Hindawi Publishing Corporation
Abstract and Applied Analysis
Volume 2013, Article ID 453689, 13 pages
http://dx.doi.org/10.1155/2013/453689

Research Article

Cascading Dynamics of Heterogenous Scale-Free Networks with Recovery Mechanism

Shudong Li,[1,2] Zhongtian Jia,[3] Aiping Li,[2] Lixiang Li,[4] Xinran Liu,[5] and Yixian Yang[4]

[1] *College of Mathematics and Information Science, Shandong Institute of Business and Technology, Yantai, Shandong 264005, China*
[2] *School of Computer Science, National University of Defense Technology, Changsha, Hunan 410073, China*
[3] *Shandong Provincial Key Laboratory of Network Based Intelligent Computing, University of Jinan, Jinan 250022, China*
[4] *Information Security Center, Beijing University of Posts and Telecommunications, P.O. Box 145, Beijing 100876, China*
[5] *National Computer Network Emergency Response Technical Team/Coordination Center, Beijing 100029, China*

Correspondence should be addressed to Shudong Li; leeshudong79@163.com

Received 11 November 2013; Accepted 6 December 2013

Academic Editor: Shuping He

In network security, how to use efficient response methods against cascading failures of complex networks is very important. In this paper, concerned with the highest-load attack (HL) and random attack (RA) on one edge, we define five kinds of weighting strategies to assign the external resources for recovering the edges from cascading failures in heterogeneous scale-free (SF) networks. The influence of external resources, the tolerance parameter, and the different weighting strategies on SF networks against cascading failures is investigated carefully. We find that, under HL attack, the fourth kind of weighting method can more effectively improve the integral robustness of SF networks, simultaneously control the spreading velocity, and control the outburst of cascading failures in SF networks than other methods. Moreover, the third method is optimal if we only knew the local structure of SF networks and the uniform assignment is the worst. The simulations of the real-world autonomous system in, Internet have also supported our findings. The results are useful for using efficient response strategy against the emergent accidents and controlling the cascading failures in the real-world networks.

1. Introduction

The robustness properties of complex networks subject to either random breakdown or intentional attacks have attracted considerable interest [1, 2], due to the blackouts in US power grids [3, 4], the large-scale congestion in the Internet [5], and the electrical blackout in Italy [6]. These accidents have threatened the network safety and resulted in enormous loss in economy.

As a result, many issues have been investigated carefully, including the robustness of the topological structure of networks [7–11], the description of cascading phenomenon and transition [12], the protection strategies against cascade [13–18], the cost of attack and defense [19, 20], and the reliability metrics of networks [21, 22]. In addition, the vulnerability of the real-world networks has become an important topic in the design of engineering safety [23, 24]. The cascading failure in power systems [25, 26] and the attacks in computer networks [27] have attracted more consideration. Some researches focus on the stability analysis for the uncertain systems [28–30] and the analysis of cyberphysical networking systems [31]. Especially, the robustness and cascading failures in interdependent networks [32–35] have become a hot topic for the past few years. Also, traffic bound [36], traffic delay [37], and the control systems of heavy inputs and delay systems [38, 39] are considered carefully.

The cascading failures [35, 40], which originate very locally but often result in a global collapse, have become one of the hottest topics in network safety. On the one hand, by characterizing the load on nodes, the considerable cascading models under the attacks on nodes have been presented. The conditions of the global cascade are explored [40, 41], where every node is assumed to have the same capacity [41]. The influence of the removal of nodes on reducing the efficiency of networks is investigated [42]. The cascading failures of the North American power grid under the loss of nodes [43] and the cascading failures induced by flux fluctuations [44] are also probed. On the other hand, the cascading dynamics induced by the edge-based attacks have also been probed. These researches focus on the cascading model by assigning the load and adopting a local load redistribution to edges [45, 46] and the model that the overloaded edges break down with some probability [47]. The size of cascade and the cost of investment under the removal of targeted edges [48] and the cascade by adopting the Ohw' and Kirchhoff conservation law [49] are also probed.

However, once the cascading failures emerged, the important question is concerned with the efficient response to disasters. In real-world networks, there always exists some emergency mechanism or "recovery mechanism" that can be regarded as the coming external resources (e.g., manpower, number of vehicles) into networks, which recovers the overloaded components to the normal state. For example, police could deal with the emergent accidents or chaos in roads and the technical experts could handle the breakdown and repair the components damaged in technical networks, such as the electric power system and the Internet network. These accidents or breakdown can be caused by the natural events (earthquakes, floods, or extreme weather) or the intentional attacks. Such recovery mechanism can effectively counteract the overload and relieve the stress, which could make the edges or nodes from "overloaded" to "congestion" (the midstate) and maybe to "normal." Yet this recovery mechanism has not been considered in previous works. Therefore, it is important to investigate the influence of the recovery mechanism on increasing the robustness of the networks against cascading failures, especially for the network safety. We argue that probing this question will give us important implications in using efficient strategy to deal with the disasters happening in real-world networks.

In this paper, induced by highest-load attack (HL) and random attack (RA) on one edge, we study the cascading dynamics of the heterogeneous scale-free (SF) network with recovery mechanism that is represented by the external resources τ entering into SF network. Our novel model defines four kinds of weighing strategies to assign the external resource to the edges for recovering the networks from cascading failures. The influence of τ, the tolerance parameter α, and the different weighting strategies on improving the robustness against cascading failures in SF networks is investigated. We find that, firstly, under intentional attack, the fourth weighing method can more effectively decrease the number of avalanched edges, reduce the spreading speed of cascading failures, and control the outburst of cascading failures in SF networks than other methods. Secondly, as the most efficient strategy under intentional attack, the fourth weighting method needs to compute the betweenness centrality of nodes, which implies that the topological structure of SF networks is needed. Therefore, the third weighting method will be optimal if we only knew the local structure of network (namely, the degree of nodes). On the other hand, as an example in real-world networks, the simulation of the autonomous system in the Internet with scale-free characteristics also shows the same results of SF network model. It means that the simulation of real-world networks supports our findings.

The rest of this paper is organized as follows. Section 2 develops the novel model of cascading dynamics with recovery mechanism under edge-based attack, in which the external resource is assigned to the links according to the weight of links in SF network. In Section 3, we describe four kinds of weighting strategies to measure the weight of the links in SF networks. In Section 4, we compare the influence of four kinds of weighting strategies on the robustness of SF network against cascading failures and analyze the results of our simulations. Section 5 summarizes the most important findings and offers the future research.

2. The Cascading Dynamics with Recovery Mechanism

In this section, we focus on the development of cascading model on the weighted scale-free network subject to random and intentional attack on one edge.

Since many real-world networks have been observed to have a typical power-law degree distribution $P(k) \propto k^{-\gamma}$ (γ is the scale exponent), the vulnerability and the robustness of such scale-free networks (SF) under attacks have been an important problem in studying the cascading failures of complex networks [10, 40, 45–47, 50].

Therefore, in this paper, we focus on the cascading dynamics of the Barabási-Albert scale-free network model generated according to the rule of growth and preferential attachment [50]. On the other hand, The large-scale congestion in the Internet has drawn attention to the robustness of the autonomous system (AS) [5]. Therefore, as an example in the real-world networks, considering that the autonomous system (AS) formed by the graph of routers comprising the Internet from the BGP (Border Gateway Protocol) logs has been observed to show power-law degree distribution [51], we also focus on the autonomous system (AS) defined as AS1470 which has 1470 nodes and 3997 edges and the mean degree $\langle k \rangle \approx 4.26$. Here, we define the adjacent matrix of network considered as $A = (a_{ij})_{N\times N}$, where $a_{ij} = 1$ if the node i links to the node j; otherwise $a_{ij} = 0$. We denote w_{ij} as the weight of the edge e_{ij} in network.

Generally, the development of cascading model is based on the following three factors: the definition of the original load, the correlation between the original load and the capacity, and the dynamical redistribution of load after the attacks. Similarly, the cascading dynamics in this paper is modeled as follows.

(1) The original load on the edge e_{ij}: in many physical network structures, the physical flows (data packets or energy) are always forwarded along the edges according to the shortest path routing strategy. For a given pair of nodes (m, n), the flows are transmitted along the shortest paths connecting them; maybe there exist some shortest paths through the edge e_{ij}. Therefore, it is natural to define the total number of shortest paths passing through e_{ij} between any pair of nodes in a network as the load on e_{ij}. Naturally, for our weighted SF network, the load $L_{ij}(t)$ on the edge e_{ij} at time t is defined

as the number of the shortest paths through it ($t = 0$ means the initial load $L_{ij}(0)$ before attack). Now we assume that the original load on e_{ij} is $L_{ij}(0)$.

