Robustness of Random Scale-Free Networks against Cascading Failure under Edge Attacks

Lin Ding[1,2] and Minsheng Tan[1]
[1]School of Computer Science and Technology, University of South China, Hengyang 421001, China
[2]Department of Electrical and Computer Engineering, University of British Columbia, Vancouver V6T 1Z4, Canada
Email: {linding1981, tanminsheng65}@163.com

Abstract—The effect of two different edge attacks on the robustness of random scale-free networks against cascading failure is investigated by establishing a cascading failure model for random scale-free networks. In this model, the initial load of an edge is defined as a nonlinear function of the product of the betweenness of its end nodes with an adjustable parameter, and the local preferential redistribution rule is applied to assign the broken edge's load. An interesting conclusion is reached through theoretical analyses and numerical simulations: there is a threshold of the load parameter. When the value of the load parameter is larger than this threshold, attacking the edges with the higher load can result in larger cascading failures; while for the case of the parameter value smaller than the threshold, attacking the edges with the lower load will be more likely to lead to global collapse. Furthermore, the threshold value has a close relation with the degree exponent of the network. This work will be not only helpful to protect the key edges selected effectively to resist the cascading failure, but also useful in the design of high-robustness networks in order to stand against all kinds of attacks.

Index Terms—Cascading failure, random scale-free network, robustness, edge attacks

I. Introduction

Large networked systems are the basic support of modern infrastructures, such as information communication networks, the Internet, power grids and transportation networks. In network science, all these real-world networks can be illustrated by complex networks. Evidence has demonstrated that in realistic complex networks, a large influence even global collapse can be triggered by the breakdown of a few components (nodes or edges) or even a single component caused by intentional attacks or random failures through the mechanism of cascading. Typical examples are breakdowns of the Internet [1] and several large blackouts of the power grid in some countries [2]. To keep these networks' safe and stable running under any condition, cascading failures robustness of complex networks under component attacks or failures becomes a hot topic, as known that the cascading disasters directly affect the quality of people's lives and bring immeasurable economic loss to us.

Up to now, a great number of works have been devoted to exploring the cascading phenomenon in complex networks, especially in scale-free networks, and many valuable results have been found, focusing on model approaches of cascading failures [3]-[7], effective protection and attack strategies [8]-[13], the cascade mechanism and control measures [14]-[20], the percolation in interdependent networks [21], [22], and so on. When modeling cascading fails, there are generally two ways of assigning the initial load on a component and the failed components' loads, including global and local strategies [3], [6]. In global strategies, both the definition of the initial load and the redistribution of the failed components' loads are according to the global topological information such as the betweenness. Applying the global methods, many studies investigated cascade-based attacks and showed that scale-free networks are robust to random failures of components, but, at the same time, very fragile to intentional attacks such as the removal of the components with the highest load [8]. This phenomenon is rooted in the heterogeneity of the load distribution originating from the network structure. However, calculating the global load always needs the global information in real time, which is not readily available in a large-scale network. Therefore, considering the simplicity of the local information such as degree, many researchers adopted the local strategies to assign loads and constructed different cascading models. In fact, it may be more realistic to consider the load dynamics of the cascading phenomenon from a combined view. For example, in the Internet or the power grids, in which the normal and steady load is formed from a long time evolving, the initial load should be treated from a global view, e.g., considering the whole network topology. But when cascading failures occur, the load redistribution should be a transient action, and naturally, the load passing through a failed component will be directly redistributed among its neighbors. From this combined perspective, the authors of [7] discussed cascading behaviors of different networks. They found that the networks have the best robustness if the load of each edge is the multiplication of the betweenness of the

Manuscript received October 22, 2016; revised December 22, 2016.
This work was supported by the National Natural Science Foundation of China under Grant No. 61403183, the Natural Science Foundation of Hunan Province of China under Grant No.2015JJ6096, the Philosophy Social Science Foundation of Hunan Province of China under Grant No.14YBA340 and the Education Department Foundation of Hunan Province of China under Grant No.14C1006.
Corresponding author email: linding1981@163.com.
doi: 10.12720/jcm.11.12.1088-1094

end nodes. Their work revealed that adjusting initial load distribution can significantly improve the robustness of scale-free networks. Such "soft" protection mechanism is regarded to have practical application because it does not require the changes of network connection and capacity layout. However, they investigated the whole robustness characteristic of the networks by cutting each edge, without considering the effect of different edge failures on network vulnerability. Furthermore, most existing studies on cascading failure robustness of scale-free networks are based on Barabási and Albert (BA) model, but they are not conformed to the real network because the degree exponent of the BA model is a constant.

