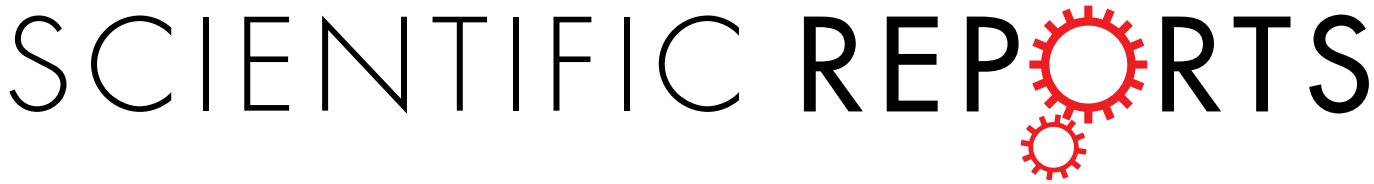

OPEN

Ability paradox of cascading model based on betweenness

Jianwei Wang, Bo Xu & Yuedan Wu

Received: 29 January 2015
Accepted: 03 August 2015
Published: 10 September 2015

Must Investing more resources to protect every node in a network improve the robustness of the whole network subject to target attacks? To answer this question, we investigate the cascading dynamics in some typical networks. In real networks, the load on a node is generally correlated with the betweenness. Considering the weight of a node, we give a new method to define the initial load on a node by the revised betweenness. Then we present a simple cascading model. We investigate the cascading dynamics by disabling a single key node with the highest load. We find that in BA scale-free networks, the bigger the capacity of every node, the stronger the robustness of the whole network. However, in WS networks and some random networks, when we increase the capacity of every node, instead, the robustness of the whole network is weaker. In US power grid and the China power grid, we also observe this counterintuitive phenomenon. We give a reasonable explanation by a simple illusion. By the analysis, we think that resurrections of some nodes in a ring network structure after removing a node may be the reason of this phenomenon.

Over the past several years, the study on the network robustness[1–11] has been attracted so much attention. In particular, many researchers focus on the vulnerability of natural and man-made complex systems under cascading failures induced by removing some critical nodes or edges. Cascading failures are ubiquitous in power grid, traffic networks, and computer networks[12–15]. In these networks, there exist the loads in forms of electricity, traffic flows, or data flows. Under normal circumstances, no cascading failure occurs and the system maintains its normal and efficient functioning, while the failures of some key nodes or edges may cause large amount of loads to redistribute among other nodes in the networks, which may trigger more nodes' failure and even entire collapse of the network. Some typical real-world examples of cascading failures are the large-scale blackouts in some countries, e.g., the blackouts of America in 2003, Italy in 2003, London in 2003, and northern India in 2012. In addition, the Internet collapse caused by the submarine earthquake near Taiwan in December 2006 and frequent traffic paralysis in some cities are also caused by long and intricate cascades of events.

Considering the vital importance of the safety of infrastructure networks, many researchers investigate the cascading phenomenon from different aspects, and many valuable conclusions have been reached, focusing on a variety of modeling approaches of cascading failures[16–24], the cascade mechanism and control measures[25–36], effective protection and attack strategies[37–40], cascading modeling in interdependent networks[41–53], cascading modeling in infrastructure networks[54–63], and so on. One of the key contents in previous works on cascading failures is how to assign the initial load on a node or an edge. In earlier studies, the initial load on a node or an edge was generally estimated by the global betweenness, of which the pioneering work by Motter *et al.*[64] discuss cascade-based attacks on complex networks and demonstrate that the attack on a single important node (one of those with high load) may trigger a cascade of overload failures capable of disabling the network almost entirely. Hereafter, to better control and defense cascading failures in complex networks, based on the betweenness method, Motter[25] introduce and investigate a costless strategy of defense based on a selective further removal of nodes and edges, right after the initial attack or failure, and find that this intentional removal of network elements can drastically reduce the size of the cascade. Crucitti *et al.*[65] propose a simple model for cascading failures based on the dynamical redistribution of the flow on the network and also show that the breakdown of a single node is sufficient to affect the efficiency of a network up to the collapse of the entire system if

School of Business Administration, Northeastern University, Shenyang 110819, P. R. China. Correspondence and requests for materials should be addressed to J.W. (email: jwwang@mail.neu.edu.cn)

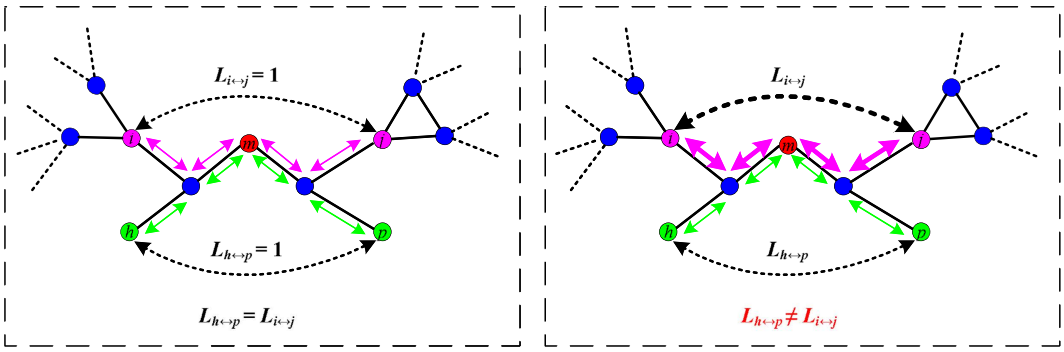

Figure 1. The scheme illustrates the correlation between the load transported between two nodes and the degrees of two ends. We use $L_{i\leftrightarrow j}$ ($L_{h\leftrightarrow p}$) denote the load transported between nodes i (h) and j (p). In traffic networks, the power grid, and the Internet, the bigger the degree of a node, the higher the load generated from it. Therefore, in general, $L_{h\leftrightarrow p} \neq L_{i\leftrightarrow j}$.

