral robustness of complex networks under cascading failures. The metric G is defined as

$$G = \frac{N'}{N}, \tag{14}$$

where N' and N are the number of nodes in the largest component after attacks and the total number of nodes in network, respectively.

Obviously, the metric G can be seen as a function of the tolerance parameter α and $0 \leq G \leq 1$. Also, it should be noticed that, with the higher G, the network maintains higher

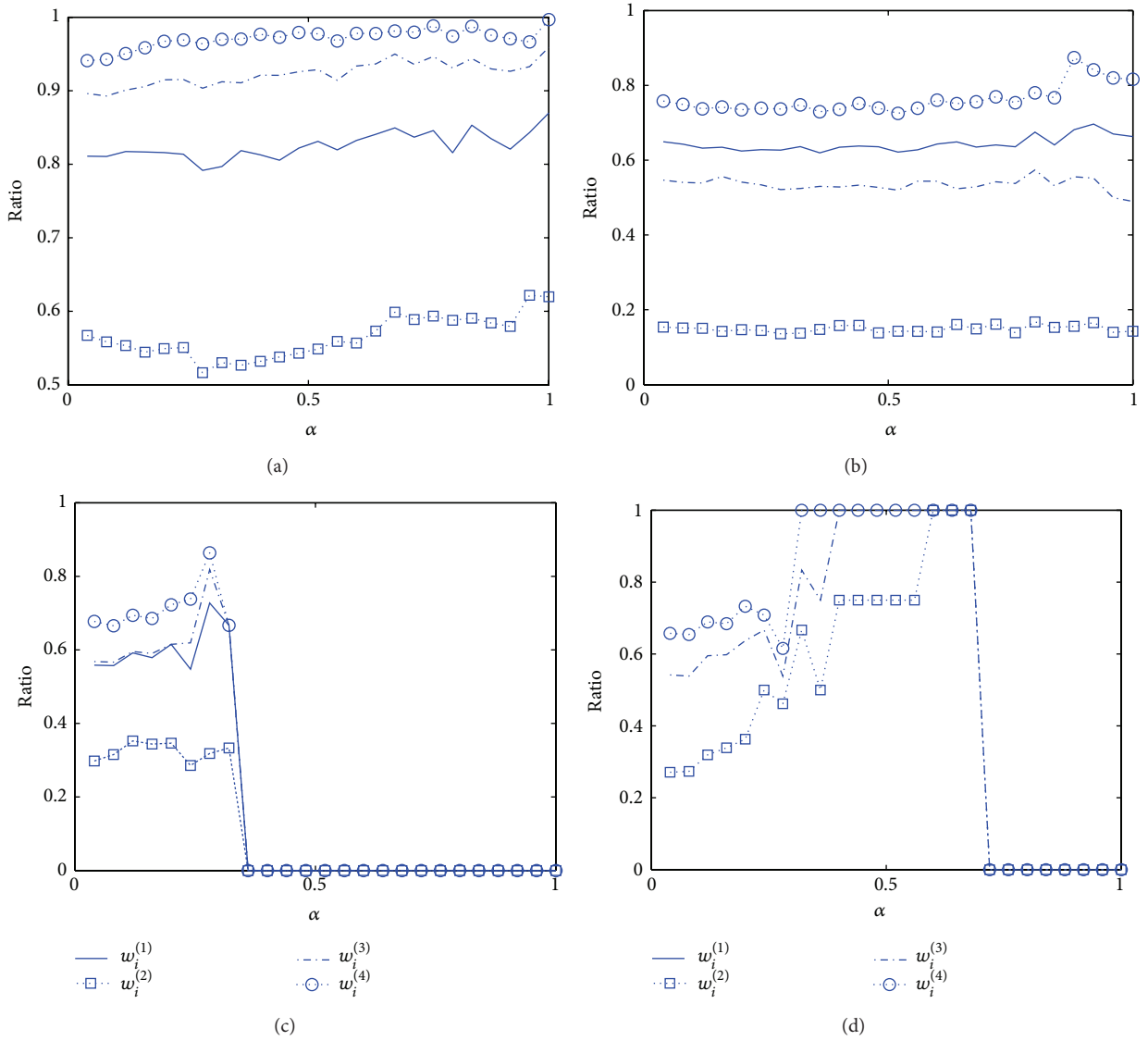

FIGURE 3: Under HL attack, the ratio for different weighting methods as a function of α for (a) SF network, (b) WS small-world network with the rewiring probability $P = 0.1$, (c) WS network with $P = 0.5$, and (d) ER random network.

connectivity and shows higher robustness against cascading failures.

