Safety Science 53 (2013) 219–225

Contents lists available at SciVerse ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

Robustness of complex networks with the local protection strategy against cascading failures

Jianwei Wang *

School of Business Administration, Northeastern University, Shenyang 110819, PR China

ARTICLE INFO

Article history:
Received 22 May 2012
Received in revised form 21 September 2012
Accepted 21 September 2012
Available online 28 November 2012

Keywords:
Cascading failure
Complex network
BA network
Mitigation strategy
Power grid

ABSTRACT

Considering the role of the neighboring nodes of an overload node, we articulate a local protection strategy to address the problem of the optimal defense in the cascading propagation. From two aspects of the global robustness and the different attacks, we numerically demonstrate the effectiveness of this strategy on Barabási–Albert (BA) scale-free networks and the power grid, and show that the robustness of diverse networks against cascading failures can be improved dramatically. And we numerically find the optimal value of the parameter, at which two types of networks can reach the strongest robust level against cascading failures. Next, in BA networks we verify this finding by theoretical analysis. Our results may be very useful for constructing the optimal protection strategy in realistic networks and for leading to insights into the mitigation of cascading failures.

1. Introduction

Over the past decade, there has been a lot of research related with the robustness and stability of networks (Albert et al., 2000; Wu et al., 2011; Schneider et al., 2011; Zhang et al., 2012). In particular, great efforts have been dedicated to the research on cascading failures, which has been one of the most central topics in the network safety. In real life, cascading failures induced by targeted attacks and random failures can occur in many natural and man-made systems, and frequently trigger many catastrophic events, e.g., the largest blackout in US history took place on 14 August 2003 (Glanz and Perez-Pena, 2003), the Western North American blackouts in July and August 1996 (Sachtjen et al., 2000), Internet collapse (Pastor-Satorras et al., 2001) caused by congestion, and the large-scale bankruptcy (Wang et al., 2010) witnessed during the recent global economical recession.

In fact, in many infrastructure networks, there exists the load on nodes, and the load can be redistributed from one node to other nodes, which may lead to the imbalance of the load on the entire network, and further trigger the cascading propagation. Cascading failures are generally induced by random failures or intentional attacks on a few nodes and take frequently place on the single and non-interacting networks. Therefore, earlier studies on cascading failures pay close attention to analyzing the evolving characteristics of cascading failures and mainly focus on the cascading modeling (Wang and Chen, 2008; Wu et al., 2008; Chang and Wu, 2011; Wang and Rong, 2009; Wang et al., 2008), the cascade control and defense strategies (Motter, 2004; Schäfer et al., 2006; Simonsen et al., 2008), the attack strategies (Motter and Lai, 2002; Zhao et al., 2005; Wang and Rong, 2009, 2011), the cascading phenomena in the diverse networks (Bao et al., 2008; Gleeson, 2008; Zheng et al., 2007), and so on. Later, many researchers find that catastrophic events induced by cascading failures can also occur in coupled networks, for instance, electrical blackouts in Italy on 28 September 2003 result from a cascade of failures between the power grid and computer network. Motivated by that fact, Buldyrev et al. (2010) developed a framework for understanding the robustness of interacting networks against cascading failures and present exact analytical solutions for the critical fraction of nodes. After that, cascading failures on coupled networks have started to be studied actively and a number of important aspects of cascading failures in coupled networks (Vespignani, 2010; Parshani et al., 2010; Gao et al., 2012; Brummitt et al., 2012) have been discussed. In all cited studies above, most works on cascading failures from the single network to coupled networks have focused only on the modeling of cascading failure, the cascade control and defense strategies, or a fundamental property of coupled networks without considering the load. However, there are few works about investigating how by the extra protection strategies of the neighboring nodes of an overload node to enhance the robustness of complex networks against cascading failures. In fact, in many infrastructure networks, when a node overloads, its neighboring nodes can provide some protection resources to avoid its failure. Therefore we deserve a careful investigation.

* Tel.: +86 024 83672631.
E-mail address: jwwang@mail.neu.edu.cn

0925-7535/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ssci.2012.09.011

To this end, taking into account the protection strategy provided by the neighboring nodes of an overload node, we propose a new mitigation method. Without changing the total protection capacities of the whole network, we numerically investigate its effectiveness on improving the robustness of BA scale-free networks (Barabási and Albert, 1999) against cascading failures and find that the simple local protection method can dramatically optimize the resilience of BA networks. In addition, adopting the mitigation strategy, we numerically discuss how BA networks can reach the strongest robust level against cascading failures and find, compared with previous results, the optimal value of the parameter decreases. We verify this result by the theoretical analysis. In addition, we examine the effectiveness of the mitigation strategy on improving the robustness of the power grid against cascading failures and give the optimal protection strategy to avoid potential cascading failures.

The rest of this paper is organized as follows: in Section 2 we introduce the protection method. In Section 3 we numerically demonstrate the effectiveness of the mitigation strategy on improving the network robustness against cascading failures. In Section 4 the numerical simulations in BA networks are verified by theoretical analysis. Finally, some summaries and conclusions are shown in Section 5.

2. The mitigation strategy

In general, a simple network can be represented by an undirected and unweighted graph $G = (V,E)$, where V is the set of nodes (for instance the stations in a railway transportation system, the substations in the power grid, or the routers in the Internet), and E is the set of undirected and unweighted edges (the lines connecting couples of stations, transmission lines connecting two substations, or the cables connecting two routers).