the node is among the ones with the largest load. Although the betweenness method to assign the initial load on a node or an edge can better reflect the flow of physical quantities in many realistic situations, it may not be practical for very large networks in some real networks such as the Internet or WWW, owing to its consideration of the whole networks topological information. Therefore, taking into account the simplicity of the strategy with the local degree, based on the information of the degrees of two nodes connected by an edge, W. X. Wang and G. R. Chen[20] propose a new approach to define the initial load on an edge and present a cascading model. Motivated by their works, many researchers define the initial load on a node or an edge from the perspective of the degree and construct different cascading models. Since the definition of the initial load in the degree method ignores the flow characteristic of the load transported between two nodes, the constructed cascading models are valid in many actual applications.

To this end, applying the information of the degree and considering the calculation of the betweenness of a node, we introduce a new method to assign the initial load on this node and construct a cascading model with a tunable parameter. We focus on how the breakdown of a single node with the highest load due to attacks or failures is sufficient to collapse the entire network. In some man-made networks and infrastructure networks, because of the dynamics of redistribution of flows on the network, we observe that all these networks undergo a global cascade of overload failures when highly loaded nodes are removed. However, in WS networks, ring-coupled networks, some ER networks, and Power grid, we surprisingly find a counterintuitive phenomenon, i.e., the improvement of the capacity of every node does not reduce the size of the cascade, instead, the robustness of the network is more weaker. While in BA networks and US air port networks, naturally, the increase of the capacity of every node reduces the damage of the cascade. We observe that the phenomenon of the ability paradox of the cascading propagation is ubiquitous in many networks. In a ring-coupled network with 13 nodes and 26 edges, we also find this phenomenon. By carefully analyzing the dynamic mechanism of the cascading propagation and the calculating process of the betweenness of a node, we speculate that a kind of the ring structure in the remaining network after removing a node may be a cause of the ability paradox. Starting from a coupled-ring network and according to the rewiring probability on each existing edge, we study the cascading propagation in a serial of networks with the ring structure and observe the ability paradox in our cascading model. Our work may have practical value for controlling various cascading-failure-induced disasters in the real world.

The Model

In many infrastructure networks, the loads of different forms are sent among nodes, e.g., data packets in computer networks, traffic flows in traffic networks, and electric current in power grid. In general, when the load is sent from one node to another, it is efficient to take a road along the shortest paths connecting these two nodes. In previous works, there are many ways to measure the load on a node or an edge, but, considering actual applications, many researchers define the initial load on a node or an edge to the total number of shortest paths passing through this node or this edge.

Although the method by shortest paths is suitable for actual applications, it ignores the differences among nodes with the different degree (see Fig. 1). In the left sub-figure of Fig. 1, in the betweenness method, the load $L_{i\leftrightarrow j}$ transported between nodes i and j is 1, i.e., only one new generated packet transmitted along the shortest paths connecting nodes i and j. Similarly, $L_{h\leftrightarrow p}=1$. Thus, $L_{h\leftrightarrow p}=L_{i\leftrightarrow j}$. However, in real networks, the bigger the degree of a node, the higher the load generated from it. In the right sub-figure of Fig. 1, owing to the effect of the differences of the node degree, $L_{h\leftrightarrow p} \neq L_{i\leftrightarrow j}$, and generally $L_{h\leftrightarrow p} < L_{i\leftrightarrow j}$. Therefore, according to the node degree and the shortest paths, we propose a new method

to assign the initial load on a node, which can more suitable for defining the physical quantity of the load than previous methods.

Next, we simply introduce a new way to measure the initial load. First, we define the weights of nodes i and j to $w_i = k_i^{\alpha}$ and $w_j = k_j^{\alpha}$, respectively. In general, the bigger the weight of a node, the higher the load generated from it. For simplicity, we assume the loads transmitted between nodes i and j to $L_{i\leftrightarrow j} = w_i w_j$, i.e., $L_{i\leftrightarrow j} = k_i^{\alpha} k_j^{\alpha}$. These loads are transmitted along the shortest paths connecting nodes i and j. If there is more than one shortest path connecting two given nodes, the packet is divided evenly at each branching point. We define $L_m^{(i,j)}$ to denote the contribution of a packet transmitted between nodes i and j to the load on node m. Thus, the contribution of the load $L_{i\leftrightarrow j}$ transmitted between nodes i and j to the load on node m is $C_m^{(i,j)} = L_{i\leftrightarrow j} L_m^{(i,j)}$. The load L_m on node m is then

$$L_m = \sum_{i,j} C_m^{(i,j)} = \sum_{i,j} L_{i\leftrightarrow j} L_m^{(i,j)}, \tag{1}$$

where the sum is over all pairs of nodes in a network.

