J Stat Phys (2010) 141: 555–565
DOI 10.1007/s10955-010-0058-x

Cascade Defense via Control of the Fluxes in Complex Networks

Ke Hu · Tao Hu · Yi Tang

Received: 6 March 2010 / Accepted: 1 September 2010 / Published online: 16 September 2010

Abstract Exploring the possible strategies to defense to prevent the cascade from propagating through the entire network is of both theoretical interest and practical significance, and several strategies of defense have been developed recently. Following the work about the strategy based on the international removal of network elements (Motter in Phys. Rev. Lett. 93:098701, 2004), we propose and investigate three novel strategies of defense by controlling the fluxes. Extensive simulations on both an artificially created scale-free network and the Internet at autonomous system level reveal that these strategies can suppress the propagation of the cascade, even avoid the cascading failure. In addition, a more intuitive and important measure to quantify the damage caused by a cascade is developed and some new features are, thus, clearly displayed.

Keywords Cascading failure · Strategy of defense · Complex network

1 Introduction

The study of the cascade dynamics in complex network [1–4] has largely benefited from the need of understanding and controlling such incidents as blackouts of electrical power [5] and Internet congestion [6, 7], which has recently become a subject of intensive investigations [8]. A number of important aspects of cascading failures in complex networks have been discussed, including disturbances in power transmission systems [5, 9], the origin of rare events [10], the analytical calculation of capacity parameter [11, 12], the modelling of the real-world data [13, 14], the theoretical model for describing cascade phenomena [3, 14–19], the effect of network growth [1, 2], the avalanche size distributions [4, 20], the congestion instabilities [21–23], and the congestion effects on the cascading failures [24–26]. In particular, a simple model of cascades of overload failures has been introduced [3], where the flows of, for example, electrical power or communication packets are characteristic for critical-infrastructure networks. The failure of components leads to a redistribution of flow. After redistribution, some of the remaining nodes and links are loaded with a

K. Hu · T. Hu · Y. Tang (✉)
Institute of Modern Physics, Xiangtan University, Xiangtan 411105, Hunan, P.R. China
e-mail: tangyii@yahoo.cn

larger flow than before. If this new load exceeds their capacity, the respective components will also fail, giving rise to more flow redistribution and possibly more failure. For heterogeneous networks, like scale-free networks, such overload avalanches might already be triggered by the failure of only one of the most-loaded nodes or links [3].

In view of the frangibility of complex networks to the cascade failure, it becomes a major task to find optimal strategy of defense, oriented to minimize the risk of cascading failures on heterogeneous loaded networks, task with immediate practical and economical implications. Generally, once a cascade occurs, the time scale needed to react may be relatively short and may not be operationally feasible for some special situations, thus most of these strategies [11, 12, 27, 28], including the optimal capacity layout [15, 16, 29, 30] and the optimal weighting scheme [31], have been designed as proactive robustness control ones. Recently, a simple reactive defense control has been proposed by Motter, where a cascade is divided in two parts [32]: (I) the initial attack, where a fraction of nodes is removed; and (II) the propagation of the cascade, where another fraction of nodes is removed due to the subsequent overload failures. He suggest that in some real networks, (I) and (II) are separated in time but this time interval is usually shorter than the time scale in which the network evolves. Thus, it is reasonable to consider that no links or nodes can be rewired or added to the system after the initial attack because any of these operations would involve extra costs. In this perspective, one can concluded that, after the initial attack, the only operations allowed in order to avoid or reduce the failure are the removal of fluxes, nodes or links. Thus far, however, studies of cascade defenses in complex networks have been focused on the removal of the network elements (i.e., nodes or links) [32] or the optimization of capacity layout [15, 16, 29, 30]. In fact, the control of fluxes may be considered in the literature. For example, in the case of power-grid networks, Anghel et al. [33] analyze the effect of operator actions with different risk optimizations of load shedding versus cascading. Additionally, in many realistic circumstances when a heavily loaded node or link is lost for some reason, an adaptive adjustment or removal of source fluxes on individual nodes can occur automatically [34], in attempt to prevent further overload failures for other nodes or links. Motivated by these considerations, we propose three costless strategies of defense based on the adjustment or control of the fluxes, and argue that the size of the cascade can be more effectively reduced by the adjustment or control of the fluxes not necessarily connected to the IR of network elements.