Next, we introduce our protection method in detail. In previous studies, the rule that the overload nodes are immediately removed from the network is widely adopted. However, few works discuss this problem: when the load on a node exceeds its capacity, whether there exist some strategies to maintain its normal and efficient functioning to avoid the cascading propagation or not? In fact, in realistic networks, for example in traffic networks, when a traffic intersection saturates, traffic police can ease the traffic flows. Motivated by this case, Wang and Rong (2009) constructed a cascading model of an overload node with the breakdown probability. However, this mechanism with the breakdown probability increases the total price of the whole network. Therefore, without changing the total price of the whole network, how to protect the overload nodes has become one of the key issues in the control and the defense of cascading failures. To this end, considering that the neighboring nodes of an overload node may provide some protection resources to this overload node to maintain its normal and efficient functioning, we propose a local protection method (see Fig. 1). In Fig. 1, when the load on node i exceeds its capacity, we define the extra capacity $\Delta C_{i,\Gamma_i}$ received by node i from its neighboring nodes to

$$\Delta C_{i,\Gamma_i} = \sum_{m\in\Gamma_i} p(C_m - L_m) \tag{1}$$

where Γ_i, C_m, and L_m represent the set of the neighboring nodes of node i, the capacity of node m to handle the load, and the initial load of node m, respectively. The parameter p represents a random number in 0 and 1, which decides to the strength of the protection resources provided by the neighboring nodes. When $p = 0$, the neighboring nodes of the overload node cannot provide the extra capacity, i.e., without adopting the mitigation strategy. While when $p = 1$, the strongest protection is provided by the neighboring nodes.

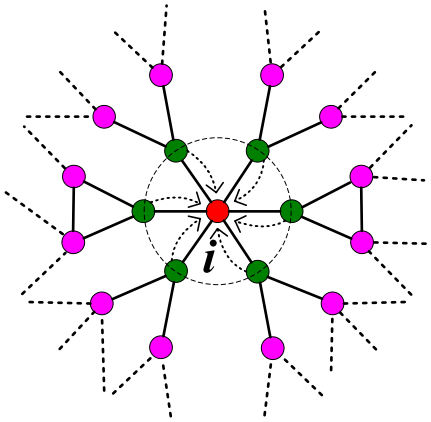

Fig. 1. The scheme illustrates that when the load on node i exceeds its capacity, its neighboring nodes can effectively protect it.

The expression $C_m - L_m$ ensures that node m can handle the initial load on it after providing some protection resources to node i. In this mitigation strategy, we can see that the total price of the whole network is not changed. For simplicity, we apply this strategy to a simple cascading model (Wang et al., 2008). In fact, our method can also be applied to other cascading models. Our purpose of this paper is to analyze to what extent this mitigation strategy can enhance the network robustness against cascading failures and what is the optimal strategy of the parameter selection after adopting this protection method. Next, we simply introduce the cascading model (Wang et al., 2008). The initial load L_i on node i in a network is defined as $L_i = k_i^{\alpha}$ with k_i being the degree of node i (i.e., the link number that node i connects other nodes), where α is a tunable parameter. The capacity C_i of node i is defined as $C_i = (1+\beta)L_i$, where the constant β is an adjustable parameter characterizing the tolerance of the network against cascading failures. After node i fails, the additional load ΔL_j received by node j, one of its neighboring nodes, is proportional to its initial load L_j, i.e., $\Delta L_j = L_i L_j / (\sum_{m\in\Gamma_i} L_m)$, where Γ_i represents the set of the neighboring nodes of node i. According to the protection strategy, at t time, when the load on node i exceeds its capacity, the capacity $C_{i,t}$ of node i can dynamically be adjusted to

$$C_{i,t} = C_{i,t-1} + \sum_{m\in\Gamma_i} p(C_{m,t-1} - L_m) \tag{2}$$

and the capacities of the neighboring nodes of node i can simultaneously be adjusted to

$$C_{m\in\Gamma_i,t} = C_{m\in\Gamma_i,t-1} - p(C_{m\in\Gamma_i,t-1} - L_{m\in\Gamma_i}) \tag{3}$$

Our aim is to investigate the effect of the capacity adjustment on the network robustness. Here we only focus on the cascading propagation induced by removing a single node. A failed node can lead to the load redistribution, and then cascading failures may occur. This process will be repeated until the load of all nodes is less than their capacities, and at this moment, cascading failures can be considered to be completed. We quantify the effectiveness of the mitigation strategy on improving the network robustness against cascading failures by two measures: the avalanche size S and the proportion $P(S)$. The avalanche size S is defined as: $S = \sum_{i\in N} s_i / n$, where N and n represent the set and the number of all nodes in the network, respectively, and s_i represents the number of the breakdown nodes induced by removing node i. The measure $P(S)$ represents the proportion between the number of the protected nodes after adopting the mitigation method and the number of the broken nodes induced before adopting the mitigation strategy.

3. Simulation analysis of the mitigation strategy

Taking into account the role of the network structure in the cascading propagation and the ubiquity of scale-free networks in natural and human-made systems, we firstly investigate the effectiveness of the mitigation strategy on improving the robustness of the scale-free networks against cascading failures. The degree distribution of the scale-free networks satisfies a power law form: $P(k) \sim k^{-\gamma}$, where k is the number of links of a randomly chosen node in the network and γ is the scaling exponent. For simplicity, the scale-free network is generated by using the standard Barabási–Albert model (Barabási and Albert, 1999). Starting from m_0 fully connected nodes, a new node with $m(m \leqslant m_0)$ edges is added to the existing network at each time step according to the preferential attachment. In computer simulations, for all networks, the network size N is equal to 5000, and the parameters m_0 and m are equal to 2. Therefore, the average degree $\langle k \rangle$ is approximately equal to 4.