(2) The capacity C_{ij} of the edge e_{ij}: we suppose that C_{ij} is the maximum load that an edge e_{ij} could handle and is proportional to the initial load $L_{ij}(0)$; that is,

$$C_{ij} = (1+\alpha)\, L_{ij}(0), \quad \forall ij, \tag{1}$$

where $\alpha \geq 0$ is the tolerance parameter. The higher α means that the edge has the higher capacity and the higher ability against failures. Also, it is rational in designing the real-world networks including power grids and the Internet, because the capacity of the links in these networks is always limited by the cost.

In most of the previous models, there were only two states assigned to a node or edge: *normal* or *overloaded*; besides the node or edge would break down (i.e., overloaded) once the load on them exceeded their capacity. However, in real-world networks, there exists some emergency mechanism that will handle the congestion state, relieve the pressure on them, and thus reduce the probability of the overload. For example, in transportation networks, the external resources (such as manpower or vehicles) will come to deal with the emergent events and recover the road from the "congested or overloaded" road to the "normal" state. Therefore, we assign a recovery rate τ_{ij} to every edge e_{ij} and assume that the threshold C^*_{ij} is the upper bound load on e_{ij} in normal state. Naturally, we define

$$\tau_{ij} = \frac{1 + \left(w_{ij}/\sum_{1\leq i<j\leq N} w_{ij}\right)\cdot\tau}{10}, \tag{2}$$

$$C^*_{ij} = \left(1 + \alpha\cdot\tau_{ij}\right) L_{ij}(0), \quad \forall ij, \tag{3}$$

where w_{ij} is the weight of the edge e_{ij} and τ is an adjustable parameter which represents the external resources entering into the network. Here we assume $\tau \geq 1$. When developing (2) and (3), we required the following.

(i) We hope that the external resources τ enter into the network according to the importance of the edge e_{ij} that is measured by the normalized weight $w_{ij}/\sum_{1\leq i<j\leq N} w_{ij}$. The recovery rate τ_{ij} should increase monotonically with the increasing τ. For some τ, the bigger w_{ij}, the more external resources are assigned to the edge e_{ij}, and then the recovery rate τ_{ij} can be closer to the upper bound $(1+\tau)/10$.

(ii) We can control the parameter τ to adjust the recovery rate τ_{ij}. When $\tau = 0$, there is no external resource and $\tau_{ij} = 0.1$ is the initial recovery rate.

(iii) We have $C^*_{ij} \propto \tau_{ij} \propto \tau$. The bigger τ is, the higher τ_{ij} is, and then the closer C^*_{ij} is to C_{ij}. It implies that, when the more external resources entering into the network are assigned to the edges, the more easily the links are recovered from the abnormal to normal state. Namely, the external resources have only positive effect on the edge e_{ij}.

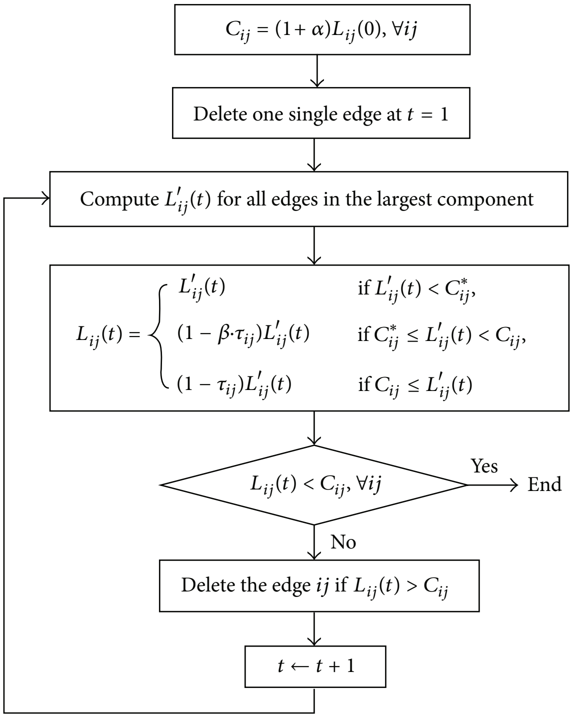

$C_{ij} = (1+\alpha)L_{ij}(0), \forall ij$
Delete one single edge at $t = 1$
Compute $L'_{ij}(t)$ for all edges in the largest component
$L_{ij}(t) = \begin{cases} L'_{ij}(t) & \text{if } L'_{ij}(t) < C^*_{ij}, \\ (1-\beta\cdot\tau_{ij})L'_{ij}(t) & \text{if } C^*_{ij} \leq L'_{ij}(t) < C_{ij}, \\ (1-\tau_{ij})L'_{ij}(t) & \text{if } C_{ij} \leq L'_{ij}(t) \end{cases}$
$L_{ij}(t) < C_{ij}, \forall ij$
Yes
End
No
Delete the edge ij if $L_{ij}(t) > C_{ij}$
$t \leftarrow t+1$

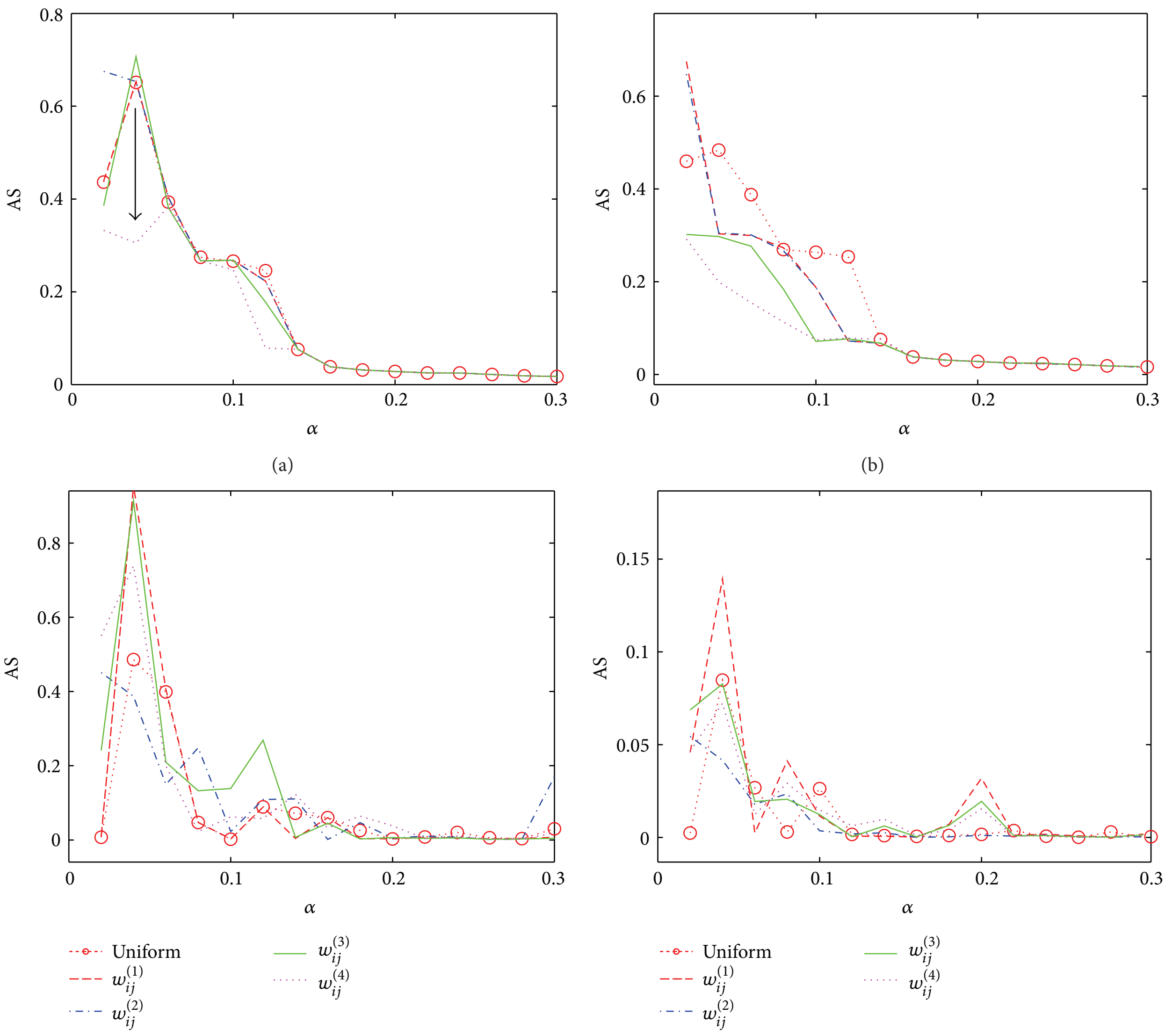
Figure 1: The evolving procedure of cascading failures in networks with the external resource τ.