When $\alpha = 0$, our method to define the load on a node reduces to the one described in Refs 25,64,65, i.e., the load at a node is the total number of shortest paths passing through the node. The load $L_m(t)$ on node m at time t is the total number of all contributions of every ordered pairs of all nodes in the network at time t. Each node m is assigned to have a finite capacity C_m, i.e., the maximum load that node can handle. Following Refs 19–21,29–31,39,40, we assume the capacity C_m of node m to be proportional to its initial load $L_m(0)$:

$$C_m = (1 + \beta) L_m(0), \quad m = 1, 2, \ldots, N, \tag{2}$$

where the parameter $\beta \geq 0$ is the tolerance parameter and N is the initial number of nodes in the network. The node m maintains its normal and efficient functioning if $L_m \leq C_m$; otherwise it fails and is removed from the network. In the initial stage at time $t = 0$, the network operates in a free-flow state. However, the removals of nodes due to attacks or failures, in general, change the distribution of the load on every node. Once the loads on some nodes exceed their capacities, these nodes will be removed from the remaining network, which will lead to a new redistribution of loads and, as a result, subsequent failures can occur. The cascading propagation will stop when the loads on all remaining nodes do not exceed their capacities.

In this paper, we only focus on the cascading propagation triggered by removing a node with the highest load. Here, we use ϖ_t to denote the resulting network after failed nodes are removed at time t. In a connected network ϖ_0 at time $t = 0$, no cascading failures occur because $L_m(0) \leq C_m(\beta \geq 0), \forall m$. We assume that an initial attack is performed at time $t = 1$, i.e., one node with the highest load is removed from the network ϖ_0 and the resulting network is denoted by ϖ_1. Since the removal of a node may change the shortest paths between some node pairs and consequently a global redistribution of the load among the remaining nodes in the network ϖ_1, we recalculate the load $L_i(1)$ on each remaining node, where $i \in \varpi_1$. The updated load on some nodes may exceed their capacities, all the overloaded nodes then are removed from the ϖ_1 and the resulting network is denoted by ϖ_2. This leads to a new redistribution of loads and subsequent overloads may occur. The overloaded nodes are removed and the resulting network is denoted by ϖ_3, and so on. When at time ε, the updated load satisfies $L_k(\varepsilon) \leq C_k$ for all the nodes k in the remaining ϖ_1, the cascading failures stop. The damage caused by a cascade is quantified in terms of the largest connected component G and the avalanche size S_{attack}.

The analysis of the cascading model. Two fundamental questions are, how the parameter α affect the network robustness against cascading failure and, the bigger the parameter β, the stronger the robustness of the network? To answer these questions, we focus on global cascades triggered by removing one node with the highest load. The reason that we choose the node with the highest load to the attacked object is because this node plays the vital role in the cascading failures in most previous studies. We illustrate how our model works in practice by considering two artificially created network topologies: a scale-free network (Barabasi-Albert)[66] and a small-world network (Watts-Strogatz)[67]. The Watts-Strogatz small-world network (WS) starts as a lattice ring with N nodes, of which each node is connected with its $2m$ neighbors (m for each side). For each link, there is then a rewiring probability p. When $p = 0.01$, the generated network (WS) with N nodes and $m * N$ edges has the small-world property. In numerical simulations, we set $N = 1000$ and $m = 2$, i.e., the average degree $\langle k \rangle$ is equal to 4. BA networks can be constructed as follows: starting from m_0 fully connected nodes, a new node with $m (m \leq m_0)$ edges is added to the existing network at each time step according to the preferential attachment, i.e., the probability of being connected to the existing node i is proportional to its k_i. We set $N = 1000$ and $m_0 = 3$, $m = 2$, i.e., the average degree $\langle k \rangle$ is about 4.

In Fig. 2, we discuss cascading failures in BA scale-free networks and WS small-world networks, as triggered by the removal of the node with the highest load. The damage caused by a cascade is quantified by two measures, i.e., the largest connected component G and the average number S_{attack} of the failed nodes. After the removal of one node with the highest load, the redistribution of other nodes in turn