In Fig. 2, we compare the average avalanche size S after and before adopting the protection strategy in four cases of $\alpha = 0.4$, $\alpha = 0.7$, $\alpha = 1.0$, and $\alpha = 1.3$. Numerical results are obtained by averaging over 50 experiments on 10 independent networks. The mitigation areas marked show that the robustness of BA networks against cascading failures can be improved dramatically. By computer simulations, we observe that the parameter p plays an important role in the effective control of cascading failures, i.e., the bigger the value p, the stronger the robustness of BA networks. Therefore, by reasonably increasing the value p, we can more effectively protect BA networks against cascading failures. In addition, we also find that the average avalanche size S after and before adopting the protection strategy shows the threshold-like behaviors marked by the critical threshold β_c. The critical threshold β_c is widely applied to many cascading models (Wang and Chen, 2008; Wu et al., 2008; Wang and Rong, 2009; Wang et al., 2008; Parshani et al., 2010; Gao et al., 2012) and can quantify the network robustness against cascading failures, that is, the smaller the value of β_c, the stronger the network robustness, and the lower the price of the whole network. Therefore, to maximize the robustness and minimize the cost, according to the role of the value β_c, the aim of many studies is to find the optimal value of the parameters in the cascading model, at which the value β_c is smallest. In the left sub-figure in Fig. 3, according the estimated β_c obtained by the minimal value when $S < 0.002$, in two cases of $p = 0.5$ and $p = 0.9$, we can observe that BA networks can obtain the strongest robust level against cascading failures when $\alpha \approx 0.8$, which is different from the optimal value $(\alpha = 1)$ without adopting the protection method (Wang et al., 2008) (While in the case of $p = 0.1$, the optimal value $\alpha \approx 1$). We will verify the results by the latter theoretical analysis. In addition, in the right-figure in Fig. 3, we can observe that, as the value α increases, according to the proportion $P(S)$, the improvement of the robustness of BA networks is bigger and bigger. And when $\beta \geqslant 0.1(\alpha = 0.4)$, $\beta \geqslant 0.088(\alpha = 0.7)$, $\beta \geqslant 0.08(\alpha = 1.0)$, and $\beta \geqslant 0.076(\alpha = 1.3)$, $P(S) > 0.99$.

Next, we focus on the role of the mitigation strategy on improving the network robustness when the diverse types of nodes are attacked. We simply apply two attacks, i.e., attacking the nodes with the highest load (HL) and attacking the ones with the lowest load (LL). In the HL, we attack the nodes in the descending order of their load (if some nodes happen to have the same highest load, we randomly choose one of them). While in the LL, we attack the nodes in the descending order of their load (if some nodes happen to have the same highest load, we randomly choose one of them). By the normalized average avalanche size S_{attack}, we quantify the network robustness after and before adopting the mitigation strategy, of which $S_{attack} = \sum_{i \in A} s_i / n_A(n-1)$, where A, n_A, and n represent the set and the number of nodes attacked and the number of all nodes in a network, respectively. In computer simulations, for both the HL and the LL, we choose 50 nodes as the attacked objects and numerical results are obtained by averaging over 50 experiments on 10 independent networks. In Fig. 4, for the HL and the LL, we observe that the mitigation strategy can dramatically enhance the network robustness against cascading failures and also find that, the bigger the value p, the stronger the network robustness. In Fig. 5, by the proportion $P(S)$, surprisingly, we find that the effectiveness orders of the mitigation method in two attacks are different, i.e., as the value α increases, in the LL the protection method is more and more effective, while in the HL, the case is the opposite. In fact, this phenomenon is mainly originated from the effect of the value α on the node capacity. Because the bigger the value α, the stronger the increased capacity of the nodes with the higher degree than the ones with the lower degree, for the LL, the neighboring nodes (the degrees of these nodes are generally bigger than the node attacked) of the node with the smallest degree attacked can provide the more protection resources, which lead to the results observed in the right sub-figure in Fig. 5. While for the HL, the case is on the contrary.

Next, taking into account the important role of the infrastructure networks, we apply the protection method to the power grid of the western United States (Watts and Strogatz, 1998) with 4941 nodes and 6594 edges. From two aspects of the global removal and two attacks, we investigate the effectiveness of the mitigation strategy on enhancing the robustness of the power grid against cascading failures. In Fig. 6, we also observe that the robustness level of the power grid against cascading failures can obtain the significant improvement and that and the effect of the value p on the cascading propagation. In the left sub-figure in Fig. 7, after adopting the mitigation strategy, we examine the correlation between the proportion $P(S)$ and the parameter β when

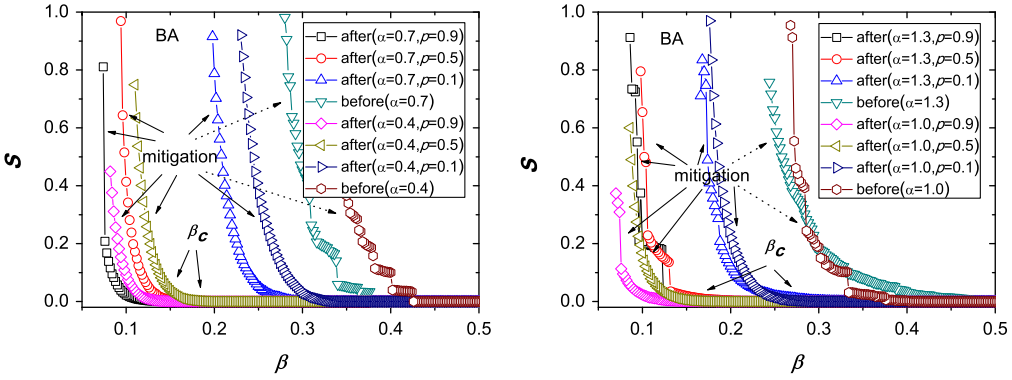

Fig. 2. Demonstration of the effectiveness of the mitigation strategy on enhancing the robust level of BA networks against cascading failures.