We can find that such definition is rational in the actual situations and highlights the protection of the important edges. Of course, we can choose other functions of (2) and (3) satisfying these conditions.

(3) The redistribution of load: when a few edges break down, at some time t, we assume the temporary load on the edge e_{ij} as $L'_{ij}(t)$ after the redistribution of load. Then, the edge e_{ij} will get a number of external resources according to (2) once the load on e_{ij} exceeds the threshold C^*_{ij}. It means that the recovery rate τ_{ij} will work according to the degree of $L'_{ij}(t)$ exceeding the threshold C^*_{ij}. Finally, the true load $L_{ij}(t)$ on e_{ij} becomes

$$L_{ij}(t) = \begin{cases} L'_{ij}(t) & \text{if } L'_{ij}(t) < C^*_{ij}, \\ \left(1-\beta\cdot\tau_{ij}\right) L'_{ij}(t) & \text{if } C^*_{ij} \leq L'_{ij}(t) < C_{ij}, \\ \left(1-\tau_{ij}\right) L'_{ij}(t) & \text{if } C_{ij} \leq L'_{ij}(t), \end{cases} \tag{4}$$

where $\beta = (L'_{ij}(t) - C^*_{ij})/(C_{ij} - C^*_{ij})$. In fact, in (4), the final load $L_{ij}(t)$ indicates the three states of edge e_{ij}: *normal* (if $L_{ij}(t) < C^*_{ij}$); *congestion* (if $C^*_{ij} \leq L_{ij}(t) < C_{ij}$); *overloaded* (if $L_{ij}(t) \geq C_{ij}$). $C^*_{ij} \leq L_{ij}(t) \leq C_{ij}$ means that the edge deals with the load busily and still works; $L_{ij}(t) \geq C_{ij}$ implies that the edge e_{ij} cannot handle the too high a load even with the recovery mechanism, and as a result, the edge fails. Thus, a larger τ_{ij} leads to the stronger ability to handle the load on the edge, and finally the network will have the stronger robustness, which is consistent with the actual situations in



(a)

(b)

(c)

(d)

Figure 2: For SF network, after the cascade stops, the avalanche size AS as a function of α for different strategies with (a) $\tau = 20$ under HL attack, (b) $\tau = 100$ under HL attack, (c) $\tau = 20$ under RA attack, and (d) $\tau = 100$ under RA attack, respectively. Here (c) and (d) are averaged over 20 runs.

many real-world networks. Generally, the more important the edges are, the higher investment and the force are on them.

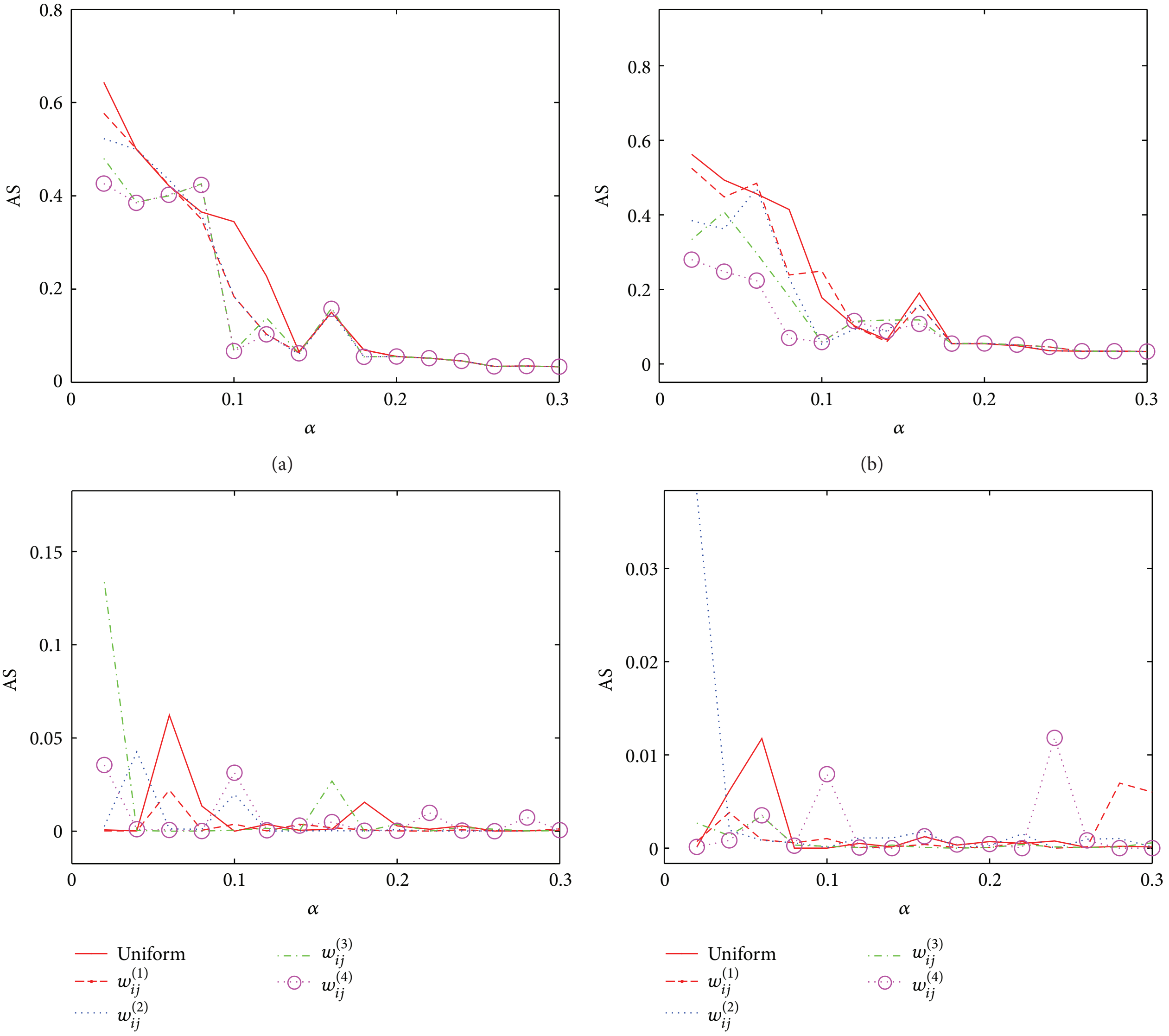
In (2), the external resource τ is assigned to the edge e_{ij} according to the weight of e_{ij}, so that (2) highlights the protection of the important edges in SF network. However, the external resources are limited and the higher τ represents the higher cost for protection. Naturally, it is needed to measure how important the edge is in order to find the efficient response strategy against disasters. This will be discussed in the following sections.

3. The Weighting Strategy

In the description of network characterization, the centrality is significant for measuring the importance of an element (node or edge) in studying cascading failures, which can be used to measure the topological position of an element in network. In this part, we will introduce four kinds of weighting methods to measure the centrality of an edge e_{ij}, which is regarded as the weight w_{ij} of e_{ij} and can reflect the importance of e_{ij} in network.