2 The Model

For concreteness, we consider the model of overload failures introduced by Motter and Lai [3], which is defined as follows. For a given network $W(V, E)$ described by the sets of nodes V and links E, we assume that at every time step one flux $s_{ij}(t)$ is sent from node i to node j along the shortest-hop path $[i \to j]$, for every ordered pair of nodes (i, j) belonging to the same connected component of W. If there is more than one shortest path connecting two given nodes, the flux is divided evenly among each path. The load L_v on a node v is the total fluxes passing node per unit of time, which is written as

$$L_v(t) = \sum_{i,j \in V} r_{sp}([i \to j]; v) s_{ij}(t). \tag{1}$$

The value of the path function $r_{sp}([i \to j]; v)$ is either 1 or 0, depending on whether the node v is part of the shortest-hop path from node i to node j or not.[1] The element of the flux matrix s_{ij} is assumed to be uniform and constant in Motter and Lai model [3], or temporal fluctuations in the recent proposed flux fluctuation model [14, 16]. Each node v is then assigned to have a finite capacity C_v. The node operates in free-flux regime if $L_v(t) \leq C_v$; otherwise the node is assumed to fail and is removed from the network. Initially, the network is assumed to be a connected one, and the load of each node is given by (1). The capacity C_v of node v is assumed to be proportional to the initial load $L_v(0)$,

$$C_v = \alpha L_v(0), \quad v = 1, 2, \ldots, N, \tag{2}$$

where $\alpha \geq 1$ is the tolerance parameter and N is the number of nodes in the initial network. The removals of nodes owing to either an initial attack or overload failures will led to the redistribution of load among the remaining nodes, and the subsequent overload, i.e., $L_v(t) > C_v$ for some nodes, may occur: the failures are propagated. The cascading process continues until the updated load satisfies $L_v(t) \leq C_v$ for all existing nodes, and the size of the largest connected component N' at the final state is measured. Usually, the damage caused by a cascade is quantified in terms of the relative size G of the largest connected component [3],

$$G = \frac{N'}{N}, \tag{3}$$

which is viewed as a measure of the robustness of network.

3 Strategies of Defense

The four strategies of defense to prevent the cascade from propagating through the entire network are employed and summarized below.

1. *RR of the fluxes*: Randomly Removal (RR) of some fluxes between randomly selected nodes;
2. *IR of the fluxes*: Intentional Removal (IR) of some fluxes between special nodes;
3. *AR of the fluxes*: Adaptive Reduction (AR) of some fluxes depending on the changes of the corresponding shortest path lengths;
4. *IR of the nodes*: Intentional Removal (IR) of some nodes [32].

After the initial attack, the RR of fluxes is implemented by selecting randomly a pair of nodes i and j, and setting $s_{ij}(t \geq 1)$ to 0 until a certain fraction f of fluxes is removed, while the IR of the fluxes is implemented according to the total load generated by the corresponding fluxes. In the initial network, if the communication or traffic flow is closed between node i and node j, the total load generated by the flux between node i and node j

$$L_{ij}^g = 2s_{ij}(d_{ij} + 1), \tag{4}$$

is removed. The factor 2 comes from the fact that a physical quantity is sent from node i to node j and another is sent from node j to node i, i.e., the flow is symmetrical. In general, the flow through the shortest path with large length d_{ij} not only generates more loads to

[1] In the case of shortest-path degeneracy, the value of the path function is reduced by a factor depending on the degrees and depths of the respective branching points.

network but also more possibly travels via the more nodes with high load. Additionally, it has been proved that if the nodes with high load are protected, network would possess high robustness against cascading failures [14]. This observation is our starting point to argue that the size of the cascade can be drastically reduced with the IR of a certain fraction f of the fluxes according to the following strategy: fluxes s_{ij} with the largest L_{ij}^g are removal first right after the initial attack, i.e., let $s_{ij}(t \geq 1) = 0$.

The AR of the fluxes can be introduced into the modeling (1) by reducing the strengths s_{ij} according to the change of the shortest path lengths Δd_{ij}. For demonstration, we adopt an exponential relation

$$s_{ij}(t) = s_{ij}(0) \exp[-\beta \Delta d_{ij}(t)], \tag{5}$$

where $\Delta d_{ij}(t) = d_{ij}(t) - d_{ij}(0)$ and $d_{ij}(t)$ denotes the shortest path length between node i and node j at time t. The nonnegative coefficient β exponentially regulated the dependence of the fluxes on change of the distance between a pair of nodes. The exponential relation is motivated by the dependent relation of links formation on spatial distance. It is presented during the development of many real networks. In biological systems, for instance, gradients of chemical concentrations, or molecule interactions, decay exponentially with distance [35]. In addition, it is worth remarking that, while we focus on the exponential relation, different choices of s_{ij} with a linear or other nonlinear relation to Δd_{ij}, or depending on the length of the effective path [36, 37] or the specific properties of each pair of nodes (degree, unoccupied capacity [14], overload probability [14]), can be considered.