In the present work, we follow the research of [7] by considering a new cascading model for random scale-free networks, wherein the cascading process is triggered by two different attacks on network edges, namely attacking the edges with the highest load and with the lowest load. The effect of two attacks on the network robustness against cascading failures in our cascading model is analyzed theoretically and numerically. It is found that there exists a threshold θ_c of model parameter θ that controls the distribution of the initial load on each edge. When $\theta = \theta_c$, the network preserves its robustness against both types of attacks; while for $\theta < \theta_c$, as unexpected, attacking the edges with the lowest load can damage the network more severely than the other one. Furthermore, the value of θ_c strongly depends on the degree exponent of the network. This paper may have practical implication for developing effective attacking/protecting and soft designing high-robustness networks for future real systems.

The rest of this paper is organized as follows: in Sec. II, we describe the cascading model of a random scale-free network in detail. In Sec. III, we discuss the effect of the model parameters on network robustness by the theoretical analysis and simulation. Finally, some summaries and conclusions are stated in Sec. IV.

The model

It has been proposed that many real-world networks show power-law degree distribution, and are termed as scale-free. There are many models which reproduce such scale-free features. BA model is the well-known one of them, in which the degree exponent γ of the produced network is constant 3. Actually, for most real networks, the γ is varying values, which has turned out to be sensitive to the detail of network structure [23]. Thus, we consider the random scale-free network [24] as the physical infrastructure in which a cascading process takes place. The network starts as N nodes, which are indexed by an integer i ($i = 1, \cdots N$). For each node, there is a weight $p_i = i^{-\alpha}$, where a is a control parameter in $[0,1)$. Then two different nodes i and j are selected with probabilities equal to the normalized weights, $p_i / \sum_k p_k$ and $p_j / \sum_k p_k$, respectively, and a new edge is added between them unless one exists already. This process is repeated until mN edges are made and N nodes are connected completely in the network. The resulting network achieves power-law degree distribution, $p(k) \sim k^{-g}$, where γ is given by $\gamma = (1+\alpha)/\alpha$. Thus, adjusting the parameter a in $[0,1)$, various values of the degree exponent γ can be obtained in the range $2 < \gamma < \infty$. In the present work, the total network size is fixed as $N = 200$ and the parameter is set to be $m = 2$ (hence the mean degree $< k >= 2m = 4$ [24]).

With the random scale-free networks at hand, let us define the cascading model based on edge failure. As is known, in real-world networks, complex networks generally transport load flow closely related to our daily life. Under normal circumstances, such flow keeps a balanced state as a result of a long time evolving, and the system maintains its normal and efficient functioning. However, due to either random breakdowns or intentional attacks, the failures of some edges may cause loads to redistribute among other edges in the network, which may trigger more edges' failure and even entire collapse of the network.

Inspired by the above consideration, we assume the initial load of an edge ij before attack to be

$$L_{ij} = (B_i B_j)^{\theta} \tag{1}$$

where $\theta \geq 0$ is an adjustable parameter and controls the distribution of the initial load, and B_i and B_j are the betweenness of nodes i and j, respectively. The betweenness of a node i is defined as follows:

$$B_i = \sum_{s \neq t} \frac{\sigma_{st}(i)}{\sigma_{st}} \tag{2}$$

where σ_{st} is the number of shortest paths from the node s to node t and $\sigma_{st}(i)$ is the number of these shortest paths making use of node i. Compared with the widely-used betweenness, the definition of this generalized betweenness considers the two end points of each shortest path, and thus avoiding the possibility that some edges may bear no loads at all. At the same time, the ranking of edge betweenness centrality keeps the same. From (1), we can see that the load on an edge has a power-law dependence on the product of betweenness of its two end nodes. This is supported by empirical evidence of real networks [7]. As an example, when a data packet is sent from one position to another through scale-free networks such as the Internet, the links between central points of high betweenness are more probable to be chosen because it can be efficient to get to the destination along them.