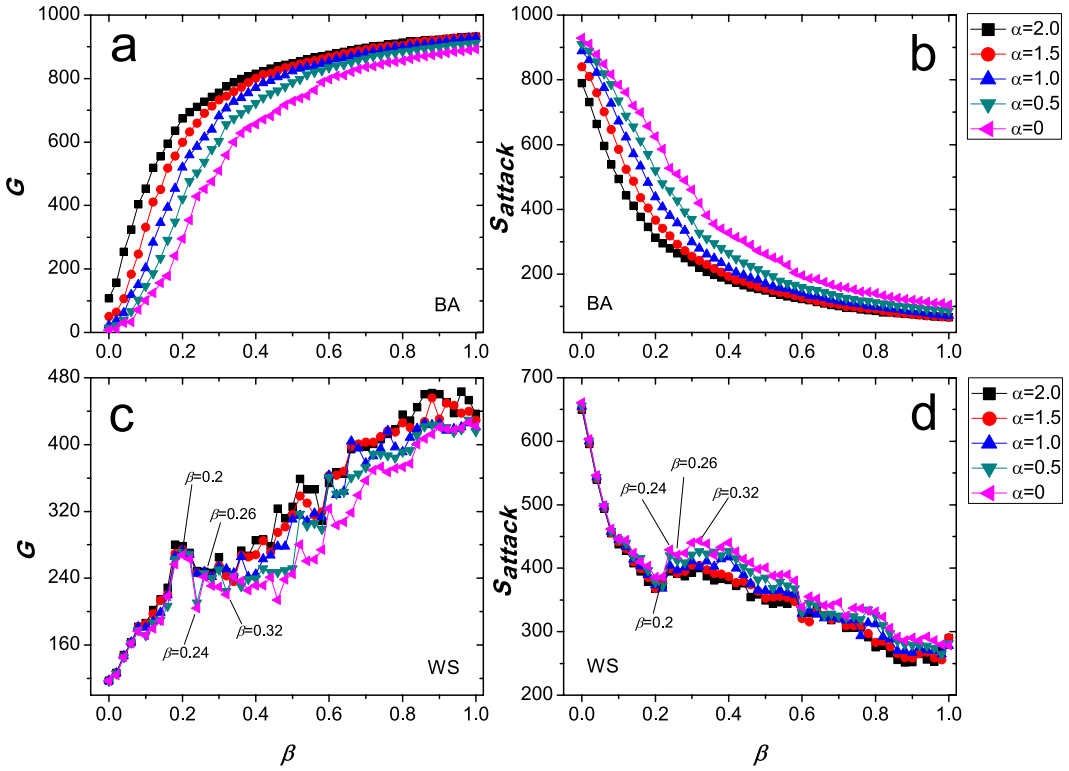

Figure 2. Cascading failures in BA scale-free networks and WS small-world networks.

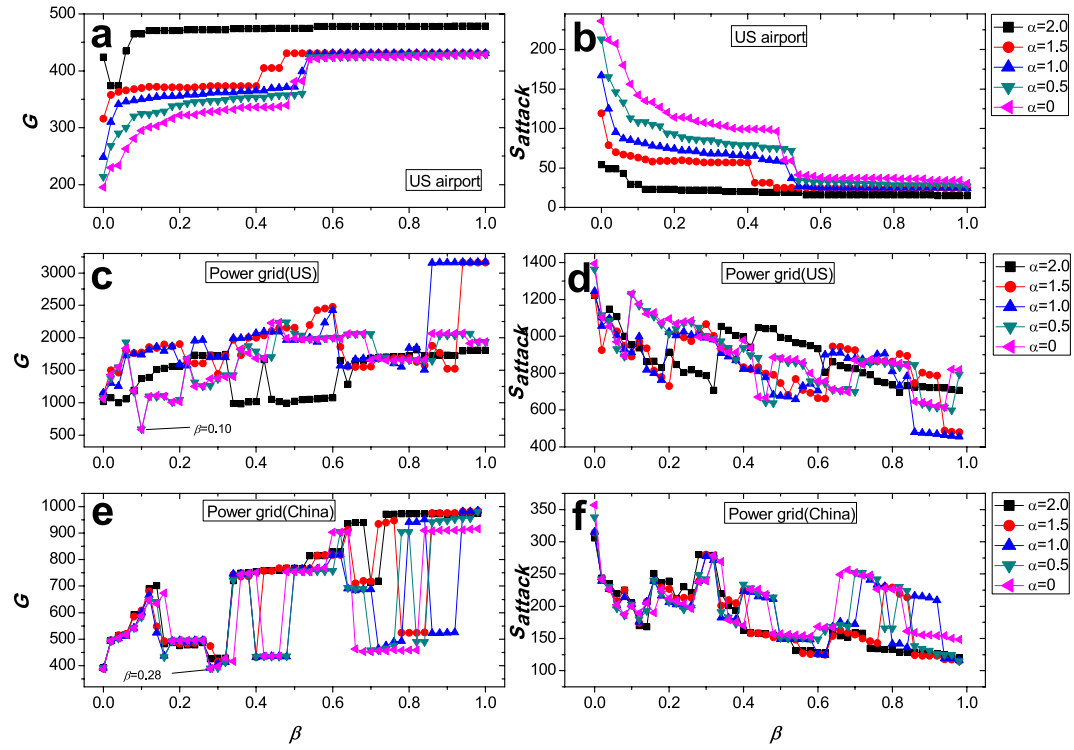

Figure 3. Cascading failures in a US airport network and two power grids.

may lead to the propagation of failures throughout the network. In Fig. 2(a,d), by gradually increasing the value of the capacity parameter β, We compare the effect of the parameter α on the robustness of BA networks and WS networks in five cases of $\alpha = 0$, $\alpha = 0.5$, $\alpha = 1.0$, $\alpha = 1.5$, and $\alpha = 2.0$. When $\alpha = 0$,