For comparison, the recent proposed strategy-the IR of nodes-is also considered, which may be implemented by adapting anyone of the four following schemes [32]: (i) nodes with smallest load L_i are removed first; (ii) nodes with smallest closeness centrality $\overline{D}_i^{-1}$ are removed first, where $\overline{D}_i$ is the average shortest path length from node i to all the others; (iii) nodes with smallest $\Delta_i = L_i - L_i^g$ are removed first where $L_i^g = \Sigma_j(d_{ij} + 1)$ is the total load generated by node i; (iv) nodes with smallest degree k_i are removed first. In random scale-free networks, since these quantities L_i, $\overline{D}_i^{-1}$, Δ_i, and k_i are strongly positively correlated, the IR of nodes based on the four different schemes shows an almost same efficiency for randomly connected networks (see Fig. 1(b) in [32]). While in non-random networks, they, perhaps, are not equivalent. Two networks: the BA network and the Internet at autonomous system level, considered here, maybe not random. Therefore we firstly need to justify whether the strategies of defense (i)–(iv) are equivalent in these two networks or not. Let g denote the faction of the removed nodes, and then the fraction of the removed fluxes $f \simeq 2g - g^2$ since the IR of nodes corresponds to the removal of all fluxes generated by the removed nodes. In Fig. 1, show the ratio G as a function of the fraction f of IRs. These simulations show that the IR of nodes based on the four different schemes have an almost same efficiency for the two networks. Therefore in the article, we consider the IR of nodes according to only one of these schemes: nodes with smallest load L_i is removed first.

4 Results

To be specific, we firstly consider the Barabási-Albert (BA) scale-free network model [38] to estimate efficiency of these strategies against the cascading failures. The BA network is a heterogeneous one which possesses the power-law degree distribution $P(k) \sim k^{-\gamma}$ with the exponent $\gamma = 3$ [38], and it has been shown that the load distribution exhibits the power-law behavior as well [39], which indicates that there exist a few nodes with very large flow passing them. We focus on the cascades triggered by intentional attacks on a small fraction

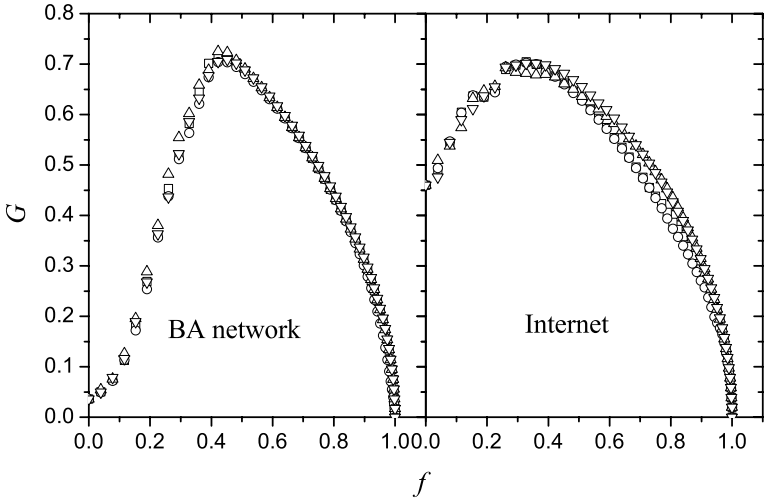

Fig. 1 The relative size G of the largest connected component as a function of the fraction f in the BA network with the system size $N = 5000$ and the average degree $\langle k \rangle = 4$, and the Internet at autonomous system level with $N = 6474$ and $\langle k \rangle \simeq 3.88$. *Different open symbols* correspond to the four different strategies. *Each curve* corresponds to an average over 100 independent realizations for the BA network, while corresponds to an average over 100 different triggers for the Internet

p of nodes with highest loads. Initially, the flux $s_{ij}(0) = 1$ for each pair of nodes. After an initial attack, i.e., a small fraction p of nodes with highest loads is removed from the network, and then the four strategies: the RR of the fluxes, the IR of fluxes, the AR of fluxes and the IR of nodes, are implemented. For the AR of the fluxes, at each time step, the fluxes for each pairs of nodes are recomputed according to (3). Particularly, $s_{ij}(t) = 0$ when node i and node j do not keep connectivity, i.e., $d_{ij}(t) = +\infty$. While in the strategy of the IR of fluxes, the fluxes with largest L_{ij}^{g} are removed first right after the initial attack; and in the IR of nodes, nodes with smallest load L_i are removed first.