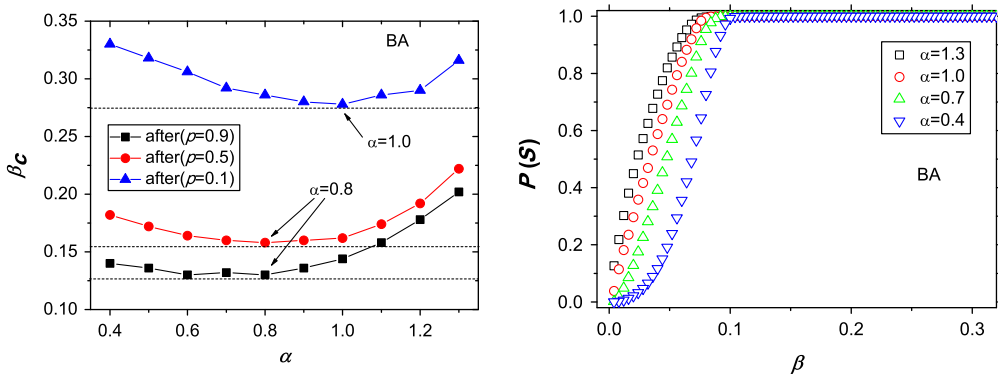

Fig. 3. Correlation between the critical threshold β_c and the parameter α and the proportion $P(S)$ as a function of the parameter β after adopting the mitigation strategy in BA networks.

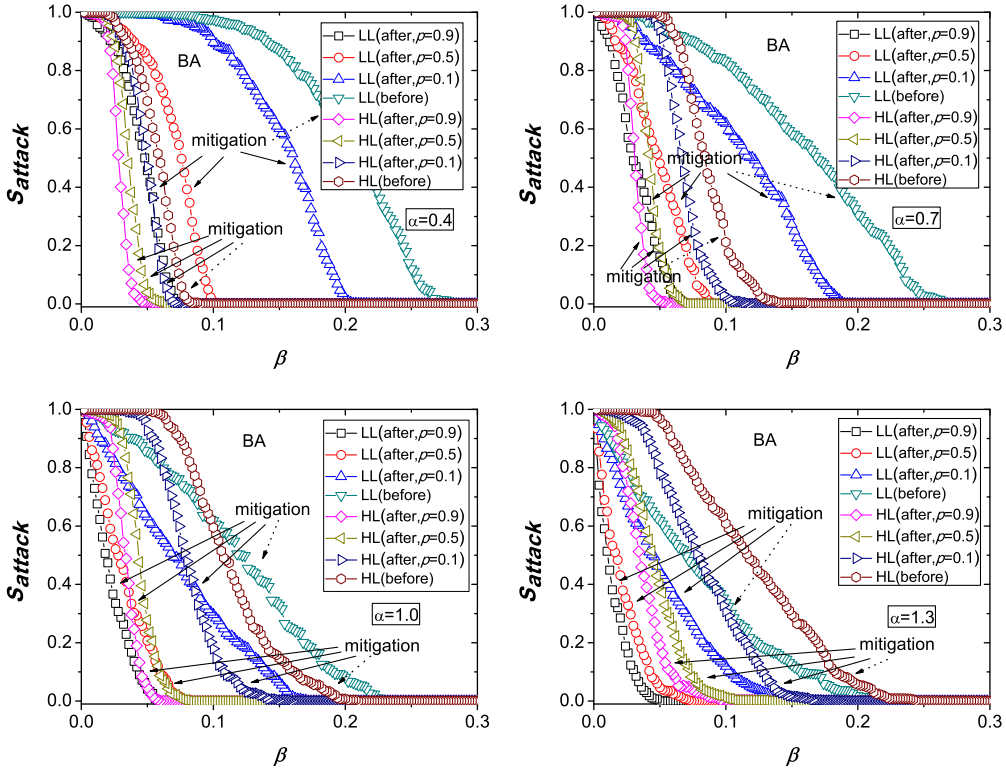

Fig. 4. Demonstration of the effect of the mitigation strategy subject to two targeted attacks on BA networks in four cases of $\alpha = 0.4$, $\alpha = 0.7$, $\alpha = 1.0$, and $\alpha = 1.3$.

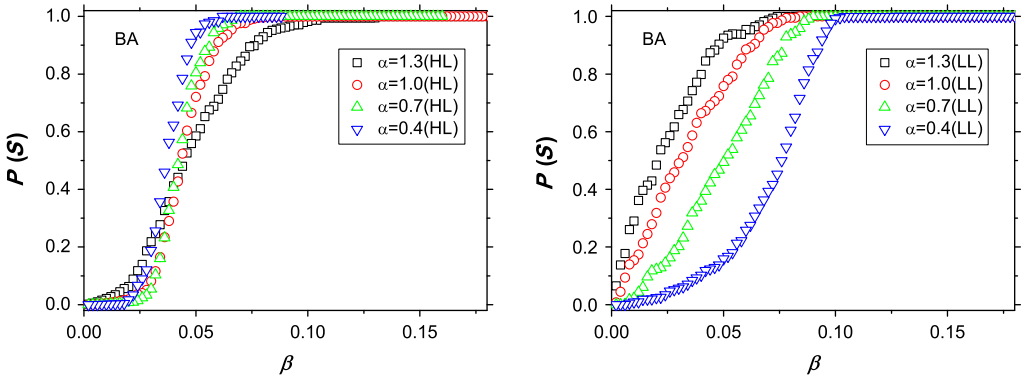

Fig. 5. Demonstration of the effect of the parameter α on the proportion $P(S)$ in the HL and the LL on BA networks.