(1) The weighting strategy $w_{ij}^{(1)}$: in many real-world networks, the flows are forwarded along the edge according to the shortest path routing strategy. Thus, the edge betweenness centrality is always used to measure the centrality of the edge [52, 53], which is defined as

$$B_{ij} = \sum_{a \neq b} \frac{\sigma_{ab}\left(e_{ij}\right)}{\sigma_{ab}}, \quad (5)$$



(a)

(b)

(c)

(d)

Figure 3: For autonomous system network, after the cascade stops, the avalanche size AS as a function of α for different strategies with (a) $\tau = 20$ under HL attack, (b) $\tau = 100$ under HL attack, (c) $\tau = 20$ under RA attack, and (d) $\tau = 100$ under RA attack, respectively. Here (c) and (d) are averaged over 20 runs.

where $\sigma_{ab}(e_{ij})$ is the number of the shortest paths between the nodes a and b passing through the edge e_{ij}. Then, we define the weight of the edge e_{ij} as

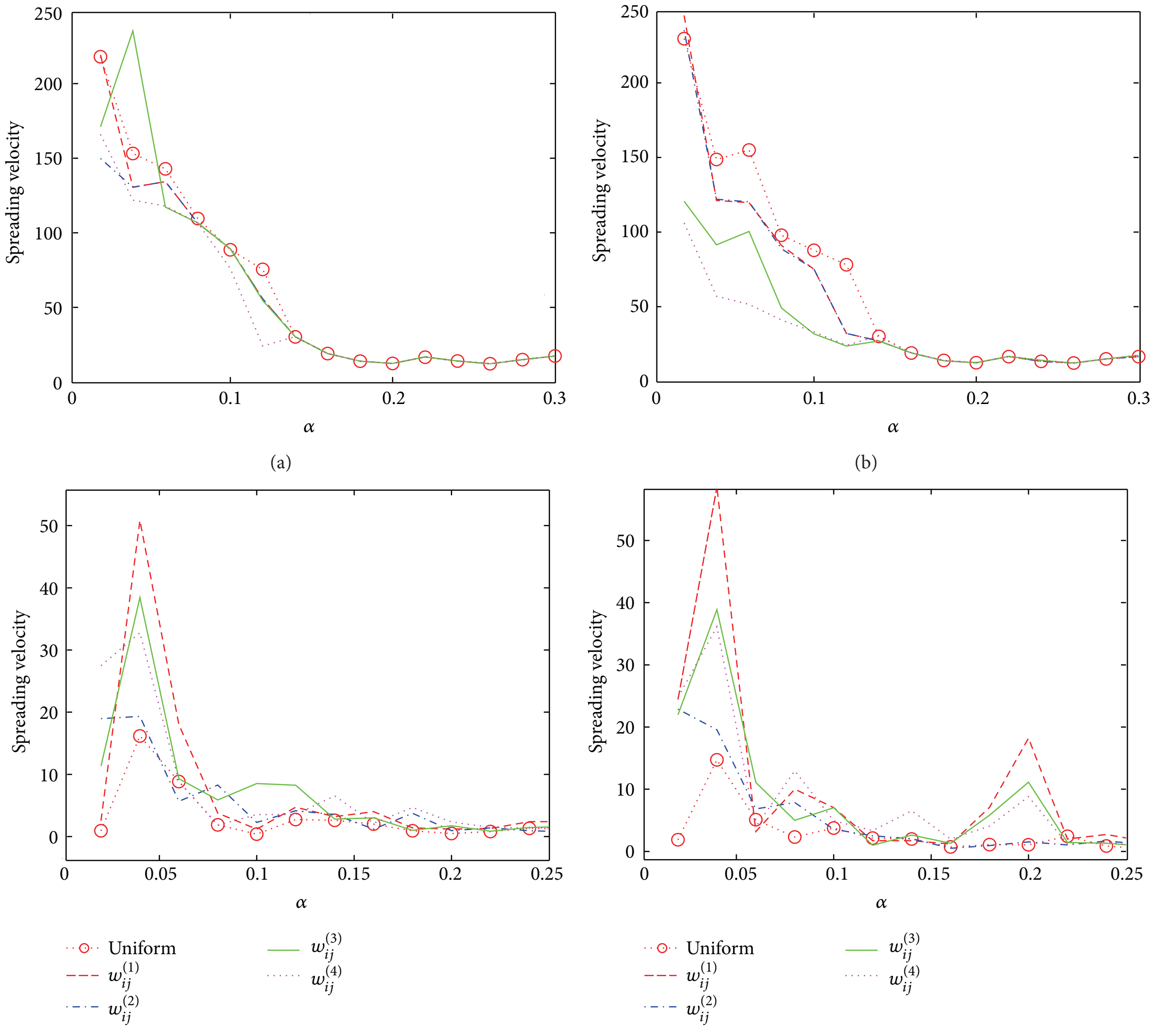
$$w_{ij}^{(1)} = B_{ij}. \tag{6}$$

(2) The weighting strategy $w_{ij}^{(2)}$: however, in real networks, the edge centrality is always related to some intrinsic quality of the end node of the edge. For example, in traffic networks, the design of the highway or the airlines always depends on the population or the economic development conditions (like GDP) among cities. These intrinsic characteristics can be seen as the quality of the node (city). The lines or roads connected to the nodes (city) with high quality always have high edge betweenness centrality, which have not been considered in the previous models yet.

Thus we define a novel edge betweenness centrality of e_{ij} as

$$B'_{ij} = \sum_{a \neq b} \frac{\sum_{k \in P_{ab}(e_{ij})} w_k}{\sum_{k \in P_{ab}} w_k}, \tag{7}$$

where P_{ab} is the set of all shortest paths between the nodes a and b, $P_{ab}(e_{ij})$ is the shortest paths between a and b passing through the edge e_{ij}, and w_k is the intrinsic quality of node k. (Here we choose the degree of node k as w_k; of course, one can choose other rational values.) Note that the definition of B'_{ij} incorporates the intrinsic characteristics of nodes with the network structure, which can better reflect the weight



(a)

(b)

(c)

(d)

Figure 4: After the cascade stops, the spreading velocity V of failures in SF network as a function of α for different strategies with (a) $\tau = 20$ under HL attack, (b) $\tau = 100$ under HL attack, (c) $\tau = 20$ under RA attack, and (d) $\tau = 100$ under RA attack, respectively. Here (c) and (d) are averaged over 20 runs.

importance of edges in actual situations. Specially, (7) will degenerate into the definition in (5) if every node has a uniform intrinsic quality ($w_k = 1$). Now we assume the weight of the edge e_{ij} as

$$w_{ij}^{(2)} = B'_{ij}. \tag{8}$$

(3) The weighting strategy $w_{ij}^{(3)}$: another centrality measure of the edge e_{ij} is the product of the nodes degree of the end node i and j, which has been used to measure the weight of the edge e_{ij} [45, 46]; that is,

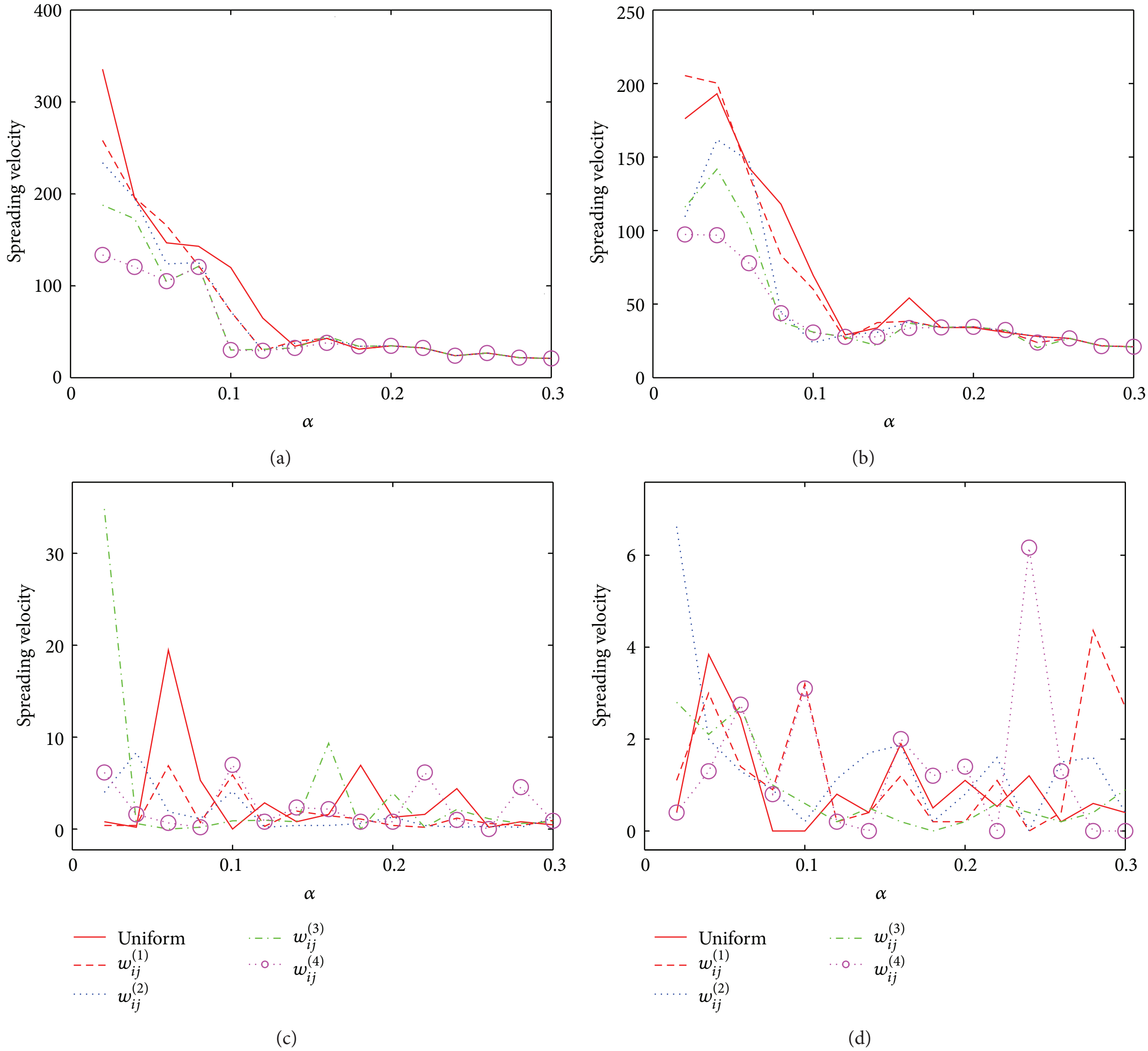
$$w_{ij}^{(3)} = \left(k_i k_j\right)^{\theta}, \tag{9}$$