Figure 1 shows the relative size G of the largest connected component after a cascade, as a function of the tolerance parameter α, for the four strategies. Without defense, i.e., $\beta = 0.0$ for the AR of fluxes or $f = 0.0$ for the other strategies of defense, the initial attack on only 0.1% (i.e., $p = 0.001$) of the nodes triggers global cascades even for relatively large values of the tolerance parameter (Figs. 2(a) and (b), stars). However, the relative size of the largest connected component G is shown to be larger when the fluxes among some pairs of nodes are reduced or removed according to the strategies of defense mechanism mentioned above (Figs. 2(a) and (b), open symbols). For example, when $\alpha = 1.5$, we have $G \simeq 0.94$ for the RR of fluxes with $f = 0.4$, $G \simeq 0.99$ for the IR of fluxes with $f = 0.4$, $G \simeq 0.64$ for the IR of nodes with $f = 0.4$, and $G \simeq 0.85$ for the AR of fluxes with $\beta = 0.5$, while $G \simeq 0.05$ without a defense. Moreover, by comparing the RR and IR of fluxes with the IR of nodes, we find that the IR of fluxes is optimal to keep a large relative size of the largest connected component. However, it should be pointed out that the measure G is overestimating the positive effect of the strategies of fluxes based on the control of fluxes when compared to the IR of nodes simply. Obviously, in the case of the control of fluxes some nodes will remain weakly connected because some of their fluxes are off, and they are counted as if they are still part of the network without taking this into account. In contrast, in the case of node removal, all nodes that remain connected remain strongly connected.

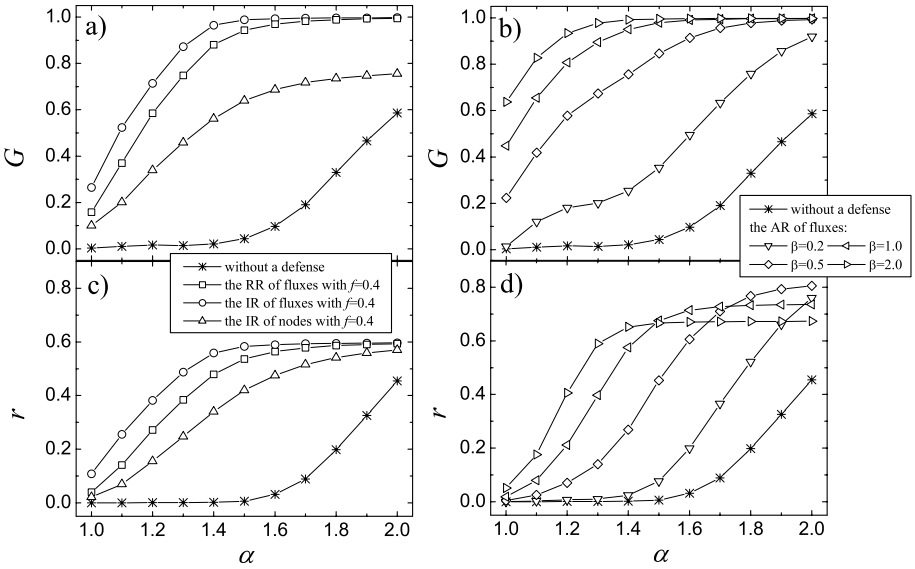

Fig. 2 The relative size G of the largest connected component and the relative remaining fluxes r as a function of tolerance parameter α in the BA network with the system size $N = 5000$ and the average degree $\langle k \rangle = 4$. *Stars* correspond to attacks without defense, while *different open symbols* correspond to the four different strategies. *Each curve* corresponds to an average over 100 independent realizations of the BA network

The final remaining fluxes that can be supported by the network may be a more visual measure for the ability of communication of network than the relative size G of the largest connected component. We define the relative remaining fluxes r as the ratio of the remaining fluxes to the initial fluxes

$$r = \frac{f_r}{f_t} = \frac{f_r}{N(N-1)}, \tag{6}$$

where f_r is the final remaining fluxes supported by the network and f_t denotes the total fluxes in the initial network. In Figs. 2(c) and (d), we report the corresponding relative remaining fluxes r. Though any removal of fluxes always causes the immediate reduction of the remaining fluxes supported by the network, the resulting r can be in this case significantly larger when a suitable fraction of fluxes is intentionally removed according to the strategies (as compared to the case without defense) because these IRs strongly suppress the propagation of the cascade. These results indicate that our strategies are effective and superior to the strategy of the IR of nodes.

Further evidence for our results is presented in Fig. 3, where we show both the ratios G and r as a function of the fraction f for the RR, IR of fluxes and IR of nodes, and as a function of the parameter β for the AR of fluxes, for $\lambda = 1.5$. Great improvement of the robustness of network against the cascading failures becomes clear when comparing the result for our strategies with that obtained from the IR of nodes. Both the relative remaining fluxes and the relative size of the largest component are larger than those for the IR of nodes. In fact, for the IR of nodes, any removal of nodes will cause the immediate reduction of the final number of nodes in the largest connected component, and thus the maximum of G is always smaller than $1 - g$ (g is the faction of the removed nodes). For