As every edge has some limited capacity determining the load-carrying ability which is generally constrained

by cost, it is reasonable to assume that the capacity C_i of edge ij is proportional to its initial load, that is

$$C_{ij} = (1+\beta)L_{ij} \tag{3}$$

where $\beta \geq 0$ is a tolerance parameter, which guarantees that initially there are no overloaded edges. Obviously, the bigger β is, the more ability the edges possess to handle the extra load, but the higher building the network costs. Therefore, there should be explored to build the strong robustness network against cascading failure with the minimum cost.

Here we focus on cascades triggered by a small attack, e.g., removal of a single edge. The load flow along the broken edge will be redistributed to the other edges in the network. Different from the load global redistribution rule, considering that the load redistribution is a transient action, the load on the failed edge must pass its nearest-neighbor edge. So the load local preferential redistribution rule is applied [6]. To be specific, the additional load ΔL_{im} that a neighboring edge im receives from the failed edge ij is proportional to its capacity, i.e.,

$$\Delta L_{im} = L_{ij} \frac{C_{im}}{\sum_{a\in\Gamma_i} C_{ia} + \sum_{b\in\Gamma_j} C_{jb}} \tag{4}$$

where Γ_i and Γ_j are the sets of neighboring nodes of i and j, respectively. This rule for the load redistribution is based on the observation in real-world networks like the Internet. If a line fails, it is reasonable to preferentially reroute traffic along those higher-capacity edges to avoid further congestions.

In this scheme, for a neighbor im of the edge ij, if

$$L_{im} + \Delta L_{im} > C_{im} \tag{5}$$

then the edge im will break apart, inducing further redistribution of its load of $L_{im} + \Delta L_{im}$ according to (4) and potentially more edges might break. Cascading failure continues as long as there is an edge whose load exceeds its capacity.

In previous studies, there are generally two cascade-based attacking strategies: random attack and intentional attack. The former is to attack some randomly chosen components. The latter is to attack the important components, which are usually considered to be the ones with the highest load. Undoubtedly, if a network is robust under intentional attacks, it will be capable of withstanding all of the attacks. Since scale-free networks are robust to random attack but fragile to intentional attack, a critical question is that how to choose the important components to execute the intentional attack, or is it always more influential for the network to attack its components with the higher load than the ones with the lower load. From this issue, two intentional attack strategies are considered in our cascading model. One is called HL strategy that attacks the edges with the highest load. The other is called LL strategy that attacks the edges with the lowest load.

The damage caused by a cascade-based attack is quantified in terms of the number of broken edges after the cascading process is over. We use CF_{ij} to denote the avalanche size induced by removing edge ij and calculate the consequence after every attacked edge fails. Since $0 \leq CF_{ij} \leq E-1$, we adopt the normalized avalanche size, i.e., $CF_{attack} = \sum_{ij\in A} CF_{ij} / (N_A(E-1))$, where E represents the total number of edges in the network, and A and N_A represents the set and the number of edges attacked, respectively. Apparently, the lower the value of CF_{attack}, the stronger the robustness of the network against cascading failure.

II. Analysis and Simulation Results

Based on the mechanism of load redistribution in the cascading model, when the edge ij fails, to avoid the emergence of cascading failure, the following condition should be satisfied:

$$L_{im} + \Delta L_{im} \leq C_{im} \tag{6}$$

According to the definitions of L_{im} and ΔL_{im}, the above (6) can be rewritten as:

$$L_{im} + L_{ij} \frac{(B_i B_m)^\theta}{\sum_{a\in\Gamma_i} (B_i B_a)^\theta + \sum_{b\in\Gamma_j} (B_j B_b)^\theta} \leq (1+\beta)(B_i B_m)^\theta \tag{7}$$

In the cascading process, an edge' load will be undoubtedly greater than its initial load, that is:

$$\begin{aligned} L_{im} &\geq (B_i B_m)^q \\ L_{ij} &\geq (B_i B_j)^q . \end{aligned} \tag{8}$$