where k_i and k_j are the degrees of nodes i and j, respectively. Here we assume $\theta = 1$.

(4) The weighting strategy $w_{ij}^{(4)}$: usually, the link is also important when the end of a link is important;this is in accordance with the real-world networks [45–47]. Moreover, the importance of one end i of a link e_{ij} can be measured by the node betweenness centrality [51, 53]; that is,

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

where $\sigma_{ab}(i)$ is the number of the shortest paths between the nodes a and b passing through the node i. This motivated the introduction of another weight measure for an edge. Therefore, we assume that the weight of the edge e_{ij} depends



(a)

(b)

(c)

(d)

FIGURE 5: After the cascade stops, the spreading velocity V of failures in autonomous system network as a function of α for different strategies with (a) $\tau = 20$ under HL attack, (b) $\tau = 100$ under HL attack, (c) $\tau = 20$ under RA attack, and (d) $\tau = 100$ under RA attack, respectively. Here (c) and (d) are averaged over 20 runs.

on the product of betweenness centrality of the end nodes i and j, which is defined as

$$w_{ij}^{(4)} = \left(B_i B_j\right)^{\theta}. \qquad (11)$$

Here we assume $\theta = 1$.

(5) The uniform strategy: finally, we should note that the SF network considered will become an unweighted network if every edge has the uniform weight (e.t., $w_{ij} = 1$). It means that every edge e_{ij} will get the uniform external resource according to (2). We defined this strategy as the uniform assignment strategy.

Now one can see that the external resource τ, the different weighting methods w_{ij}, and the tolerance parameter α would have great influence on the robustness of SF network subject to attacks on edges. This will be discussed in the following sections.

4. The Simulation and Analysis

In this paper, we mainly consider two kinds of attacks on one edge e_{ij}. (1) Highest-load attack (HL): we remove one edge with the highest initial load; (2) random attack (RA): we randomly choose one edge e_{ij} and then remove it. The attack originates from the removal of one edge and leads to the redistribution of load on other edges, and then some of them would fail as the load exceeds the capacity. This process is repeated until no edge fails, and at this moment, the cascade can be considered to be completed. Thus, the cascading process with the recovery mechanism τ under

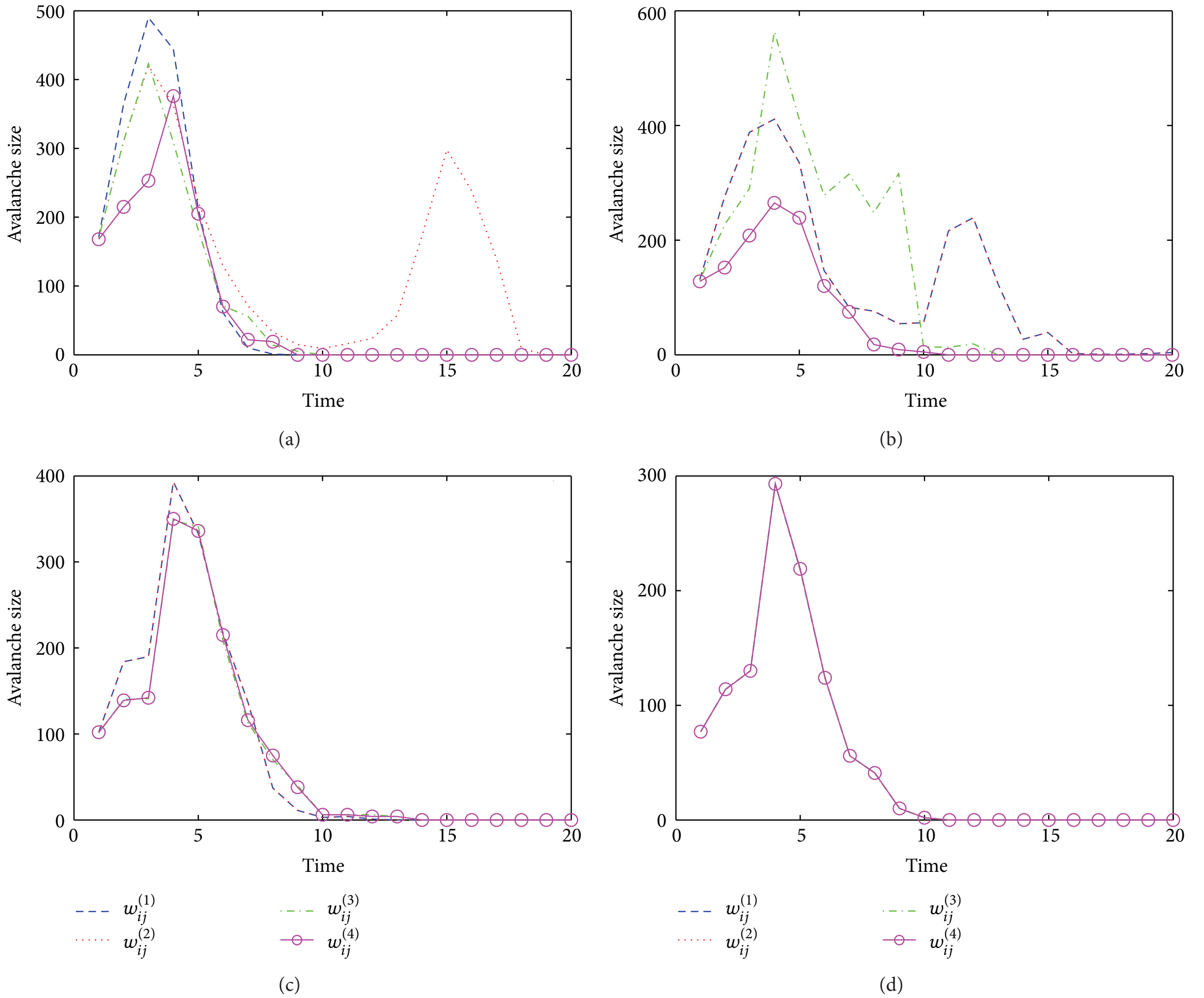


FIGURE 6: For SF network with $\tau = 20$ under HL attack, the avalanche size $N_{\text{ae}}(t)$ in each time step t as a function of t for (a) $\alpha = 0.02$, (b) $\alpha = 0.04$, (c) $\alpha = 0.06$, and (d) $\alpha = 0.08$, respectively.

edge-based attacks can be described in Figure 1. Now, in the following section, we will reveal the function of the recovery mechanism on the network robustness against cascading failures from three aspects: improving the integral robustness, controlling the spreading velocity of cascading failures, and controlling the burst of cascading failures.

4.1. Improving the Integral Robustness against Cascading Failures. Now, in the first part of this section, we focus on the function of the recovery mechanism on improving the robustness of the heterogeneous scale-free network (SF) against cascading failures, which is quantified by the following metrics: the avalanche size (AS) after cascade failures which is defined as follows:

$$\text{AS} = \frac{\sum_t N_{\text{ae}}(t)}{N_e - 1}, \qquad (12)$$

where $N_{\text{ae}}(t)$ and N_e are the number of the avalanched edges at each time step t under attack and the total number of edges in initial networks, respectively. From (12), we can see that the metric AS can be regarded as a function of α and τ, and then AS could quantify the integral robustness of structure against cascading failures.