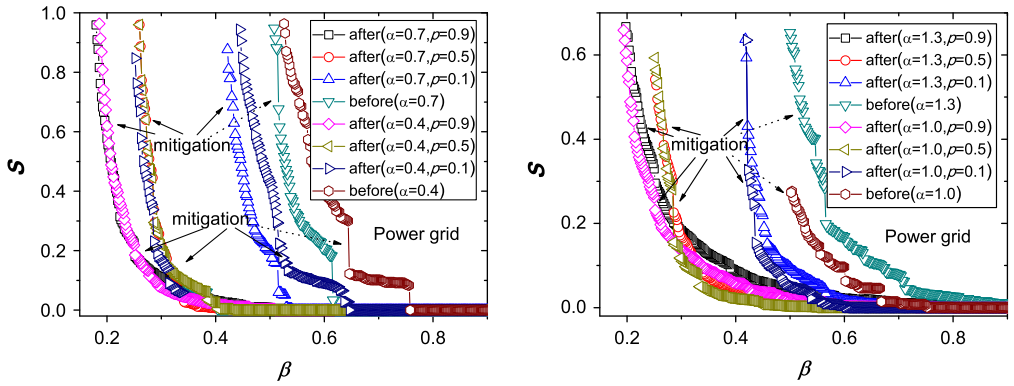

Fig. 6. Demonstration of the effect of the mitigation strategy on improving the robustness of the power grid against cascading in four cases of $\alpha = 0.4$, $\alpha = 0.7$, $\alpha = 1.0$, and $\alpha = 1.3$.

$\alpha = 0.4$, $\alpha = 0.7$, $\alpha = 1.0$, and $\alpha = 1.3$ and find that as the value α increases, the protection method is more and more effective. And when $\beta \geqslant 0.196$ ($\alpha = 0.4$), $\beta \geqslant 0.196$ ($\alpha = 0.7$), $\beta \geqslant 0.188$ ($\alpha = 1.0$), and $\beta \geqslant 0.18$ ($\alpha = 1.3$), $P(S) > 0.99$. In the right sub-figure in Fig. 7, according the estimated β_c obtained by the minimal value when $S < 0.002$, after adopting the mitigation strategy, we compare the value β_c in the different value α and find that when $\alpha = 0.4$ and $\alpha = 0.7$ the power grid can obtain the stronger robust level against cascading failures. In Figs. 8 and 9, for the HL and the LL, we investigate the effect of the mitigation strategy on improving the robustness of the power grid against cascading failures and find the similar results with ones in BA networks.

4. Theoretical analysis of cascading model

After adopting the mitigation strategy, we analyze the correlation between the parameter α and the critical threshold β_c in BA networks. Our aim is to seek for the the minimal value β_c. Therefore, after node i, we assume the load on its neighboring node j fails to exceed its capacity, thus the extra capacity $\Delta C_{j,\Gamma_j}$ received by node j can further protect node j. According to the capacity C_j and the extra $\Delta C_{j,\Gamma_j}$ of node j, to avoid the cascading propagation induced by the load redistribution on node i, the neighboring node j of node i should satisfy

$$L_j + \Delta L_j < C_j + \Delta C_{j,\Gamma_j} \tag{4}$$

Here,

$$\Delta C_{j,\Gamma_j} = \sum_{n\in\Gamma_j} p(C_n - L_n) = \sum_{n\in\Gamma_j} p((1+\beta)k_n^\alpha - k_n^\alpha) = p\beta\sum_{n\in\Gamma_j} k_n^\alpha \tag{5}$$

So, the above inequality (4) is represented as

$$k_j^\alpha + k_i^\alpha \frac{k_j^\alpha}{\sum_{m\in\Gamma_i} k_m^\alpha} < (1+\beta)k_j^\alpha + p\beta\sum_{n\in\Gamma_j} k_n^\alpha \tag{6}$$

Next, by the probability theory and the network structure, we focus on the mathematical expectations of the expressions $\sum_{m\in\Gamma_i} k_m^\alpha$ and $\sum_{n\in\Gamma_j} k_n^\alpha$. Taking into account the characteristic of the no degree–degree correlation in BA networks, we have

$$E\left(\sum_{m\in\Gamma_i} k_m^\alpha\right) = \sum_{k'=k_{min}}^{k_{max}} k_i P(k'|k_i) k'^\alpha = \sum_{k'=k_{min}}^{k_{max}} k_i \frac{k' P(k') k'^\alpha}{\langle k\rangle} = \frac{k_i \langle k^{\alpha+1}\rangle}{\langle k\rangle} \tag{7}$$

where $P(k'|k_i)$ (In BA network, $P(k'|k_i) = k'P(k')/\langle k\rangle$) is the conditional probability that node i with the degree k_i has a neighbor node with the degree k'. Similarly, we have

$$E(\sum_{n\in\Gamma_j} k_n^\alpha) = \sum_{k'=k_{min}}^{k_{max}} k_j P(k'|k_i) k'^\alpha = \sum_{k'=k_{min}}^{k_{max}} k_j \frac{k' P(k') k'^\alpha}{\langle k\rangle} = \frac{k_j \langle k^{\alpha+1}\rangle}{\langle k\rangle} \tag{8}$$

So, the above inequality (6) is simplified to

$$\frac{k_i^{\alpha-1}\langle k\rangle}{\langle k^{\alpha+1}\rangle} \frac{k_j^{\alpha-1}\langle k\rangle}{k_j^{\alpha-1}\langle k\rangle + p\langle k^{\alpha+1}\rangle} < \beta \tag{9}$$

Analyzing the above inequality (9), we can obtain the critical threshold β_c in three ranges of $\alpha < 1$, $\alpha = 1$, and $\alpha > 1$.