By inserting (8) into (7), we can get

$$\frac{(B_i B_j)^\theta}{\sum_{a\in\Gamma_i} (B_i B_a)^\theta + \sum_{b\in\Gamma_j} (B_j B_b)^\theta} \leq \beta \tag{9}$$

Since the relation of betweenness and degree meets the following equation [24]:

$$B \sim k^{(\gamma-1)/(\delta-1)} \tag{10}$$

where γ and δ are the power-law parameters of degree distribution, $P(k) \sim k^{-\gamma}$, and betweenness distribution, $P(B) \sim B^{\delta}$, respectively. Substituting (10) into (9), and let $\theta(\gamma-1)/(\delta-1) = \lambda$, then we can get

$$\frac{1}{\sum_{a\in\Gamma_i} (k_i k_a)^\lambda + \sum_{b\in\Gamma_j} (k_j k_b)^\lambda} (k_i k_j)^\lambda \leq \beta \tag{11}$$

According to the knowledge of degree and probability, we know

$$\sum_{a\in\Gamma_i} k_a^{\lambda} = k_i \sum_{k'=k_{\min}}^{k_{\max}} P(k'|k_i) k'^{\lambda} \tag{12}$$

where $k_{\min}$ and $k_{\max}$ are the minimum and the maximum node degrees, and $P(k'|k_i)$ is the conditional probability that a node of k_i has a neighbor of k'. Since most scale-free networks such as random scale-free networks in the present work have no degree-degree correlation, $P(k'|k_i) = k'P(k')/<k>$. So we can get

$$\sum_{a\in\Gamma_i} k_a^{\lambda} = k_i \sum_{k'=k_{\min}}^{k_{\max}} \frac{k'P(k')k'^{\lambda}}{<k>} = \frac{k_i <k^{\lambda+1}>}{<k>} \tag{13}$$

$$\sum_{b\in\Gamma_j} k_b^{\lambda} = k_j \sum_{k'=k_{\min}}^{k_{\max}} \frac{k'P(k')k'^{\lambda}}{<k>} = \frac{k_j <k^{\lambda+1}>}{<k>} \tag{14}$$

Based on (13) and (14), (11) can be expressed by:

$$\frac{<k>}{<k^{\lambda+1}>} \frac{1}{\frac{k_i}{k_j^{\lambda}} + \frac{k_j}{k_i^{\lambda}}} \le \beta \tag{15}$$

Since

$$\frac{k_i}{k_j^{\lambda}} + \frac{k_j}{k_i^{\lambda}} \ge \frac{2}{(k_i k_j)^{\frac{\lambda-1}{2}}} \tag{16}$$

from (15), we can get

$$\frac{<k>(k_i k_j)^{\frac{\lambda-1}{2}}}{2<k^{\lambda+1}>} \le \beta \tag{17}$$

According to (10), for scale-free networks, $k \sim B^{(d-1)/(g-1)}$, then (17) is rewritten as:

$$\frac{(B_i B_j)^{\frac{1}{2}(\theta-\frac{\delta-1}{\gamma-1})} < B^{\frac{\delta-1}{\gamma-1}} >}{2<B^{(\theta+\frac{\delta-1}{\gamma-1})}>} \le \beta \tag{18}$$

In order to prevent large-scale cascading failures, (18) must be satisfied. According to [24] and [25], the parameter $\frac{\gamma-1}{\delta-1}$ is a positive value. From (18), we can see that the behavior of network will be mainly determined by the expression $\theta - \frac{\delta-1}{\gamma-1}$. For detail, when $\theta - \frac{\delta-1}{\gamma-1} > 0$, namely $\theta > \frac{\delta-1}{\gamma-1}$, it is easier for the larger $B_i B_j$ to dissatisfy (18), thus the removal of edges with the larger betweenness or the higher initial load has a more important impact on the network. While for $\theta - \frac{\delta-1}{\gamma-1} < 0$, namely $\theta < \frac{\delta-1}{\gamma-1}$, in turn it is easier for the smaller $B_i B_j$ to dissatisfy (18), thus the removal of edges with the smaller betweenness or the lower initial load has a more important impact on the network. Similarly, when $\theta - \frac{\delta-1}{\gamma-1} = 0$, namely $\theta = \frac{\delta-1}{\gamma-1}$, attacking the edges with the higher initial load or the lower initial load makes no difference, so the threshold is $\theta_c = \frac{\delta-1}{\gamma-1}$.