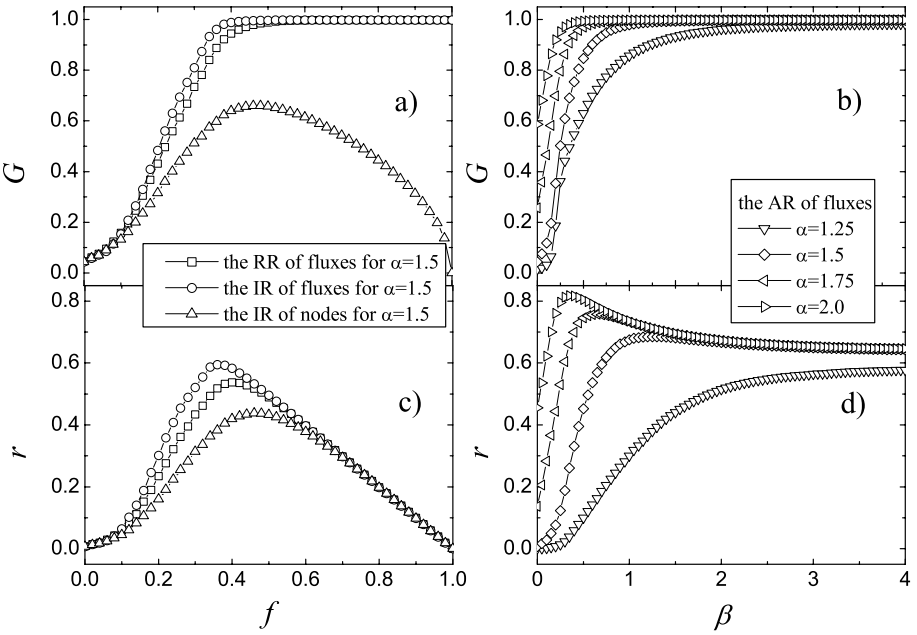

Fig. 3 The relative size G of the largest connected component and the relative remaining fluxes r as a function of parameter f for the RR of fluxes, the IR of fluxes, and the IR of nodes ((**a**) and (**c**)), and as a function of parameter β for the AR of fluxes ((**b**) and (**d**)) in the BA network with the system size $N = 5000$ and the average degree $\langle k \rangle = 4$. *Each curve* corresponds to an average over 100 independent realizations of the BA network

the RR, IR, and AR of fluxes, since no damage is caused by the removal or reduction of fluxes, G can approximate to 1. Indeed, it is intuitively clear that the removal and reduction of fluxes will reduce the probability of a cascade failure and keep G large. However, any limitation of fluxes will cause the immediate reduction of the remaining fluxes, and abate the function of the networks. Thus it will be of practical importance for how to enhance the robustness of network by reducing least fluxes. In Figs. 3(c) and (d), we report the relative remaining fluxes r as a function of the fraction f of the RR, IR of fluxes and IR of nodes, and as a function of the parameter β of the AR of fluxes. For all these strategies, the ratio r displays a well-defined maximum. When f or β is large, the propagation of the cascade is strongly suppressed and nearly all reduction of fluxes is caused by the removals or adaptive reduction. When f or β is small, the ratio r is small since most of the fluxes are broken down by the cascade itself. The maximum of r lies in a region of intermediate f or β where the propagation of the cascade is significantly suppressed and the reduction of fluxes caused by the removals or adaptive reduction is relatively small. Moreover, by comparing the results for the RR, IR, and AR of fluxes with that for the IR of nodes, we find that the relative remaining fluxes r are significant larger than that for the IR of nodes (see Fig. 3(c)). In fact, the IR of nodes corresponds to the removal of all fluxes generated by the removed nodes. However, for these fluxes, only a part of them indeed play an important role to trigger further overload failure. In this stage, our strategies, based on the reduction and removal of the fluxes, save a large amount of fluxes since it is not necessary to remove the total fluxes $s_i = 2\Sigma_j s_{ij}$ sent out and received by node i to prevent the prop-