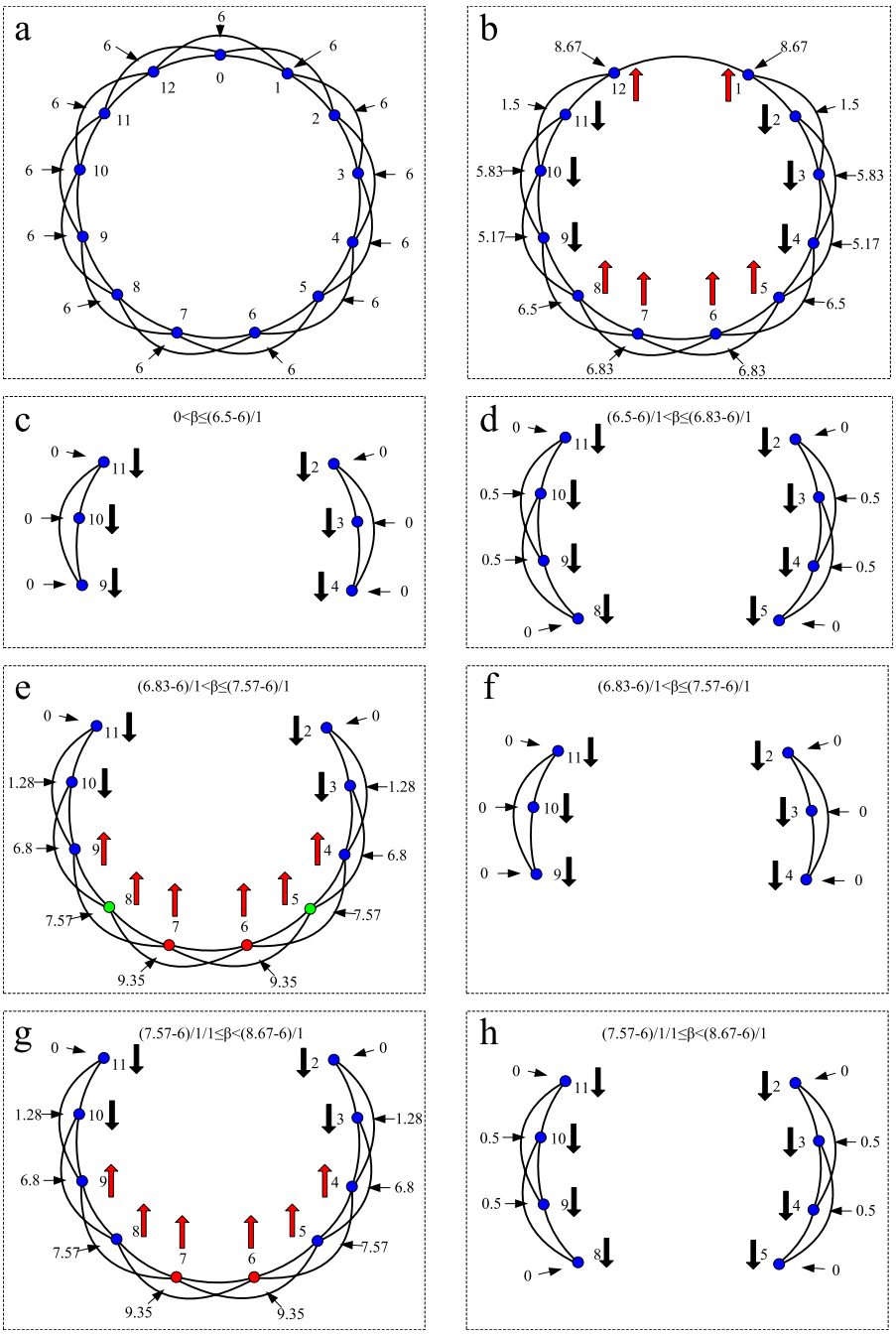

Figure 4. Analysis of the ability paradox in a coupled-ring network with 13 nodes and 26 edges.

the cascading model in Ref. 31 is a special case of our new model. Each curve is obtained by averaging over experiments on 20 independent networks. By two measures of G and S_{attack}, we can clearly see that, as the value α increases, the robustness of BA networks and WS networks is stronger. In addition, we observe an interesting phenomenon, i.e., the ability paradox in the cascading model. According to the definition of the cascading model, the larger the value of the parameter β, the stronger the capacity of each node in a network. Generally, we intuitively think that, the stronger the capacity of each node in a network, the stronger the robustness of the whole network against cascading failures. While in WS networks (Fig. 2(c,d)), the numerical results are not what we expected. There exist some unusual data points in every curve of $\alpha = 0$, 0.5, 1.0, 1.5, 2.0, for example G and S_{attack} in the cases of $\beta = 0.24$ (from $\beta = 0.2$ to $\beta = 0.24$) and $\beta = 0.32$ (from $\beta = 0.2$ to $\beta = 0.24$) when $\alpha = 0$. From most previous cascading models, it is difficult to understand this strange phenomenon. In Fig. 2, we observe that this ability paradox only exists in WS networks. In other words, this interesting phenomenon is not universal in all networks. Using our cascading model, we further investigate cascading failures in real networks, i.e., a US airport network and two power grids.