As to the value of δ for different scale-free networks with the degree parameter γ, [24] and [25] indicated that $\delta \approx 2.2$ is a universal value in the range of $2 < \gamma \le 3$; while for $\gamma > 3$, δ depends on g in a way that it increases as g increases. As an example, when $\gamma = 3$, which corresponds to the degree exponent of the classic BA model. Adopting $\delta = 2.2$, $\theta_c = \frac{\delta-1}{\gamma-1} = 0.6$. Moreover, although we do not obtain theoretical values of δ for approximating the values of θ_c for $\gamma > 3$, we can estimate the θ_c values for $\gamma > 3$ numerically.

Next, for better understanding the cascading phenomenon and verifying the above analytic results, extensive simulation tests are performed using MATLAB.

According to our cascading model, different random scale-free networks with total size $N = 200$ and average degree $<k>=4$ can be constructed. Then, the effect of θ and γ on the robustness of random scale-free networks under the HL and the LL attacking strategies is investigated. For each strategy, 8 edges are chosen as the attacked objects. Considering the effect of the difference of the network topologies generated by the random scale-free model on simulation results, every curve in the following is obtained by averaging over experiments on 20 independent networks. In the cascading model, for a given value of g, the bigger the value θ, the higher the heterogeneity of the load distribution. Therefore, first fixing $\gamma = 3$, we focus on the effect of the load parameter θ on the robustness against cascading failure.

Fig. 1 shows the normalized avalanche size CF_{attack} under the HL strategy and the LL strategy as a function of the tolerance parameter β for $\theta = 0.2$ and $\theta = 0.4$. It is originally expected the HL strategy may be prone to trigger large-scale cascading failures than the LL. However, we can find that when $\theta = 0.2$ or $\theta = 0.4$, their LL curves locate in the right of their corresponding HL curves, which indicates that given a value of b, the values of the corresponding CF_{attack} of the LL curves are not smaller. Thus, large-scale cascading failures can be more likely to be triggered by attacking the edges with the lower load in the case of $\theta = 0.2$ or $\theta = 0.4$.

It also can be found from Fig. 1 that a phase transition occurs at a critical threshold β_c of β for each curve, where for $\beta > \beta_c$, no cascading failure arises and the network maintains its normal and efficient functioning. On the other hand, for $\beta < \beta_c$, cascading failure suddenly emerges, causing the whole or part of the network to stop working. So the lower the value of β_c, the stronger the robustness of the network. When $\theta = 0.2$ or $\theta = 0.4$, the values of β_c under the LL strategies are larger than the ones under the strategies. This reproves that in the case of $\theta = 0.2$ or $\theta = 0.4$, attacking the lower load edge is a more efficient strategy.

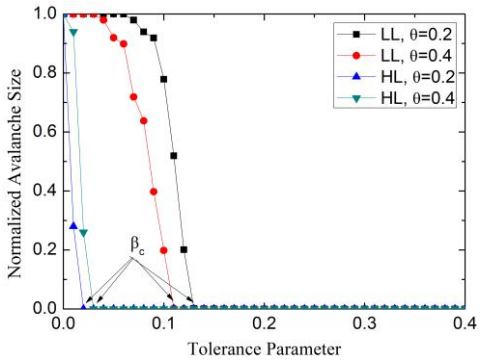


Fig. 1. Comparison between two attack strategies when $\theta = 0.2$ and $\theta = 0.4$.

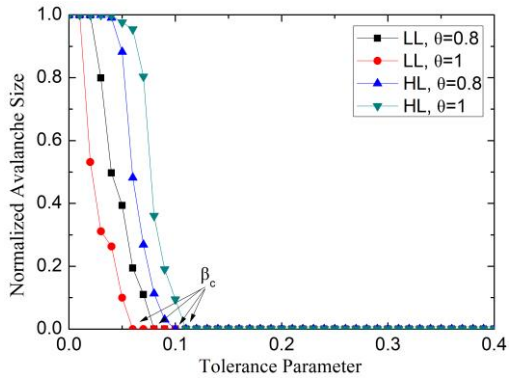


Fig. 2. Comparison between two attack strategies when $\theta = 0.8$ and $\theta = 1$.