From Figures 2(a) and 2(b), it is clear that, for SF network model and the autonomous system network AS1470 subject to HL attack, as the external resources τ are assigned to the edges according to the weighting method $w_{ij}^{(4)}$, it could be better at decreasing the avalanche size (AS) thus improving the integrity of SF networks than other strategies. Especially, the effect is obvious for smaller tolerance parameter α ($\alpha < 0.2$) and more external resources ($\tau = 100$). For example, as $\alpha = 0.04$ and $\tau = 20$, the weighting method $w_{ij}^{(4)}$ could decrease the avalanche size AS from about 0.71 to 0.3 (see the arrow in Figure 2(a)). The simulations of the real-world networks (AS1470) have proved these findings (see Figures 3(a) and 3(b)). Moreover, as shown in Figures 2(b) and 3(b), the weighting method $w_{ij}^{(3)}$ is suboptimal and the uniform

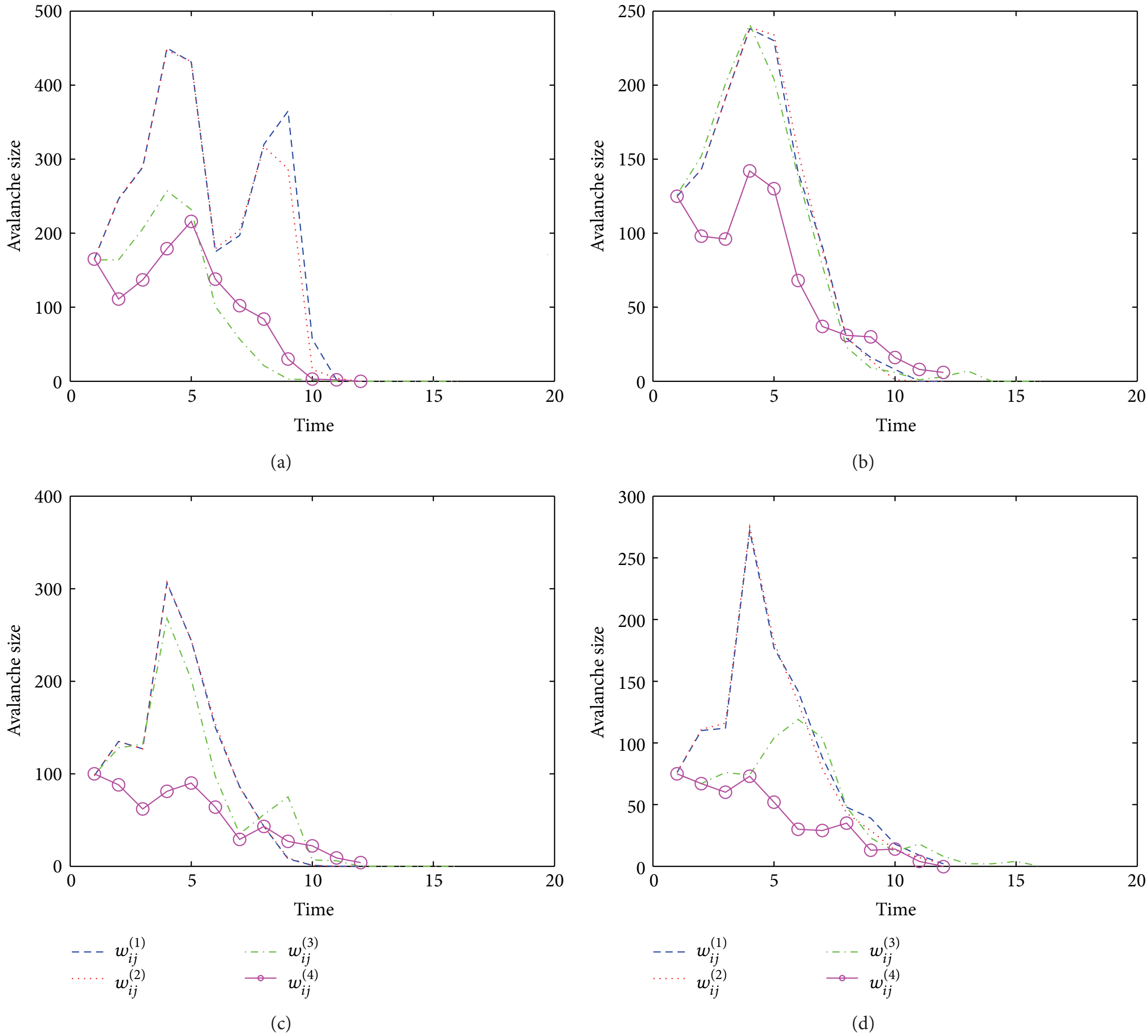


FIGURE 7: For SF network with $\tau = 100$ under HL attack, the avalanche size $N_{\text{ae}}(t)$ in each time step t as a function of t for (a) $\alpha = 0.02$, (b) $\alpha = 0.04$, (c) $\alpha = 0.06$, and (d) $\alpha = 0.08$, respectively.

method ($w_{ij} = 1$) is the worst. Although the weighting method $w_{ij}^{(4)}$ is optimal, it depends on the betweenness centrality of the nodes that needs to know the whole topological structure of SF network from (11). It implies that the third weighting strategy $w_{ij}^{(3)}$ is suggested if we only knew the local structure of networks, such as the degree of nodes.

On the other hand, as shown in Figures 2(c), 2(d), 3(c), and 3(d), under RA attack, the difference among the four kinds of weighting strategies is not clear if with fewer external resource (e.g., $\tau = 20$). But, as $\alpha \geq 0.1$, it seems that the second weighting strategy $w_{ij}^{(2)}$ and the uniform assignment strategy ($w_{ij} = 1$) are optimal if with sufficient external resource (e.g., $\tau = 100$).

4.2. Controlling the Spreading Velocity of Cascading Failures. In the second part of this section, to further measure how efficient the different weighting strategies are in response to the cascading failures in SF network, we will explore the spreading velocity of cascading failures, which is computed by V:

$$V = \frac{\sum_t N_{\text{ae}}(t)}{T}, \qquad (13)$$

where $N_{\text{ae}}(t)$ is the number of the avalanched edges at each time step t under attacks and T is the evolving time step of cascading propagation in networks (see Figure 1).

As shown in Figures 4(a), 4(b), 5(a), and 5(b), under HL attack, the weighing method $w_{ij}^{(4)}$ can obviously reduce the spreading velocity of cascading failures in both the SF network model and AS1470 network, regardless of the quantity of external resources τ. Moreover, the third weighting method $w_{ij}^{(3)}$ is suboptimal if having more resources