Secondly, to identify the features of the vulnerable nodes in complex networks, we numerically computed the ratio of the failed nodes with four kinds of weights less than their respective average weights to the total of the failed ones in networks when the iterative process of complex networks in Figure 1 is stopped (at this time, the cascading failures are completed); namely,

$$\text{ratio} = \frac{\sum_{t:w_i^{(n)}<\overline{w^{(n)}}} as(t)}{\sum_t as(t)}, \quad n = 1, 2, 3, 4, \tag{15}$$

where $\overline{w^{(n)}}$ is the average value of the nth kind of weight defined in Section 3 in network ($n = 1, 2, 3, 4$). $as(t)$ is the number of failed nodes at time step t after attacks in network.

One can see that the ratio in (15) can mainly distinguish the characteristics of the failed nodes in complex networks.

5.1. The Analysis of Complex Networks Models. In this part, induced by random attack (RA) and the highest-load attack (HL), we mainly focus on analyzing the integral robustness and identifying the vulnerable nodes of three kinds of typical complex networks models: scale-free networks (SF), WS small-world networks (WS), and ER random networks (ER).

(1) From the relative size of nodes in the largest component G, as shown in Figure 2, being subject to intentional attack (HL), SF network and WS small-world network with $P = 0.1$ are more vulnerable, while WS network with $P = 0.5$ and ER random network are more robust. being subject to random attack (RA), SF network model is more robust. It means that SF