When $\theta = 0.8$ and $\theta = 1.0$, Fig. 2 shows the relationship between the tolerance parameter β and the normalized avalanche size CF_{attack} under two attack strategies. We can observe that different from Fig. 1, the HL curves move to the right of the LL curves, and the β_c values of the HL curves become larger than the LL ones. So when $\theta = 0.8$ and $\theta = 1.0$, attacking the edges with the higher load is more prone to large-scale cascading failures, which is mainly originated from that as the value θ increases to $\theta = 0.8$ or $\theta = 1.0$, the strength of the heterogeneity of the distribution of the load makes the edges with the higher load more important. These are consistent with previous studies that attacking the components with the highest load can bring the most serious damage to the network [3], [4], [8], [17], which is a special case of our model.

In addition, as the value θ increases, another interesting observation is that the HL curves and the LL curves have the trend of getting closer in Fig. 1, while they have the trend of getting apart from each other in Fig. 2. Thus a natural question arises: is there a value θ_c between $\theta = 0.4$ and $\theta = 0.8$ at which the effect of two attacks is almost identical?

To address this problem, the relationship between the tolerance parameter β and the normalized avalanche size CF_{attack} is investigated when $\theta = 0.6$. From Fig. 3, it is easy to find that in the case of $\theta = 0.6$, the HL curve and the LL curve are very close to each other, and the β_c values originating from the two curves are almost the same. The β_c values of two attack strategies for $\theta = 0.6$ are also compared with ones for the other values of θ between $\theta = 0.4$ and $\theta = 0.8$. As shown in Table I, when $\theta = 0.6$, for the HL and the LL attacks $\beta_c \approx 0.09$, and $\theta = 0.6$ leads to their smallest difference of β_c. So for the scale-free network with $\gamma = 3$, it surely exists a threshold θ_c around 0.6, which corresponds to the theoretical estimate obtained. At this threshold, the effect on the network is almost the same for the HL and the LL attacks, in other words, the network preserves its robustness against the HL and the LL attacks.

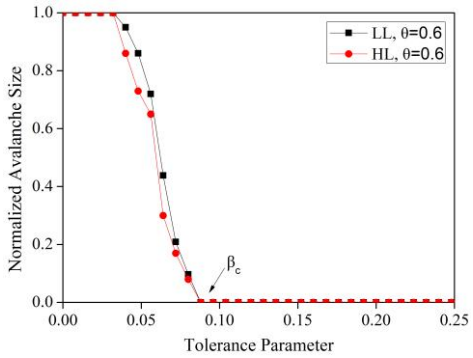


Fig. 3. Comparison between two attack strategies when $\theta = 0.6$.

TABLE I: THE TOLERANCE THRESHOLDS β_c OF TWO ATTACK STRATEGIES BETWEEN $\theta = 0.4$ AND $\theta = 0.8$

Attack strategies	$q = 0.4$	$q = 0.5$	$q = 0.6$	$q = 0.7$	$q = 0.8$
HL	0.032	0.068	0.091	0.104	0.111
LL	0.117	0.102	0.093	0.081	0.072

We also take the case of $\gamma > 3$ into account. The same thing that there exist the critical thresholds θ_c happens in scale-free networks with different values of γ. The relationship between the degree exponent γ and the critical threshold θ_c is portrayed in Fig. 4. Integrating with above simulation analysis, we can draw a conclusion that for the random scale-free network

whose degree exponent is adjusted, there is a threshold θ_c. When $\theta > \theta_c$, the HL strategy is more likely to lead to large-scale cascading failures than the LL strategy; while, on the contrary in the case of $\theta < \theta_c$. Meanwhile, our theoretical results are verified.