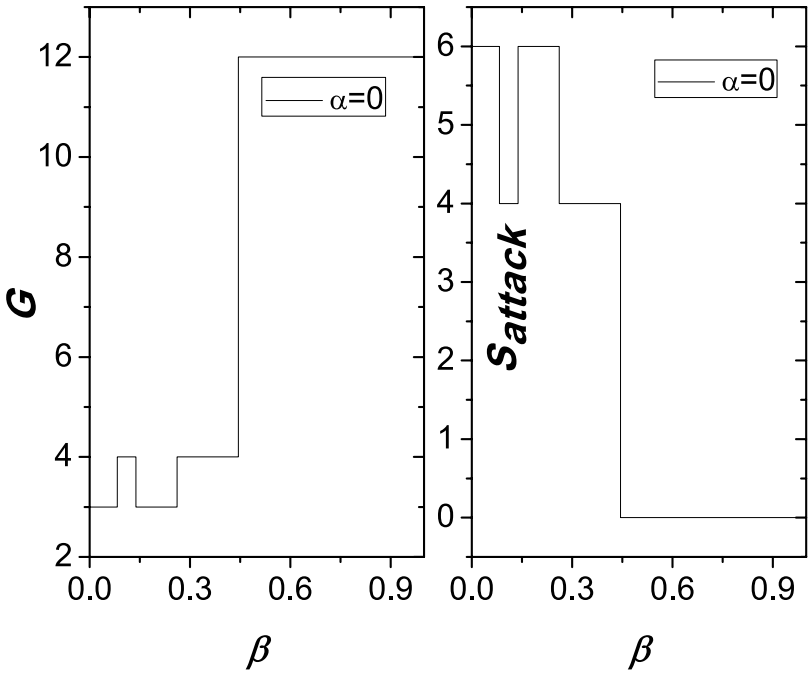

Figure 5. Correlation between two measures (G and S_{attack}) and the parameter β after removing a node in Fig. 4.

In Fig. 3(a–f), we investigate cascading failures in a US airport network and two power grids (the power grid of five provinces in China southern with 1658 nodes and 4116 edges[68] and the power grid in the western United States with 4941 nodes and 6594 edges[67]), as triggered by the removal of the node with the highest load. The legends and other parameters are the same as Fig. 2. In the US airport network (Fig. 3(a)), only when $\alpha = 2.0$, we can observe the phenomenon of the ability paradox from 0 to 0.02 (values of β). While in two power grids (Fig. 3(c–f)), all curves show the obvious and wide fluctuation, which shows that sometimes investing more resources to protect a network is often played an opposite effect. For example, according to the largest connected component G in the US power grid (Fig. 3(c)), the network robustness of $\beta = 0$ is significantly stronger than that of $\beta = 0.10$ in the case of $\alpha = 0$, which means that investing more protected resources makes the network more fragile. Similarly, in the power grid of five provinces in China southern (Fig. 3(e)), we can see that the values of G in two cases of $\beta = 0$ and $\beta = 0.28$ are almost same. Next, a natural question arises: what causes this counterintuitive phenomenon? We carefully analyze the cascading dynamical mechanisms, and speculate that some types of the local topology in a network may be the culprit of the ability paradox. We further try to explain this counterintuitive phenomenon by the local topology in a network.

Firstly, using a coupled-ring network with 13 nodes and 26 edges, we analyze the interesting phenomenon of the ability paradox by the load change after removing one node with the highest load. In every sub-figures in Fig. 4, the numbers inside and outside the coupled-ring network represent the labels of nodes and the initial load on each node in the case of $\alpha = 0$ in our model. (*a*) In the initial state, the initial load on each node is 6. (*b*) After node 0 is removed from the network, we recalculate the load on each node and label the fluctuation of the load on each node by arrows, of which red arrow up represents that the load on a node increases, and black arrow down represent that the load on a node decreases, compared with the initial state in *a* sub-figure. In *c*, *d*, *e*, *f*, *g*, and *h* sub-figures, as values of the parameter β increase, we describe the cascading dynamical process of our model. (*c*) When $0 < \beta \leq (6.5 - 6)/6$, by analyzing *a* sub-figure, we can find that the loads on nodes 1, 5, 6, 7, 8, and 12 exceed their capacities, thus these nodes are removed from the network. After those nodes fail, because that the loads on the remaining nodes 2, 3, 4, 9, 10, and 11 do not exceed their capacities, no cascading failures occur and the system including nodes 2, 3, 4, 9, 10, and 11 maintains its normal and efficient functioning. Thus, in *c* sub-figure, the largest connected component G and the number S_{attack} of the failed nodes are 3 and 6, respectively. (*d*) By the similar analysis, when $(6.5 - 6)/6 < \beta \leq (6.83 - 6)/6$, we can obtain that the values of G and S_{attack} are 4 and 4, respectively. (*e*) when $(6.83 - 6)/6 < \beta \leq (7.75 - 6)/6$, by analyzing *a* sub-figure, we find that, nodes 1 and 12 fail in the first stage of the cascading propagation. Then we recalculate the load on each remaining node (see *e*) and find that the loads on nodes 5, 6, 7, and 8 exceed their capacities. (*f*) Therefore, in the second stage of the cascading propagation, nodes 5, 6, 7, and 8 are removed from the network, and because that the loads on the remaining nodes 2, 3, 4, 9, 10, and 11 do not exceed their capacities, no cascading failures occur and the system including nodes 2, 3, 4, 9,