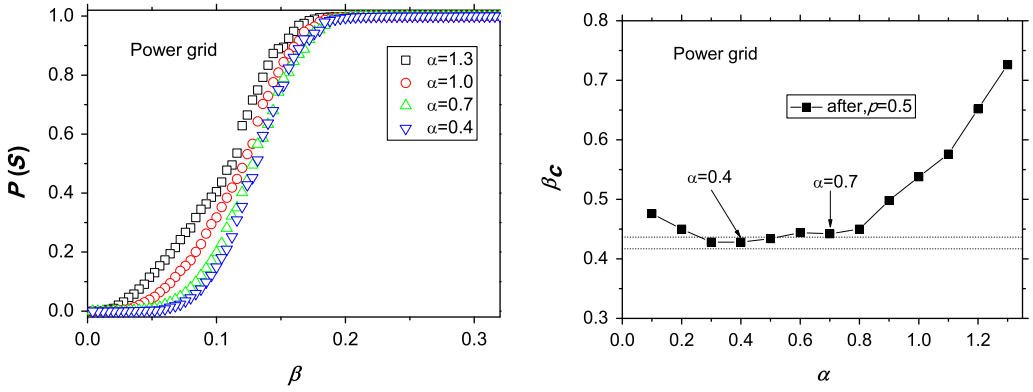

Fig. 7. Illustration of the effectiveness of the mitigation strategy on enhancing the robustness of the power grid against cascading failures and correlation between the critical threshold β_c and the parameter α.

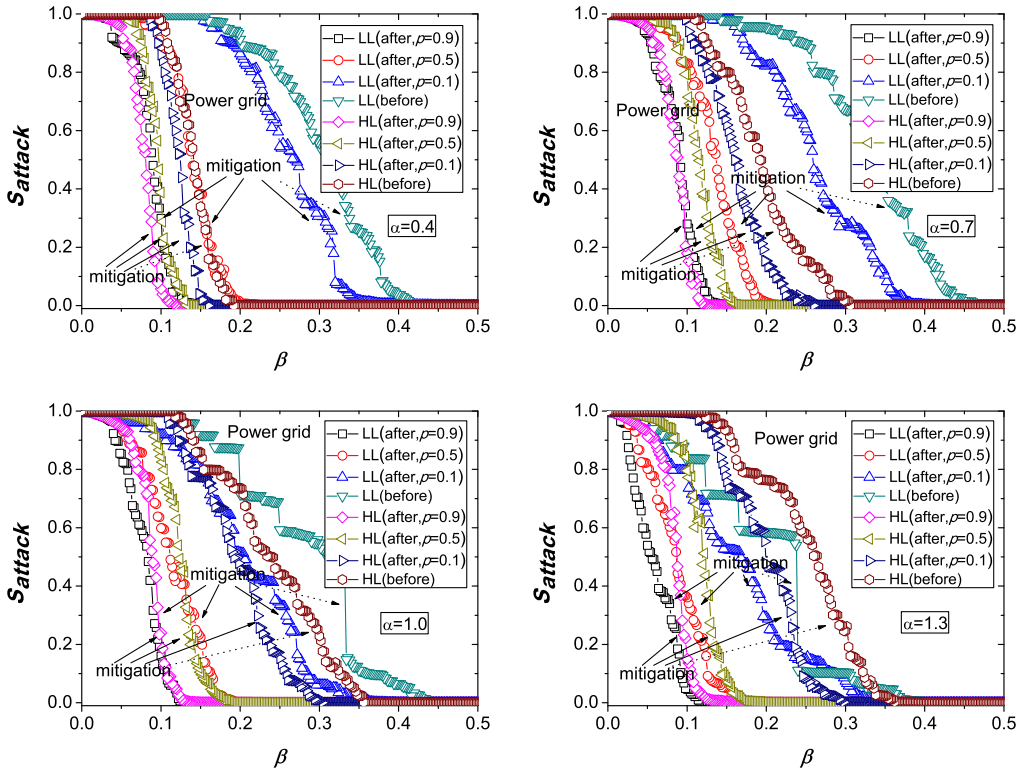

Fig. 8. Demonstration of the effect of the mitigation strategy subject to two attacks on enhancing the robustness of the power against cascading failures in four cases of $\alpha = 0.4$, $\alpha = 0.7$, $\alpha = 1.0$, and $\alpha = 1.3$.

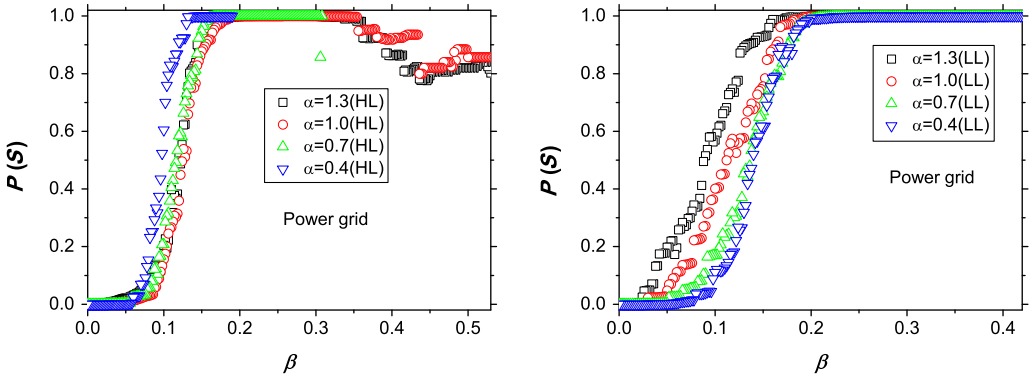

Fig. 9. Demonstration of the effect of the parameter α on the proportion $P(S)$ in the HL and the LL on the power grid.