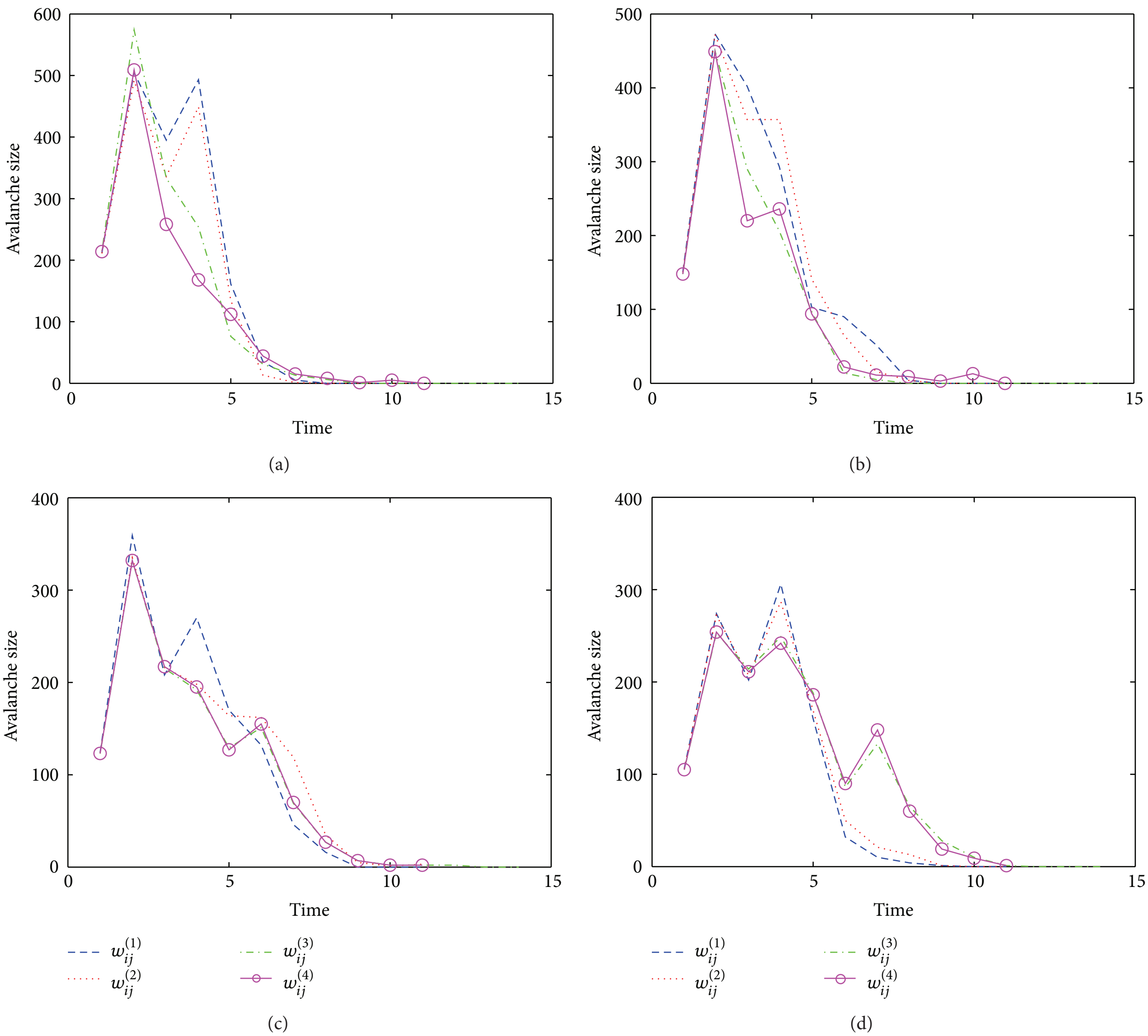


Figure 8: For autonomous system network with $\tau = 20$ under HL attack, the avalanche size $N_{\text{ae}}(t)$ in each time step t as a function of t for (a) $\alpha = 0.02$, (b) $\alpha = 0.04$, (c) $\alpha = 0.06$, and (d) $\alpha = 0.08$, respectively.

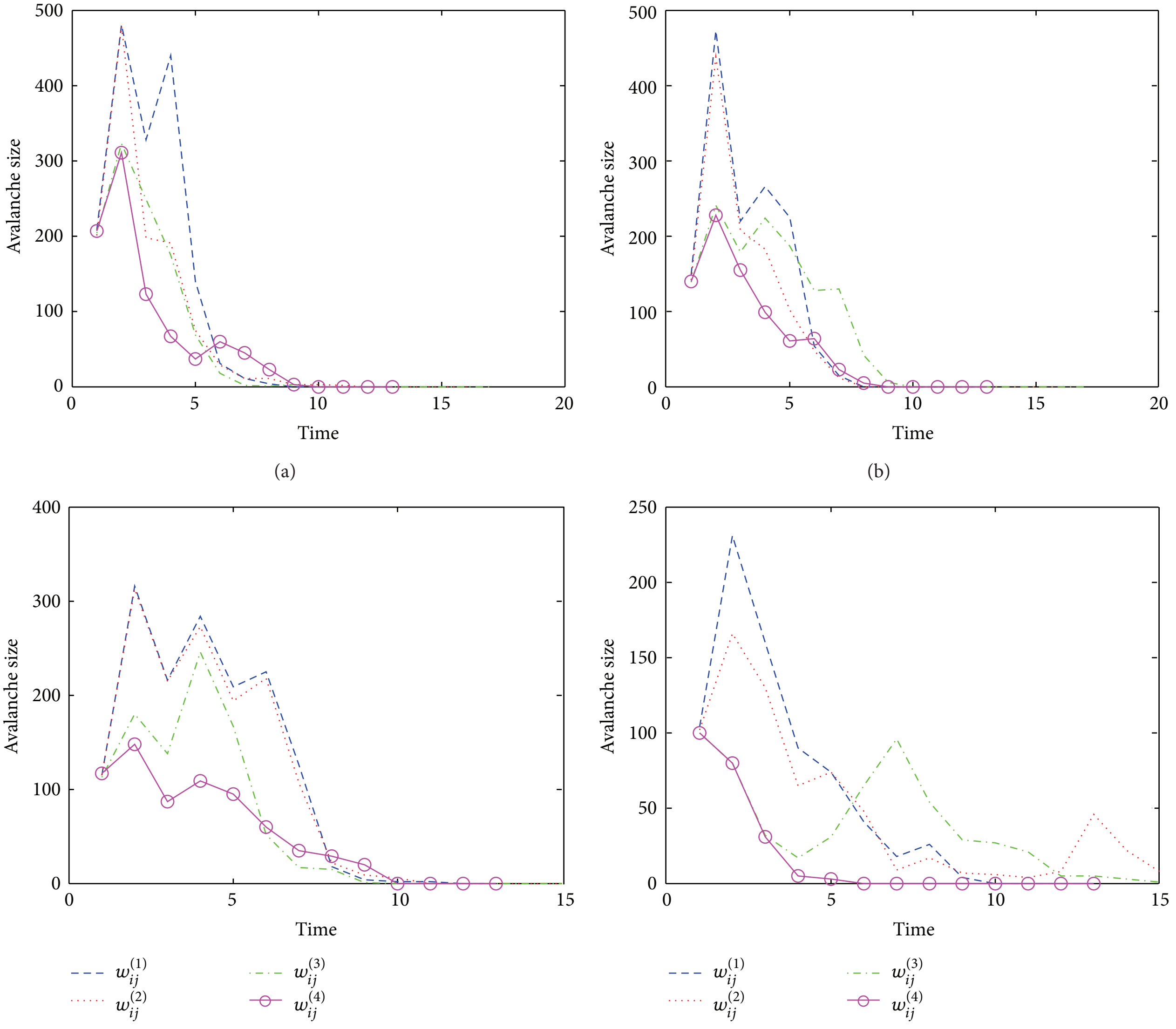
(e.g., $\tau = 100$). It reveals that, under HL attack, the external resource assigned to edges according to the method $w_{ij}^{(4)}$ can control the spreading speed V of cascading failures in heterogeneous scale-free networks more efficiently.

4.3. Controlling the Process of Cascading Failures. In the previous two parts of this section, the function of different weighting methods on improving the robustness of networks against cascading failures has been shown. However, another question that whether the weighting methods could control the outbreak of cascading failures also should be considered. In this part of this section, we focus on controlling the process of cascading failures in networks and plot the avalanche size $N_{\text{ae}}(t)$ in each time step t under HL attack to explore this question.

As shown in Figures 6 and 7, under HL attack with different tolerance parameters α ($\alpha = 0.02$, 0.04, 0.06, and 0.08), we can see that the weighting method $w_{ij}^{(4)}$ can more effectively control the outburst of cascading failures in SF network model than other methods. Especially, with more external resources ($\tau = 100$), the more obviously can $w_{ij}^{(4)}$ reduce the peak of cascading failures (see Figure 7). Moreover, the simulations of the autonomous system AS1470 also show the similar findings (see Figures 8 and 9).

5. Conclusion

In this paper, we study the cascading dynamics of heterogeneous scale-free (SF) network with the recovery mechanism subject to edge-based attack. The recovery mechanism is



(a)

(b)

(c)

(d)

FIGURE 9: For autonomous system network with $\tau = 100$ under HL attack, the avalanche size $N_{\text{ae}}(t)$ in each time step t as a function of t for (a) $\alpha = 0.02$, (b) $\alpha = 0.04$, (c) $\alpha = 0.06$, and (d) $\alpha = 0.08$, respectively.

represented by the external resources τ that are distributed to the edge e_{ij} according to five kinds of weighting strategies: $w_{ij}^{(1)}$, $w_{ij}^{(2)}$, $w_{ij}^{(3)}$, $w_{ij}^{(4)}$, and the uniform strategy. We mainly investigate the influence of τ and different weighting strategies on the cascading dynamics of SF networks subject to intentional attack and random breakdown. On the whole, the main contributions of this paper are listed as follows.

(1) Under intentional attack, $w_{ij}^{(4)}$ is the most efficient response strategy against cascading failures in SF networks, which can obviously improve the integral robustness, simultaneously reduce the spreading speed, and control the outbreak of cascading failures in SF networks. Especially, the more external resources are, the more efficient $w_{ij}^{(4)}$ is. The uniform assignment strategy is the worst strategy.