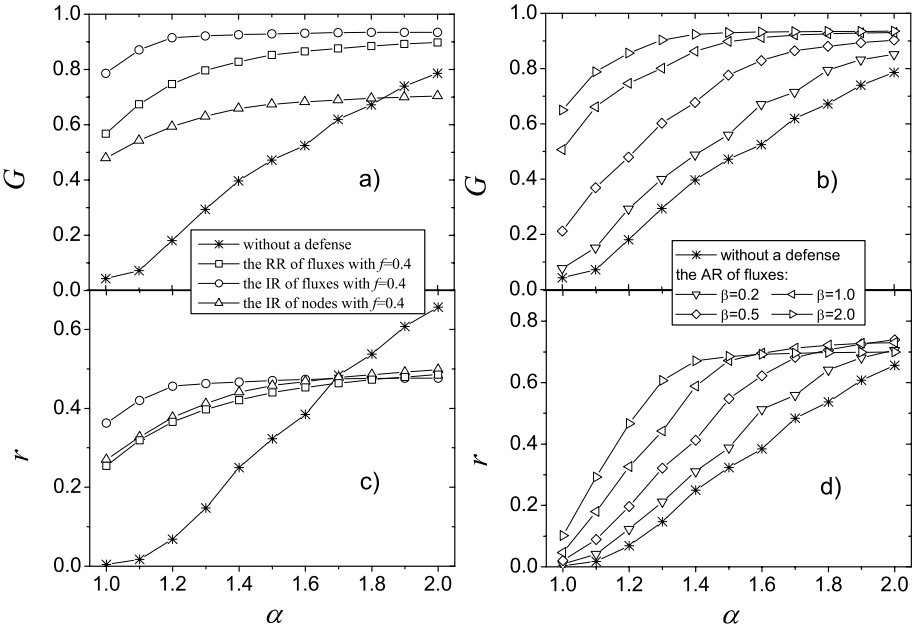

Fig. 4 The relative size G of the largest connected component and the relative remaining fluxes r as a function of tolerance parameter α in the Internet at autonomous system level, which has $N = 6474$ and $\langle k \rangle \simeq 3.88$. *Stars* correspond to attacks without defense, while *different open symbols* correspond to the four different strategies. *Each curve* corresponds to an average over 100 different triggers for attacks in 5 nodes which are randomly selected from 10 highest loaded nodes

agation of a cascade. Moreover, fewer fluxes are needed to be removed in our strategies for preventing the propagation of the cascade, and thus the relative remaining fluxes r is larger than that for the IR of nodes. In addition, for the AR of fluxes, with the increasing of β, the relative remaining fluxes firstly increase sharply and then encounter a slow decrease, finally approach a nonzero plateau value for even large value of β. In general, increasing of β seems to make the final fluxes reduced even more. However, the reduction of fluxes can effectively prevent further overload failures of nodes and thus stop the further reduction of the fluxes.

Secondly, we consider the Internet at autonomous system level to estimate efficiency of these strategies against the cascading failures. The real map of the Internet considered here, provided by the National Laboratory for Applied Network Research and available at the web site http://pil.phys.uni-roma1.it/~gcalda/cosinsite/extra/data/internet/nlanr.html, contains 6474 nodes and 12572 links, corresponding to an average connectivity $\langle k \rangle \simeq 3.88$. The Internet is a heterogeneous network in term of the degree distribution or the load distribution. The connectivity distribution is scale-free, with a connectivity exponent $\gamma = 2.21$. In addition, it exhibits a strong negative degree-degree correlations [40], and its Pearson correlation coefficient is equal to -0.18, which indicates that it is not a random scale-free network. In such network, our simulations present the results that have not a fundamental deviation from those in the BA scale-free network (see Figs. 4 and 5). Perhaps, the efficiencies of these strategies are determined by the broad degree or load distribution, while less dependent on the degree-degree correlation.

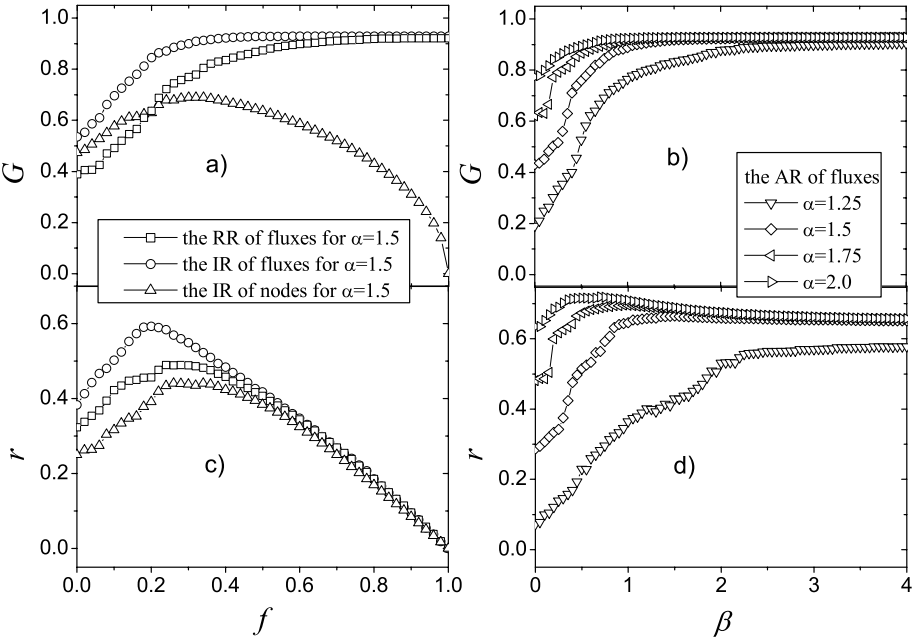

Fig. 5 The relative size G of the largest connected component and the relative remaining fluxes r as a function of parameter f for the RR of fluxes, the IR of fluxes, and the IR of nodes ((**a**) and (**c**)), and as a function of parameter β for the AR of fluxes ((**b**) and (**d**)) in the western U.S. power transmission grid, which has $N = 6474$ and $\langle k \rangle \simeq 3.88$. *Each curve* corresponds to an average over 100 different triggers for attacks in 5 nodes which are randomly selected from 10 highest loaded nodes