$$\beta_c = \begin{cases} \frac{k_{max}^{\alpha-1}\langle k\rangle}{\langle k^{\alpha+1}\rangle} \frac{k_{max}^{\alpha-1}\langle k\rangle}{k_{max}^{\alpha-1}\langle k\rangle + p\langle k^{\alpha+1}\rangle} & \alpha > 1 \\ \frac{\langle k\rangle}{\langle k^2\rangle} \frac{\langle k\rangle}{\langle k\rangle + p\langle k^2\rangle} & \alpha = 1 \\ \frac{k_{min}^{\alpha-1}\langle k\rangle}{\langle k^{\alpha+1}\rangle} \frac{k_{min}^{\alpha-1}\langle k\rangle}{k_{min}^{\alpha-1}\langle k\rangle + p\langle k^{\alpha+1}\rangle} & \alpha < 1 \end{cases} \quad (10)$$

Here, k_{max} and k_{min} represent the minimum and maximum degree of nodes in a network, respectively. When the value p is equal to 0, the equation has been verified by Wang et al. (2008). Next, for $p \neq 0$, we first compare the value β_c in two cases of $\alpha > 1$ and $\alpha = 1$. When $\alpha > 1$, we have

$$\frac{k_{max}^{\alpha-1}\langle k\rangle}{k_{max}^{\alpha-1}\langle k\rangle + p\langle k^{\alpha+1}\rangle} = \frac{\langle k\rangle}{\langle k\rangle + \frac{p\langle k^{\alpha+1}\rangle}{k_{max}^{\alpha-1}}} \quad (11)$$

$$\frac{p\langle k^{\alpha+1}\rangle}{k_{max}^{\alpha-1}} = p\frac{1}{N}\sum_{i=1}^{N} k_i^2 \left(\frac{k_i}{k_{max}}\right)^{\alpha-1} < p\langle k^2\rangle \quad (12)$$

Therefore, according the Eq. (10) and the inequality (12) and the correctness of the Eq. (12) when $p = 0$, we can get $\beta_c(\alpha > 1) > \beta_c(\alpha = 1)$. Similarly, in the case of $\alpha < 1$, we can also obtain $\beta_c(\alpha < 1) > \beta_c(\alpha = 1)$.

However, in Fig. 3, we observe that the optimal value α is about 0.8. The smaller deviation between computer simulations and theoretical analysis mainly derives from the above approximation in the analytical predictions, i.e., two nodes i and j connected by other other simultaneously have the minimum degree. In fact, in BA networks generated by the BA model, according to the evolving mechanism of the BA model, two nodes with the lowest degree can be not connected by each other. For example, for a BA network with 5000 nodes and 9997 edges, there is not a connection between two nodes with the minimum degree, which may lead to the difference in comparison.

By the Eq. (10), we further analyze the effect of the mitigation strategy on the critical threshold β_c. We compare the value β_c in

two cases of $p = 0$ and $p \neq 0$, correspond to not adopting and adopting the mitigation, respectively. We calculate the value $\beta_{c,p\neq0}/\beta_{c,p=0}$, i.e.,

$$\beta_{c,p\neq0}/\beta_{c,p=0} = \begin{cases} \frac{k_{max}^{\alpha-1}\langle k\rangle}{k_{max}^{\alpha-1}\langle k\rangle + p\langle k^{\alpha+1}\rangle} & \alpha > 1 \\ \frac{\langle k\rangle}{\langle k\rangle + p\langle k^2\rangle} & \alpha = 1 \\ \frac{k_{min}^{\alpha-1}\langle k\rangle}{k_{min}^{\alpha-1}\langle k\rangle + p\langle k^{\alpha+1}\rangle} & \alpha < 1 \end{cases} \tag{13}$$

For simplicity, we only calculate the value $\beta_{c,p\neq0}/\beta_{c,p=0}$ in the case of $\alpha = 1$. We first calculate the value $\langle k^2\rangle$. For a BA network with the finite size, its degree distribution is $P(k) = 2m^2k^{-3}$, where m is equal to k_{min} (here $k_{min} = \frac{1}{2}\langle k\rangle$). Thus, $\langle k^2\rangle$ in a BA network can be calculated by

$$\begin{aligned}\langle k^2\rangle &= \int_{k_{min}}^{k_{max}} P(k)k^2dk = \int_{k_{min}}^{k_{max}} 2k_{min}^2k^{-1}dk \\ &= 2k_{min}^2(lnk_{max} - lnk_{min})\end{aligned} \tag{14}$$

In BA networks, k_{max} can be calculated by $\int_{k_{max}}^{\infty} P(k)dk = 1/N$, i.e.,

$$\int_{k_{max}}^{\infty} 2m^2k^{-3}dk = 1/N \Rightarrow k_{max} = \sqrt{N}k_{min} \tag{15}$$

So, we have

$$\langle k^2\rangle = k_{min}^2 lnN = \frac{\langle k\rangle^2 lnN}{4} \tag{16}$$

Therefore, when $\alpha = 1$, we can get

$$\beta_{c,p\neq0}/\beta_{c,p=0} = \frac{4}{4 + p\langle k\rangle lnN} \tag{17}$$

In computer simulations, the parameter p, the average degree $\langle k\rangle$, and the network size N is 0.5, 4, and 5000, respectively. So, only in the case of $p = 0.5$, we can obtain $\beta_{c,p=0.5}/\beta_{c,p=0} \approx 0.05545$, which shows that the network robustness can dramatically be improved. In addition, we also find that the bigger the value p, the smaller the value β_c, the stronger the network robustness.