Moreover, from Fig. 4, it is obvious that the critical threshold θ_c is increasing with the increase of the degree exponent γ when $\gamma \le 4$, and θ_c presents ascendant trend after dropping first with the increase of g when $\gamma \ge 4$ and $\gamma \le 5$. Anyhow, θ_c ($\gamma > 3$) is greater than θ_c ($\gamma = 3$), which indicates that the degree exponent γ has an important influence on the value of θ_c. And the results shown in Fig. 4 give each class of networks with the different value γ a threshold θ_c, which can make little difference to attack the edges with the lower load or with the higher load.

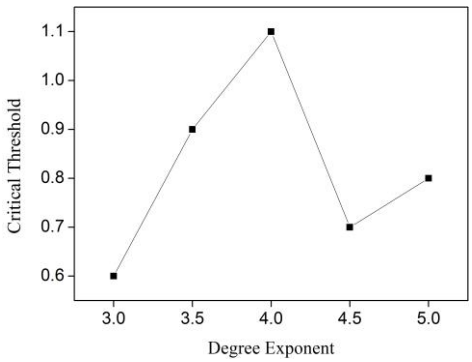


Fig. 4. The relation between the degree exponen γ and the critical threshold θ_c.

III. Conclusions

Cascading failures triggered by a small initial attack can do great harms to complex networks, especially to the infrastructure networks. Protecting the network against cascading failure under all kinds of attacks is particularly important. In this article, the factors affecting robustness of random scale-free networks against cascading failure under edge-based initial attacks are studied. A model of the random scale-free network for cascading failure is constructed based on a function of the betweenness and control parameter θ. According to the random scale-free network whose degree exponent is adjusted, the network robustness for cascading failure is investigated. The analytic results and the numerical simulations both show that: there exists a threshold θ_c. On the one hand, when $\theta > \theta_c$, attacking the edges with the highest load certainly works more efficient. On the other hand, when $\theta < \theta_c$, as unexpected, attacking the edges with the lowest load is more harmful. Moreover, the degree exponent of the network significantly affects the value of θ_c. Such interesting and enlightening phenomenon indicates that the load and degree distributions must be taken into account to determine the "critical" edges in order to protect them to prevent large-scale cascading failures. Our studies also provide a basis to design high robustness random scale-free network by the reasonably distributing loads among the network according to the node betweenness, which can effectively resist all kinds of edge attacks in future.

Acknowledgment

This work was supported by the National Natural Science Foundation of China under Grant No. 61403183, the Natural Science Foundation of Hunan Province of China under Grant No.2015JJ6096, the Philosophy Social Science Foundation of Hunan Province of China under Grant No.14YBA340 and the Education Department Foundation of Hunan Province of China under Grant No.14C1006.

References

[1] H. Dong and L. R. Cui, "System reliability under cascading failure models," *IEEE Trans. on Reliability*, vol. 65, no. 2, pp. 929-940, June 2016.

[2] V. Rampurkar, P. Pentayya, H. A. Mangalvedekar, and F. Kazi, "Cascading failure analysis for Indian power grid," *IEEE Trans. on Smart Grid*, vol. 7, no. 4, pp. 1951-1960, July 2016.

[3] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Phys. Rev. E*, vol. 66, pp. 065102, December 2002.

[4] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E*, vol. 69, pp. 045104, April 2004.

[5] X. L. Fang, Q. Yang, and W. J. Yan, "Modeling and analysis of cascading failure in directed complex networks," *Safe Science*, vol. 65, pp. 1-9, June 2014.

[6] W. X. Wang and G. R. Chen, "Universal robustness characteristic of weighted networks against cascading failure," *Phys. Rev. E*, vol. 77, pp. 026101, February 2008.

[7] B. Mirzasoleiman, M. Babaei, M. Jalili, and M Safari, "Cascaded failures in weighted networks," *Phys. Rev. E*, vol. 84, pp. 046114, October 2011.

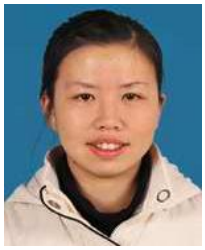
[8] Z. J. Bao, Y. J. Cao, L. J. Ding, and G. Z. Wang, "Comparion of cascading failures in small-world and scale-free networks subject to vertex and edge attacks," *Physica A*, vol. 388, pp. 4491-4498, July 2009.