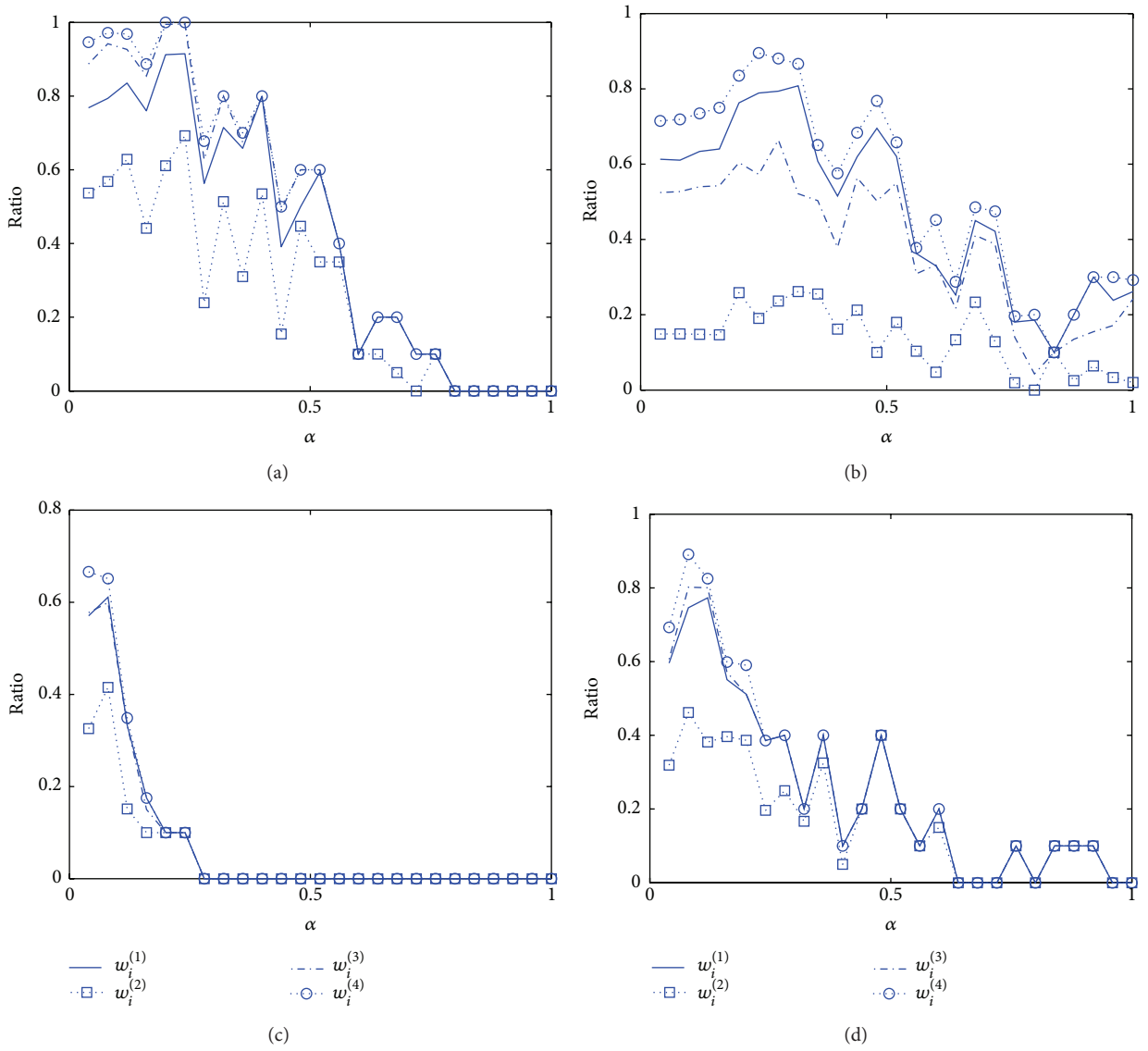

FIGURE 4: Under RA attack, the ratio for different weighting methods as a function of α for (a) SF network, (b) WS small-world network with the rewiring probability $P = 0.1$, (c) WS network with $P = 0.5$, and (d) ER random network. The simulations under RA attack are averaged over 20 times.

network models show the dual characteristics of both robustness and vulnerability.

(2) From the ratio in (15), under HL attack, as shown in Figure 3, for SF network models, the ratio of the failed nodes with small weighting value to the total failed ones is always more than 50%. Especially, we should notice that the highest ratio is the one of the failed nodes with small $w_i^{(4)}(w_i^{(4)} < \overline{w^{(4)}})$ and it is always more than 90%. In addition, the second highest is the ratio of the failed ones with small $w_i^{(3)}$. These results reveal that, under intentional attack, the nodes with small $w_i^{(4)}$ are more vulnerable.

For WS small-world network, from Figure 3(b), under HL attack, as the rewiring probability $P = 0.1$, the ratio of the failed nodes with small $w_i^{(4)}$ is almost more than 80% and also the ratio of the failed nodes with small $w_i^{(2)}$ is less than 20% (it implies that the ratio of the failed nodes with big $w_i^{(2)}$ is more than 80%). At the same time, for $P = 0.5$, since $\alpha = 0.2$ is the transition point of the connectivity of WS network from low to high (see the arrow in Figure 2(c)) and there are few failed nodes when $\alpha > 0.2$, here, we mainly focus on the case of $\alpha < 0.2$. As shown in Figure 3(c), for $\alpha < 0.2$, the ratio of the failed nodes with small $w_i^{(4)}$ is more than 70%. Also, the ratio of the failed nodes with small $w_i^{(2)}$ is less than 40%. Now, obviously, we can see that, under intentional attack, for WS small-world network, the nodes with small $w_i^{(4)}$ are more vulnerable and also the ones with big $w_i^{(2)}$ (namely, the nodes with high degree) are easy to break down.