5. Conclusion

In summary, by the local dynamical adjustment of the capacity of an overload node, without changing the total price of the whole network, we propose a method to effectively protect the overload node to avoid its breakdown. Applying a simple cascading model, we numerically investigate the effectiveness of the mitigation strategy on improving the robustness against cascading failures in BA scale-free networks and the power grid. According to the average avalanche size and the proportion between the protected nodes by the mitigation strategy and the failed nodes before adopting the mitigation strategy, we find that the mitigation strategy can effectively enhance the network robustness and obtain the correlation between the network robustness and some parameters. In addition, after applying the mitigation strategy, we obtain the optimal value α, at which both BA networks and the power grid can reach the strongest robust level against cascading failures. We also verify the result in BA networks by the latter theoretical analysis. Considering that the mitigation strategy can be easily applied to many real-life networks, these results may be very useful for guiding the improvement robustness of infrastructure networks and avoiding various cascading-failure-induced disasters in the real world.

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grant Nos. 71101022 and 70801011 and the Fundamental Research Funds for the Central Universities under Grant No. N110406003.

References

Albert, R., Jeong, H., Barabási, A.-L., 2000. Attack and error tolerance in complex networks. Nature 406, 378–382.
Bao, Z.J., Cao, Y.J., Ding, L.J., Han, Z.X., Wang, G.Z., 2008. Dynamics of load entropy during cascading failure propagation in scale-free networks. Phys. Lett. A 372 (36), 5778–5782.
Barabási, A.-L., Albert, R., 1999. Emergence of Scaling in Random Networks. Science 286, 509–512.
Brummitt, C.D., D'souza, R.M., Leicht, E.A., 2012. Suppressing cascades of load in interdependent networks. Proc. Natl. Acad. Sci. USA. http://dx.doi.org/10.1073/pnas.1110586109.
Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S., 2010. Catastrophic cascade of failures in interdependent networks. Nature 464, 1025–1028.
Chang, L., Wu, Z.G., 2011. Performance and reliability of electrical power grids under cascading failures. Int. J. Elec. Power 33 (8), 1410–1419.
Gao, J., Buldyrev, S.V., Stanley, H.E., Havlin, S., 2012. Networks formed from interdependent networks. Nature Phys. 8, 40–48.
Glanz, J., Perez-Pena, R., 2003. 90 s That Left Tens of Millions of People in the Dark, vol. 26, New York Times, 2003.
Gleeson, J.P., 2008. Cascades on correlated and modular random networks. Phys. Rev. E 77 (4), 046117.
Motter, A.E., 2004. Cascade control and defense in complex networks. Phys. Rev. Lett. 93 (9), 098701.
Motter, A.E., Lai, Y.C., 2002. Cascade-based attacks on complex networks. Phys. Rev. E 66 (6), 065102, R.
Parshani, R., Buldyrev, S.V., Havlin, S., 2010. Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition. Phys. Rev. Lett. 105 (4), 048701.
Pastor-Satorras, R., Vázquez, A., Vespignani, A., 2001. Dynamical and correlation properties of the Internet. Phys. Rev. Lett. 87, 258701.
Sachtjen, M.L., Carreras, B.A., Lynch, V.E., 2000. Disturbances in a power transmission system. Phys. Rev. E 61 (5), 4877–4882.
Schäfer, M., Scholz, J., Greiner, M., 2006. Proactive robustness control of heterogeneously loaded networks. Phys. Rev. Lett. 96 (10), 108701.
Schneider, C.M., Moreira, A.A., Andrade Jr., J.S., Havlin, S., Herrmann, H.J., 2011. Mitigation of malicious attacks on networks. Proc. Natl. Acad. Sci. USA. http://dx.doi.org/10.1073/pnas.1009440108.
Simonsen, I., Buzna, L., Peters, K., Bornholdt, S., Helbing, D., 2008. Transient dynamics increasing network vulnerability to cascading failures. Phys. Rev. Lett. 100 (21), 218701.
Watts, D.J., Strogatz, S.H., 1998. The raw data used in "Collective dynamics of 'small-world' networks": describing the US power grid. Nature 393 (6684), 440.
Vespignani, A., 2010. The fragility of interdependency. Nature 464, 984–985.
Wang, W.X., Chen, G.R., 2008. Universal robustness characteristic of weighted networks against cascading failure. Phys. Rev. E 77, 026101.
Wang, J.W., Rong, L.L., 2009. A model for cascading failures in scale-free networks with a breakdown probability. Physica A 388 (7), 1289–1298.
Wang, J.W., Rong, L.L., 2009. Cascade-based attack vulnerability on the US power grid. Safety Sci. 47 (10), 1332–1336.
Wang, J.W., Rong, L.L., 2011. Robustness of the western United States power grid under edge attack strategies due to cascading failures. Safety Sci. 49 (6), 807–812.
Wang, J.W., Rong, L.L., Zhang, L., Zhang, Z.Z., 2008. Attack vulnerability of scale-free networks due to cascading failures. Physica A 387 (26), 6671–6678.
Wang, W.X., Yang, R., Lai, Y.C., 2010. Cascade of elimination and emergence of pure cooperation in coevolutionary games on networks. Phys. Rev. E 81, 035102, R.
Wu, Z.X., Peng, G., Wang, W.X., Chan, S., Wong, E.E.M., 2008. Cascading failure spreading on weighted heterogeneous networks. J. Stat. Mech. P05013.
Wu, J., Barahona, M., Tan, Y.J., Deng, H.Z., 2011. Spectral measure of structural robustness in complex networks. IEEE Trans. Syst., Man, Cybern. A, Syst., Humans 41 (6), 1244–1252.
Zhang, J.H., Xu, X.M., Hong, L., Wang, S.L., Fei, Q., 2012. Attack vulneralility of self-organizing networks. Safety Sci. 50, 443–447.
Zhao, L., Park, K., Lai, Y.C., Ye, N., 2005. Tolerance of scale-free networks against attack-induced cascades. Phys. Rev. E 72 (2), 025104.
Zheng, J.F., Gao, Z.Y., Zhao, X.M., 2007. Clustering and congestion effects on cascading failures of scale-free networks. Europhys. Lett. 79 (5), 58002.