[9] M. Babaei, H. Ghassemieh, and M. Jalili, "Cascading failure Tolerance of modular small-world networks," *IEEE Trans. on Circuits and Systems—II: Express Briefs*, vol. 58, no. 8, pp. 527-531, August 2011.

[10] X. Z. Peng, H. Yao, J. Du, Z. Wang, and C Ding, "Invulnerability of scale-free network against critical node failures based on a renewed cascading failure model, " *Physica A*, vol. 421, pp. 69-77, March 2015.

[11] B. Wu, A. Tang, and J. Wu, "Modeling cascading failures in interdependent infrastructures under terriorist attacks," *Reliablility Engineering and System Safety*, vol. 147, pp. 1-8, March 2016.

[12] J. Seo, S. Mishra, X. Li, and M. T. Thai, "Catastrophic cascading failures in power networks," *Theoretical Computer Science*, vol.607, pp. 306-319, November 2015.
[13] F. Molnár. Jr, N. Derzsy, B. K. Szymanski, and G. Korniss, "Building damage-resilient dominating sets in complex networks against random and targeted attacks," Scientific Reports, vol. 5, pp. 8321, February 2015.
[14] S. Mizutaka and K Yakubo, "Robustness of scale-free networks to cascading failures induced by fluctuating loads," *Phys. Rev. E*, vol. 92, pp. 012814, July 2015.
[15] M. Schafer, J. Scholz, and M. Greiner, "Proactive robustness control of heterogeneously loaded networks," *Phys. Rev. Lett*., vol. 96, pp. 108701, March 2006.
[16] R. Yang, W. X. Wang, Y. C. Lai, and G. R. Chen, "Optimal weighting scheme for suppressing cascades and traffic congestion in complex networks," *Phys. Rev. E*, vol. 79, pp. 026112, February 2009.
[17] J. W. Wang, "Abnormal cascading failure spreading on complex networks," *Chaos, Solitons and Fractals*, vol. 91, pp. 695-701, October 2016.
[18] A. Eslami and C. Huang, "Cascading failures in load-dependent finite-size random geometric networks," *IEEE Trans. on Network Science and Enginerring*, vol. 9, pp. 1-12, September 2016.
[19] A. Majdandzic, B. Podobnik, S. V. Buldyrev, D. Y. Kenett, S. Havlin, and H. E. Stanley, "Spontaneous recovery in dynamical networks," *Nature Physics*, vol. 10, pp. 34-38, October 2014.
[20] C. R. Liu and D. Q. Li, "A modeling framework for system restoration from cascading failures," *PLoS One*, vol. 9, no. 12, pp. e112363, September 2014.
[21] S. V. Buldyrev, R. Parshani, G. Paul, H. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, pp. 1025-1028, February 2010.
[22] S. D. S. Reis, Y. Q. Hu, A. Babino, J. S. Andrade Jr, S Canals, *et al*., "Avoiding catastrophic failure in correlated networks of networks," *Nature Physics*, vol. 14, pp. 762-767, September 2014.
[23] Q. Xuan, Y. Li, and T. J. Wu, "Growth model for complex networks with hierarchical and modular structures," *Phys. Rev. E*, vol. 73, pp. 036105, March 2006.
[24] K. I. Goh, B. Kahng, and D. Kim, "Universal behavior of load distribution in scale-free networks," *Phys. Rev. Lett*., vol. 87, pp. 278701, December 2001.
[25] K. I. Goh, B. Kahng, and D. Kim, "Packet transport and load distribution in scale-free network models," Physica A, vol. 318, pp. 72-75, February 2003.



Lin Ding was born in Hunan Province, China. He received the Ph.D. degree from Qingdao University, Qingdao, China, in 2013. She is currently an associate professor in University of South China and a visiting associate professor in University of British Columbia. Her major interests include complex networks and information security for the communication systems.

Minsheng Tan was born in Hunan Province, China. He received the B.S. degree from Wuhan University, Wuhan, China, in 1986. He is currently a professor in University of South China. His major interests include complex networks and information security for the communication systems.