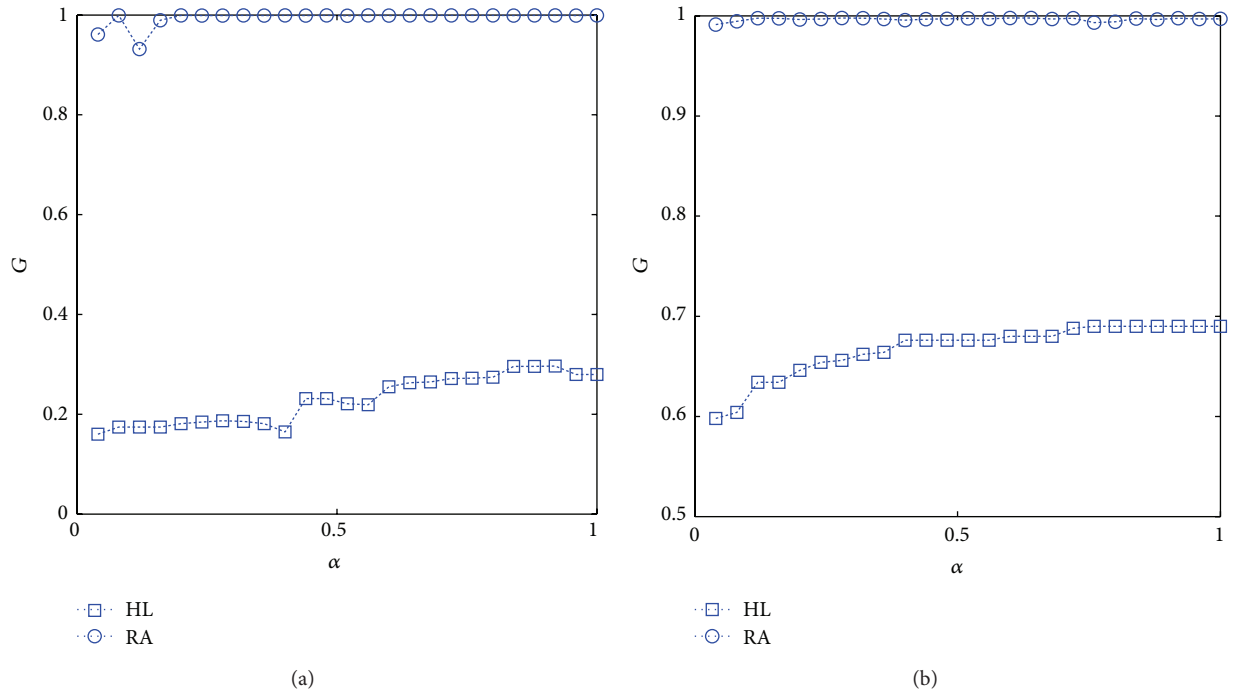

FIGURE 5: Under RA and HL attacks, the relative size of nodes in the largest component G as a function of α for (a) the autonomous system network (AS) and (b) US airport network. The simulations under RA attack are averaged over 20 times.