5 Discussion and Conclusion

In summary, we have proposed and investigated three strategies of defense to prevent the propagation of a cascade. By applying them to both the artificially created scale-free network and the Internet at autonomous system level, we have shown that the size of the cascade can be drastically reduced and at the same time the remaining fluxes supported by the networks is large by selectively removing a small fraction of fluxes exchanged between the nodes. Recent evidence has shown that the fragility of networks to cascading failures is rooted in the broad load distribution. Specially, the existence of nodes with high load can make the network vulnerable to cascading failures which have been observed in many transportation networks [39, 41, 42]. Thus a more effective strategy might be designed by considering the intentional removal of the fluxes that flows through the nodes with high load. In addition, it is true that the intentional removal of nodes would require more than strictly local information, but it should be acknowledged that these strategies based on the control of fluxes require even more detailed information about the structure and dynamics of the entire network. Such global information often proves hard to gather [43]. From this perspective, it will be of practical importance to develop effective strategy of defense by using only local information about network.

In addition, the adaptive reduction mechanism of fluxes described here, which may stem from alternative dynamical schemes of fluxes, should be considered as only the first step to explore the underlying factors driving the fluxes temporal fluctuations [14, 16] or dynamical evolution [15]. Proper formation of complex adjustment mechanism requires taking many

more detailed factors into account. Also, the adaptive reduction can be viewed as the possible responding mechanism of networked systems to the cascading failures.

Acknowledgements This work has been supported by the General Project of Hunan Provincial Educational Department of China under Grant No. 07C754, and the National Natural Science Foundation of China under Grant No. 30570432. We are also grateful for the comments and suggestions from the two anonymous referees.

References

1. Holme, P., Kim, B.J.: Vertex overload breakdown in evolving networks. Phys. Rev. E **65**, 066109 (2002)
2. Holme, P.: Edge overload breakdown in evolving networks. Phys. Rev. E **66**, 036119 (2002)
3. Motter, A.E., Lai, Y.-C.: Cascade-based attacks on complex networks. Phys. Rev. E **66**, 065102(R) (2002)
4. Moreno, Y., Gómez, J.B., Pacheco, A.F.: Instability of scale-free networks under node-breaking avalanches. Europhys. Lett. **58**, 630–636 (2002)
5. Sachtjen, M.L., Carreras, B.A., Lynch, V.E.: Disturbances in a power transmission system. Phys. Rev. E **61**, 4877–4882 (2000)
6. Jacobson, V.: Congestion avoidance and control. Comput. Commun. Rev. **18**, 314–329 (1988)
7. Guimerà, R., Arenas, A., Díaz-Guilera, A., Giralt, F.: Dynamical properties of model communication networks. Phys. Rev. E **66**, 026704 (2002)
8. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., Hwang, D.-U.: Complex networks: structure and dynamics. Phys. Rep. **424**, 175–308 (2006)
9. Carreras, B.A., Lynch, V.E., Dobson, I., Newman, D.E.: Critical points and transitions in an electric power transmission model for cascading failure blackouts. Chaos **12**(4), 985–994 (2002)
10. Watts, D.J.: A simple model of global cascades on random networks. Proc. Natl. Acad. Sci. USA **99**, 5766–5771 (2002)
11. Zhao, L., Park, K., Lai, Y.-C.: Attack vulnerability of scale-free networks due to cascading breakdown. Phys. Rev. E **70**, 035101(R) (2004)
12. Zhao, L., Park, K., Lai, Y.-C., Ye, N.: Tolerance of scale-free networks against attack-induced cascades. Phys. Rev. E **72**, 025104(R) (2005)
13. Kinney, R., Crucitti, P., Albert, R., Latora, V.: Modeling cascading failures in the North American power grid. Eur. Phys. J. B **46**, 101–107 (2005)
14. Kim, D.-H., Motter, A.E.: Fluctuation-driven capacity distribution in complex networks. New J. Phys. **10**, 053022 (2008)
15. Simonsen, I., Buzna, L., Peters, K., Bornholdt, S., Helbing, D.: Transient dynamics increasing network vulnerability to cascading failures. Phys. Rev. Lett. **100**, 218701 (2008)
16. Heide, D., Schäfer, M., Greiner, M.: Robustness of networks against fluctuation-induced cascading failures. Phys. Rev. E **77**, 056103 (2008)
17. Wang, B., Kim, B.J.: A high-robustness and low-cost model for cascading failures. Europhys. Lett. **78**, 48001 (2007)
18. Crucitti, P., Latora, V., Marchiori, M.: Model for cascading failures in complex networks. Phys. Rev. E **69**, 045104(R) (2004)
19. Wang, W.-X., Chen, G.: Universal robustness characteristic of weighted networks against cascading failure. Phys. Rev. E **77**, 026101 (2008)
20. Goh, K.-I., Lee, D.-S., Kahng, B., Kim, D.: Sandpile on scale-free networks. Phys. Rev. Lett. **91**, 148701 (2003)
21. Moreno, Y., Pastor-Satorras, R., Vázquez, A., Vespignani, A.: Critical load and congestion instabilities in scale-free networks. Europhys. Lett. **62**, 292–298 (2003)
22. Guimerà, R., Díaz-Guilera, R.A., Vega-Redondo, F., Cabrales, A., Arenas, A.: Optimal network topologies for local search with congestion. Phys. Rev. Lett. **89**, 248701 (2002)
23. Albert, R., Albert, I., Nakarado, G.L.: Structural vulnerability of the North American power grid. Phys. Rev. E **69**, 025103 (2004)
24. Zhao, X.M., Gao, Z.Y.: Topological effects on the performance of transportation networks. Chin. Phys. Lett. **24**, 283–286 (2007)
25. Wu, J.J., Gao, Z.Y., Sun, H.J., Huang, H.J.: Congestion in different topologies of traffic networks. Europhys. Lett. **74**, 560–566 (2006)
26. Zheng, J.F., Gao, Z.Y., Zhao, X.M.: Clustering and congestion effects on cascading failures of scale-free networks. Europhys. Lett. **79**, 58002 (2007)