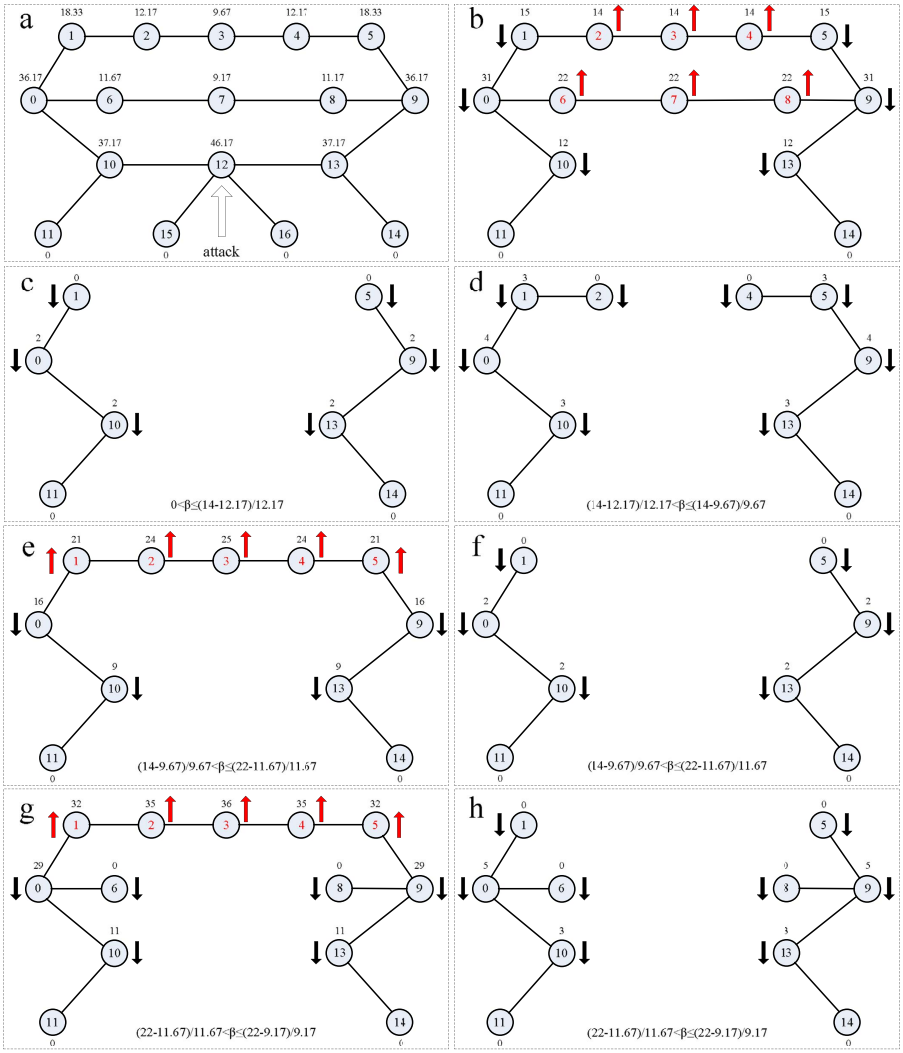

Figure 6. Analysis of the ability paradox in a network with the typical topology structure.

10, and 11 maintains its normal and efficient functioning. Finally, we get that the values of G and S_{attack} are 3 and 6, respectively. As the value of β increases from $(6.56-6)/6 < \beta \leq (6.83-6)/6$ to $(6.83-6)/6 < \beta \leq (7.75-6)/6$, interestingly we observe that, the robustness of the network is weaken. By analyzing *e* sub-figure again, we find that, after the first stage of cascading failures occurs, it is because of the survivals of nodes 6 and 7 lead to the failures of nodes 5 and 8 (labeled by green circles), which maintain their normal and efficient functioning in *d* sub-figure. (*g*) By the similar analysis above, when $(7.57-6)/6 < \beta \leq (8.67-6)/6$, we give the states of every remaining nodes after the first stage of the cascading propagation. (*h*) After the second stage of the cascading propagation in *g* sub-figure, we can obtain that the values of G and S_{attack} are 4 and 4, respectively. When $(8.67-6)/6 < \beta$, the removal of node 0 does not trigger the failure of other nodes. Thus, the network eventually stabilize at the state of *b* sub-figure. Therefore, When $(8.67-6)/6 < \beta$, we can get that the values of G and S_{attack} are 12 and 0, respectively. In Fig. 5, we graphically give the correlation between two measures (G and S_{attack}) and the parameter β after removing a node in Fig. 4. Similar with some curves in Fig. 3, we also see that two curves show the obvious and wide fluctuation, which means that there exist the phenomena of the ability paradox in Fig. 4. By the analysis of Fig. 4, we speculate that this ability paradox is mainly originated from that the resurrections of some nodes lead to a sharp increase of the load on other nodes, and further trigger the failures of these nodes due to not handle the extra load.