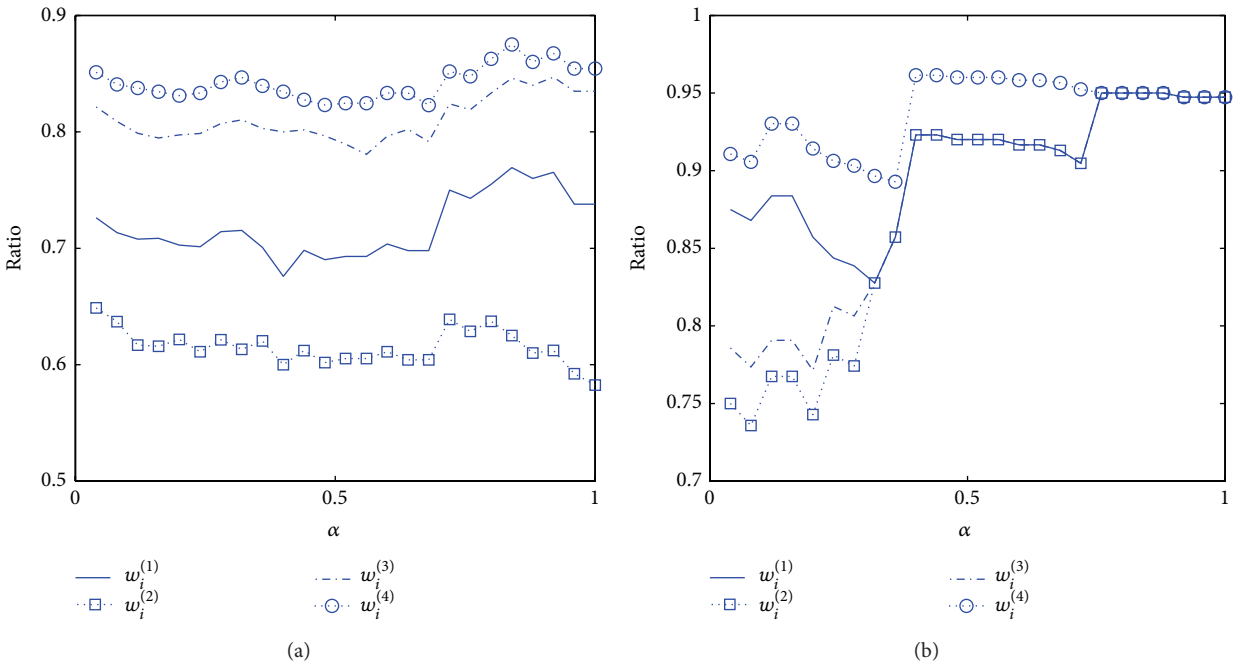

FIGURE 6: Under HL attack, the ratio for different weighting methods as a function of α for (a) the autonomous system network (AS) and (b) US airport network.

For ER random network under HL attack, as $\alpha < 0.2$ ($\alpha = 0.2$ is the turning point of the connectivity from low to high; see the arrow in Figure 2(d)), ER random network shows similarity to WS small-world network; namely, the nodes with small $w_i^{(4)}$ are more vulnerable and also the ones with big $w_i^{(2)}$ are easy to break down.

(3) Under RA attack, there are the failed nodes only for small α (see the curves in Figure 2); thus, we only consider the case of small α. Figure 4 shows that most of the failed nodes in SF network are still the ones with small $w_i^{(4)}$. While WS small-world network and ER random network show similarity to their case under

HL attack; namely, the nodes with small $w_i^{(4)}$ are more vulnerable and also the ones with big $w_i^{(2)}$ (the nodes with high degree) are easy to break down.

5.2. The Analysis of Real-World Networks. In order to compare with the simulations of the network models, we also analyze two real-world networks: the autonomous system network (AS) and US airport network.

As shown in Figure 5, both AS network and US airport network are very robust under RA attack and vulnerable under HL attack. Especially, AS network is more vulnerable under HL attack. Then, in the following discussion of this part, we only consider the case under HL attack because of their strong robustness against random disturbance.

From Figure 6(a), it is obvious that AS network with scale-free characteristics shows similarity to SF network model, and also the ratio of the failed nodes with small weighting values to the total failed ones is always more than 50%. Especially, the ratio of the failed nodes with small $w_i^{(4)}$ ($w_i^{(4)} < \overline{w^{(4)}}$) is highest and always more than 80%. The second highest is the ratio of the failed ones with small $w_i^{(3)}$. It reveals that, for SF networks under intentional attack, the nodes with small $w_i^{(4)}$ are more vulnerable than other nodes and these nodes are easy to break down.

For US airport network, as shown in Figure 6(b), similarly, this ratio of the failed nodes with small $w_i^{(4)}$ is highest and it is more than 90%. Also, the nodes with small $w_i^{(4)}$ are more vulnerable under intentional attack.

6. Conclusions

In the research on cascading dynamics, finding and distinguishing the vulnerable nodes of networks are very important for the protection of infrastructures systems, but the traditional research on the vulnerability of complex networks has not considered this. This paper mainly probes the question of how to identify the vulnerable nodes of complex networks in cascading failures caused by the overload on nodes. We model the cascading dynamics of complex networks induced by deleting some proportion of nodes that are chosen randomly or intentionally. Then, four kinds of weighting methods of node are introduced to distinguish the failed nodes of complex networks, including BA scale-free networks, WS small-world networks, ER random networks, and two real-world networks. The main contributions of this paper are as follows.