27. Huang, L., Lai, Y.-C., Chen, G.: Understanding and preventing cascading breakdown in complex clustered networks. Phys. Rev. E **78**, 036116 (2008)
28. Gallos, L.K., Cohen, R., Argyrakis, P., Bunde, A., Havlin, S.: Stability and topology of scale-free networks under attack and defense strategies. Phys. Rev. Lett. **94**, 188701 (2005)
29. Schäfer, M., Scholz, J., Greiner, M.: Proactive robustness control of heterogeneously loaded networks. Phys. Rev. Lett. **96**, 108701 (2006)
30. Li, P., Wang, B.-H., Sun, H., Gao, P., Zhou, T.: A limited resource model of fault-tolerant capability against cascading failure of complex network. Eur. Phys. J. B **62**, 101–104 (2008)
31. Yang, R., Wang, W.-X., Lai, Y.-C., Chen, G.: Optimal weighting scheme for suppressing cascades and traffic congestion in complex networks. Phys. Rev. E **79**, 026112 (2009)
32. Motter, A.E.: Cascade control and defense in complex networks. Phys. Rev. Lett. **93**, 098701 (2004)
33. Anghel, M., Werley, K.A., Motter, A.E.: Stochastic model for power grid dynamics. In: Proceedings of the Fortieth Hawaii International Conference on System Sciences, Big Island, Hawaii, January 3–6, 2007. arXiv:physics/0609217 [physics.soc-ph]
34. Newth, D., Ash, J.: Evolving cascading failure resilience in complex networks. Complex. Int. **11**, 125–136 (2005)
35. Murray, J.D.: Mathematical Biology. Springer, Heidelberg (1990)
36. Yan, G., Zhou, T., Hu, B., Fu, Z.-Q., Wang, B.-H.: Efficient routing on complex networks. Phys. Rev. E **73**, 046108 (2006)
37. Zhao, H., Gao, Z.-Y.: Cascade defense via navigation in scale free networks. Eur. Phys. J. B **57**, 95–101 (2007)
38. Barabási, A.-L., Albert, R.: Emergence of scaling in random networks. Science **286**, 509–512 (1999)
39. Goh, K.I., Kahng, B., Kim, D.: Universal behavior of load distribution in scale-free networks. Phys. Rev. Lett. **87**, 278701 (2001)
40. Newman, M.E.J.: Assortative mixing networks. Phys. Rev. Lett. **89**, 208701 (2002)
41. Ohira, T., Sawatari, R.: Phase transition in a computer network traffic model. Phys. Rev. E **58**, 193–195 (1998)
42. Holme, P.: Congestion and centrality in traffic flow on complex networks. Adv. Complex Syst. **6**, 163–176 (2003)
43. Cohen, R., Havlin, S., ben-Avraham, D.: Efficient immunization strategies for computer networks and populations. Phys. Rev. Lett. **91**, 247901 (2003)