(2) Although the method $w_{ij}^{(4)}$ is optimal, it needs to compute the betweenness centrality of node that depends on the whole structure of networks. Therefore, $w_{ij}^{(3)}$ will be optimal if we only knew the local structure of SF network (e.g., the degree of nodes). The simulations of autonomous system network have proved these results. However, the recent research [54] has shown that, the node betweenness centrality can be approximately estimated by using the local information of nodes in order to reduce the computational complexity in large networks. This implies that the weighting method $w_{ij}^{(4)}$ defined in this paper has great significance in the protection of actual scale-free networks.

(3) Under random breakdown, although the difference among the five kinds of weighting methods is not

clear in terms of the protection result against cascading effect, the uniform assignment strategy ($w_{ij} = 1$) can better decrease the spreading velocity of failures in SF network than other strategies.

The results remind us to take different actions on handling and controlling the emergent disasters in heterogeneous SF networks. Here we just highlight the protection of the important links. Our approach makes contributions to understanding the dynamics of disaster spreading and provides some possible countermeasures to control the disasters and finally to repair the system damaged.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant nos. 61202362, 61121061, 61262057, 61372191, 11301302, and 91124002), State Key Development Program of Basic Research of China 973 (Grant nos. 2013CB329601 and 2011CB302600), National Key Technology Program (Grant no. 2012BAH38B-04), China Postdoctoral Science Foundation Program (2013M542560, BS2013SF009, 2012m520114, and 2013T60037), and 863 programs (Grant nos. 2012AA01A401, 2010AA-012505, and 2011AA010702).

References

[1] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attacktolerance of complex networks," *Nature*, vol. 406, pp. 378–382, 2000.

[2] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, "Network robustness and fragility: percolation on random graphs," *Physical Review Letters*, vol. 85, no. 25, pp. 5468–5471, 2000.

[3] A. E. Motter, "Cascade control and defense in complex networks," *Physical Review Letters*, vol. 93, no. 9, Article ID 098701, 2004.

[4] 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.

[5] R. Pastor-Satorras, A. Vázquez, and A. Vespignani, "Dynamical and correlation properties of the internet," *Physical Review Letters*, vol. 87, no. 25, Article ID 258701, 4 pages, 2001.

[6] 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.

[7] A. Santiago and R. M. Benito, "Robustness of heterogeneous complex networks," *Physica A*, vol. 388, no. 11, pp. 2234–2242, 2009.

[8] Y. X. Xia and D. J. Hill, "Attack vulnerability of complex communication networks," *IEEE Transactions on Circuits and Systems II*, vol. 55, no. 1, pp. 65–69, 2008.

[9] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Physical Review E*, vol. 65, no. 5, Article ID 056109, 2002.

[10] 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.

[11] S. V. Buldyrev, N. W. Shere, and G. A. Cwilich, "Interdependent networks with identical degrees of mutually dependent nodes," *Physical Review E*, vol. 83, no. 1, Article ID 016112, 8 pages, 2011.

[12] I. Simonsen, L. Buzna, K. Peters, S. Bornholdt, and D. Helbing, "Transient dynamics increasing network vulnerability to cascading failures," *Physical Review Letters*, vol. 100, no. 21, Article ID 218701, 2008.

[13] A. E. Motter, "Cascade control and defense in complex networks," *Physical Review Letters*, vol. 93, no. 9, Article ID 098701, 4 pages, 2004.

[14] L. K. Gallos, R. Cohen, P. Argyrakis, A. Bunde, and S. Havlin, "Stability and topology of scale-free networks under attack and defense strategies," *Physical Review Letters*, vol. 94, no. 18, Article ID 188701, 2005.

[15] L. Buzna, K. Peters, H. Ammoser, C. Kühnert, and D. Helbing, "Efficient response to cascading disaster spreading," *Physical Review E*, vol. 75, no. 5, Article ID 056107, 7 pages, 2007.

[16] B. A. Rezaei, N. Sarshar, V. P. Roychowdhury, and P. O. Boykin, "Disaster management in power-law networks: recovery from and protection against intentional attacks," *Physica A*, vol. 381, no. 1-2, pp. 497–514, 2007.

[17] K. Peters, L. Buzna, and D. Helbing, "Modelling of cascading effects and efficient response to disaster spreading in complex networks," *International Journal of Critical Infrastructures*, vol. 4, no. 1-2, pp. 46–62, 2008.

[18] R. Yang, W.-X. Wang, Y.-C. Lai, and G.-R. Chen, "Optimal weighting scheme for suppressing cascades and traffic congestion in complex networks," *Physical Review E*, vol. 79, no. 2, Article ID 026112, 2009.

[19] B.-L. Dou, X.-G. Wang, and S.-Y. Zhang, "Robustness of networks against cascading failures," *Physica A*, vol. 389, no. 11, pp. 2310–2317, 2010.

[20] J. Domingo-Ferrer and U. González-Nicolás, "Decapitation of networks with and without weights and direction: the economics of iterated attack and defense," *Computer Networks*, vol. 5, no. 1, pp. 119–130, 2011.

[21] M. Ouyang, L. Hong, Z.-J. Mao, M.-H. Yu, and F. Qi, "A methodological approach to analyze vulnerability of interdependent infrastructures," *Simulation Modelling Practice and Theory*, vol. 17, pp. 817–828, 2009.

[22] 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.

[23] 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.

[24] 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.

[25] J.-W. Wang and L. Rong, "Robustness of the western United States power grid under edge attack strategies due to cascading failures," *Safety Science*, vol. 49, pp. 807–812, 2011.

[26] H. Ren and I. Dobson, "Using transmission line outage data to estimate cascading failure propagation in an electric power system," *IEEE Transactions on Circuits and Systems Part II*, vol. 55, no. 9, pp. 927–931, 2008.

[27] 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.

[28] M.-G. Hua, P. Cheng, J.-T. Fei, J.-Y. Zhang, and J.-F. 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.

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

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

[31] 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.

[32] 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.

[33] J.-X. 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.

[34] X. Q. 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, 2011.

[35] W. Li, A. Bashan, S. V. Buldyrev et al., "Cascading failures in interdependent lattice networks: the critical role of the length of dependency links," *Physical Review Letters*, vol. 108, Article ID 228702, 2012.

[36] M. Li and W. Zhao, "Representation of a stochastic traffic bound," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1368–1372, 2010.

[37] M. Li, W. Zhao, and C. Cattani, "Delay bound: fractal traffic passes through servers," *Mathematical Problems in Engineering*, vol. 2013, Article ID 157636, 15 pages, 2013.

[38] S. He, Z. Ding, and F. Liu, "Output regulation of a class of continuous-time Markovian jumping systems," *Signal Processing*, vol. 93, no. 2, pp. 411–419, 2013.

[39] S. He and F. Liu, "Finite-time H_∞ control of nonlinear jump systems with time-delays via dynamic observer-based state feedback," *IEEE Transactions on Fuzzy Systems*, vol. 20, no. 4, pp. 605–614, 2012.

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

[41] F. Holme and B. J. Kim, "Vertex overload breakdown in evolving networks," *Physical Review E*, vol. 65, no. 6, Article ID 066109, 2002.

[42] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Physical Review E*, vol. 69, Article ID 045104, 4 pages, 2004.

[43] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the North American power grid," *European Physical Journal B*, vol. 46, no. 1, pp. 101–107, 2005.

[44] D. Heide, M. Schafer, and M. Greiner, "Robustness of networks against fluctuation-induced cascading failures," *Physical Review E*, vol. 77, no. 5, Article ID 056103, 2008.

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

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

[47] J.-W. Wang and L.-L. Rong, "A model for cascading failures in scale-free networks with a breakdown probability," *Physica A*, vol. 388, no. 7, pp. 1289–1298, 2009.

[48] S. J. Qin, Y. Chen, and M. Yang, "A edge-based-attack robust model of capacity for cascading failures," in *Proceedings of the IEEE International Conference on Advanced Computer Control (ICACC '10)*, pp. 136–139, March 2010.

[49] W.-X. Wang and Y.-C. Lai, "Abnormal cascading on complex networks," *Physical Review E*, vol. 80, no. 3, Article ID 036109, 2009.

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

[51] 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*, pp. 177–187, Chicago, Ill, USA, August 2005.

[52] M. Girvan and M. E. J. Newman, "Community structure in social and biological networks," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 99, no. 12, pp. 7821–7826, 2002.

[53] 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.

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