(1) For SF networks, under HL attack, the nodes with small $w_i^{(4)}$ are most vulnerable and the ones with small $w_i^{(3)}$ are also easy to break down. The simulation of the autonomous system network (AS) with power-law distribution also verifies our findings. However, the weight $w_i^{(4)}$ involved in computing the node betweenness needs to know the whole structure of networks. In fact, The complexity of computing node betweenness is high, especially for large-scale networks. While, computing the weight $w_i^{(3)}$ only needs to know the local structure of networks. Therefore, we should pay attention to the nodes with small $w_i^{(3)}$ in distinguishing the vulnerable components of large networks. It should be pointed out that the recent research of Ercsey demonstrates that the local information can be used to approximately calculate the node betweenness of large-scale networks in order to reduce the complexity [40].

(2) For WS small-world networks and ER random network, when the tolerance ability of node is low, no matter under RA attack or HL attack, the nodes with small $w_i^{(4)}$ are more vulnerable and also the ones with big $w_i^{(2)}$ are easier to break down.

The findings of this paper provide important theory basis for analyzing network security, mining the hidden potential risk of networks, and protecting various real-world networks with load assigned to nodes.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant nos. 61202362, 61121061, 61262057, 61372191, and 91124002), the 863 programs (Grant nos. 2012AA01A401, 2010AA-012505, and 2011AA010702), the State Key Development Program of Basic Research of China 973 (Grant nos. 2013CB329601 and 2011CB302600), the China Postdoctoral Science Foundation Programs (BS2013SF009, 2012m520114, and 2013T60037), and the Beijing Higher Education Young Elite Teacher Project.

References

[1] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 6, Article ID 065102, 4 pages, 2002.

[2] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. de Porcellinis, and R. Setola, "Modelling interdependent infrastructures using interacting dynamical models," *International Journal of Critical Infrastructures*, vol. 4, no. 1-2, pp. 63–79, 2008.

[3] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, "Complex networks: structure and dynamics," *Physics Reports*, vol. 424, no. 4-5, pp. 175–308, 2006.

[4] S. Boccaletti, J. Buldú, R. Criado et al., "Multiscale vulnerability of complex networks," *Chaos*, vol. 17, no. 4, Article ID 043110, 2007.

[5] I. Mishkovski, M. Biey, and L. Kocarev, "Vulnerability of complex networks," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 1, pp. 341–349, 2011.

[6] I. Petreska, I. Tomovski, E. Gutierrez, L. Kocarev, F. Bono, and K. Poljansek, "Application of modal analysis in assessing attack vulnerability of complex networks," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 4, pp. 1008–1018, 2010.

[7] P. Crucitti, V. Latora, and M. Marchiori, "A topological analysis of the Italian electric power grid," *Physica A*, vol. 338, no. 1-2, pp. 92–97, 2004.

[8] E. Bompard, M. Masera, R. Napoli, and F. Xue, "Assessment of structural vulnerability forpower grids by network performance

based on complex networks," in *Critical Information Infrastructure Security*, vol. 5508 of *Lecture Notes in Computer Science*, pp. 144–154, 2009.

[9] R. V. Solé, M. Rosas-Casals, B. Corominas-Murtra, and S. Valverde, "Robustness of the European power grids under intentional attack," *Physical Review E*, vol. 77, no. 2, Article ID 026102, 2008.

[10] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: a topological approach," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1334–1340, 2011.

[11] B. K. Mishra and A. K. Singh, "Two quarantine models on the attack of malicious objects in computer network," *Mathematical Problems in Engineering*, vol. 2012, Article ID 407064, 13 pages, 2012.

[12] M. Hua, P. Cheng, J. Fei, J. Zhang, and J. Chen, "Network-based robust H_∞ filtering for the uncertain systems with sensor failures and noise disturbance," *Mathematical Problems in Engineering*, vol. 2012, Article ID 945271, 19 pages, 2012.

[13] M. Li and W. Zhao, "On $1/f$ noise," *Mathematical Problems in Engineering*, vol. 2012, Article ID 673648, 23 pages, 2012.

[14] M. Li, "Fractal time series—a tutorial review," *Mathematical Problems in Engineering*, vol. 2010, Article ID 157264, 26 pages, 2010.

[15] M. Li and W. Zhao, "Visiting power laws in cyber-physical networking systems," *Mathematical Problems in Engineering*, vol. 2012, Article ID 302786, 13 pages, 2012.

[16] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 6, Article ID 065102, 4 pages, 2002.

[17] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Physical Review E*, vol. 69, no. 4, Article ID 045104, 4 pages, 2004.

[18] H. J. Sun, H. Zhao, and J. J. Wu, "A robust matching model of capacity to defense cascading failure on complex networks," *Physica A*, vol. 387, no. 25, pp. 6431–6435, 2008.

[19] Y. Xia, J. Fan, and D. Hill, "Cascading failure in Watts-Strogatz small-world networks," *Physica A*, vol. 389, no. 6, pp. 1281–1285, 2010.

[20] M. Babaei, H. Ghassemieh, and M. Jalili, "Cascading failure tolerance of modular small-world networks," *IEEE Transactions on Circuits and Systems II*, vol. 58, no. 8, pp. 527–531, 2011.

[21] J.-W. Wang and L.-L. Rong, "Cascade-based attack vulnerability on the US power grid," *Safety Science*, vol. 47, no. 10, pp. 1332–1336, 2009.

[22] J.-W. Wang and L.-L. Rong, "Edge-based-attack induced cascading failures on scale-free networks," *Physica A*, vol. 388, no. 8, pp. 1731–1737, 2009.

[23] W.-X. Wang and G. Chen, "Universal robustness characteristic of weighted networks against cascading failure," *Physical Review E*, vol. 77, no. 2, Article ID 026101, 5 pages, 2008.

[24] B. Mirzasoleiman, M. Babaei, M. Jalili, and M. Safari, "Cascaded failures in weighted networks," *Physical Review E*, vol. 84, no. 4, Article ID 046114, 8 pages, 2011.

[25] S. Li, L. Li, Y. Yang, and Q. Luo, "Revealing the process of edge-based-attack cascading failures," *Nonlinear Dynamics*, vol. 69, no. 3, pp. 837–845, 2012.

[26] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[27] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," *Physical Review E*, vol. 83, no. 6, Article ID 065101, 4 pages, 2011.

[28] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Networks formed from interdependent networks," *Nature Physics*, vol. 8, no. 1, pp. 40–48, 2012.

[29] W. Li, A. Bashan, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Cascading failures in interdependent lattice networks: the critical role of the length of dependency links," *Physical Review Letters*, vol. 108, no. 22, Article ID 228702, 5 pages, 2012.

[30] J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of a network of networks," *Physical Review Letters*, vol. 107, no. 19, Article ID 195701, 5 pages, 2011.

[31] R. Parshani, S. V. Buldyrev, and S. Havlin, "Critical effect of dependency groups on the function of networks," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 108, no. 3, pp. 1007–1010, 2011.

[32] C. Howson and P. Urbach, *Scientific Reasoning: The Bayesian Approach*, Open Court, La Salle, Ill, USA, 1993.

[33] Z. Nikoloski, N. Deo, and L. Kucera, "Degree-correlation of a scale-free random Graph process," in *Proceedings of the European conference on combinatorics, Graph Theory and Applications*, pp. 239–244, Berlin, Germany, September 2005.

[34] T. B. Hashimoto, M. Nagasaki, K. Kojima, and S. Miyano, "BFL: a node and edge betweenness based fast layout algorithm for large scale networks," *BMC Bioinformatics*, vol. 10, article 19, 2009.

[35] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[36] D. J. Watts and S. H. Strogatz, "Collective dynamics of "small-world" networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[37] P. Erdős and A. Rényi, "On the evolution of random graphs," in *Publication of the Mathematical Institute of the Hungarian Academy of Sciences*, vol. 5, pp. 17–61, 1960.

[38] J. Leskovec, J. Kleinberg, and C. Faloutsos, "Graphs over time: densification laws, shrinking diameters and possible explanations," in *Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '05)*, pp. 177–187, New York, NY, USA, August 2005.

[39] V. Colizza, R. Pastor-Satorras, and A. Vespignani, "Reaction-diffusion processes and metapopulation models in heterogeneous networks," *Nature Physics*, vol. 3, no. 4, pp. 276–282, 2007.

[40] M. Ercsey-Ravasz and Z. Toroczkai, "Centrality scaling in large networks," *Physical Review Letters*, vol. 105, no. 3, Article ID 038701, 4 pages, 2010.