A fundamental question is, what type of the local network structure can lead to the phenomenon of the ability paradox? By analysis of the Figs 3 and 4, we speculate that the ring structure after removing a node may trigger this unusual phenomenon. To this end, we construct a simple network with the ring structure after removing a node. (*a*) We first calculate the initial load on every node in the case of $\alpha = 0$ and remove the node (node 12) with the highest load (46.17). (*b*) We recalculate the load on every

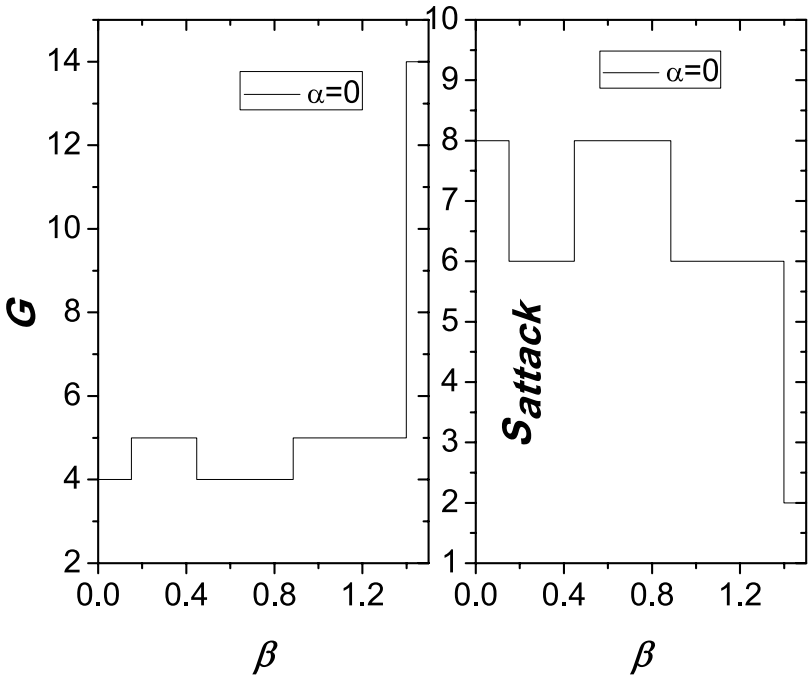

Figure 7. Correlation between two measures (G and S_{attack}) and the parameter β after removing the node with the highest load in Fig. 6.

remaining node, of which red arrow up represents that the load on a node increases, and black arrow down represent that the load on a node decreases, compared with the initial state in *a* sub-figure. (*c*) When $0 < \beta \leq (14 - 12.17)/12.17$, nodes 2, 3, 4, 6, 7, 8, 15, and 16 fail. We obtain that G and S_{attack} are 4 and 8, respectively. (*d*) When $(14 - 12.17)/12.17 < \beta \leq (14 - 9.67)/9.67$, nodes 2 and 4 resurrect. Therefore, we get that the values of G and S_{attack} are 5 and 6, respectively. (*e*) When $(14 - 9.67)/9.67 < \beta \leq (22 - 11.67)/11.67$, the resurrection of node 3 leads to a sharp increase of the load on nodes 2, 3, and 4. (*f*) Because nodes 2, 3, and 4 can not handle the extra load on them, they fail. Thus, we can get that the values of G and S_{attack} are 4 and 8, respectively. (*g*) When $(22 - 11.67)/11.67 < \beta \leq (22 - 9.17)/9.17$, nodes 6 and 8 resurrect. And the load on nodes 1, 2, 3, 4, and 5 sharply increases. (*h*) When cascading failures stop, we get that the values of G and S_{attack} are 5 and 6, respectively. When $(22 - 9.17)/9.17 < \beta$, the removal of node 12 does not trigger the failure of other nodes. Thus, the network eventually stabilize at the state of *b* sub-figure. Therefore, we can get that the values of G and S_{attack} are 14 and 2, respectively. Similarly, in Fig. 7, we graphically give the correlation between two measures (G and S_{attack}) and the parameter β after removing a node in Fig. 6. We clearly see that two curves show the obvious and wide fluctuation. By the analysis of Figs 3,4 and 7, we think that the phenomenon of the ability paradox is common in the network with the ring structure after removing a node, because in this type of network, some resurrection nodes due to the characteristics of the shortest paths easily lead to a sharp increase of the load on other nodes, and further trigger the failures of more nodes, while these nodes maintain their normal and efficient functioning in the case of their lower capacities.

Starting from the coupled-ring network, we further analyze the universality of this phenomenon. In Fig. 8(a–h), we explore cascading failures in four types of networks, as triggered by the removal of the node with the highest load. We construct a ring-coupled network (RCN) with 1000 nodes (Fig. 8(a,b)), of which each node is connected with its 4 neighbors. For each link, there is then a rewiring probability p. Each curve corresponds to a realization of the network. Firstly, in Fig. 8(a,b), we investigate the effects of the parameters α and β on the robustness of a ring-coupled network ($p = 0$). From the values of G and S_{attack}, we can observe that, the bigger the value of α, the stronger the robustness of RCN. with the increase of the value of β, we clearly see the ability paradox of cascading model at many points, for example, when $\beta = 0$, $\beta = 0.04$, $\beta = 0.12$, $\beta = 0.17$, and $\beta = 0.22$ correspond to $\alpha = 0$, $\alpha = 0.5$, $\alpha = 1.0$, $\alpha = 1.5$, and $\alpha = 2.0$, respectively. In Fig. 8(c,d), different from Fig. 2(c,d), we perform an experiment and obviously observe the interesting phenomenon of the ability paradox of cascading model, e.g., the abnormal curves at the data point $\beta = 0.16$ for five different values of α. Similarly, in Fig. 8(e,f), as the value of β increases, five curves fluctuate more frequently. While in Fig. 8(g,h), only when $\alpha = 0$, $\alpha = 0.5$, and $\alpha = 1$, there is the phenomenon of the fluctuation in three curves. This ability paradox of

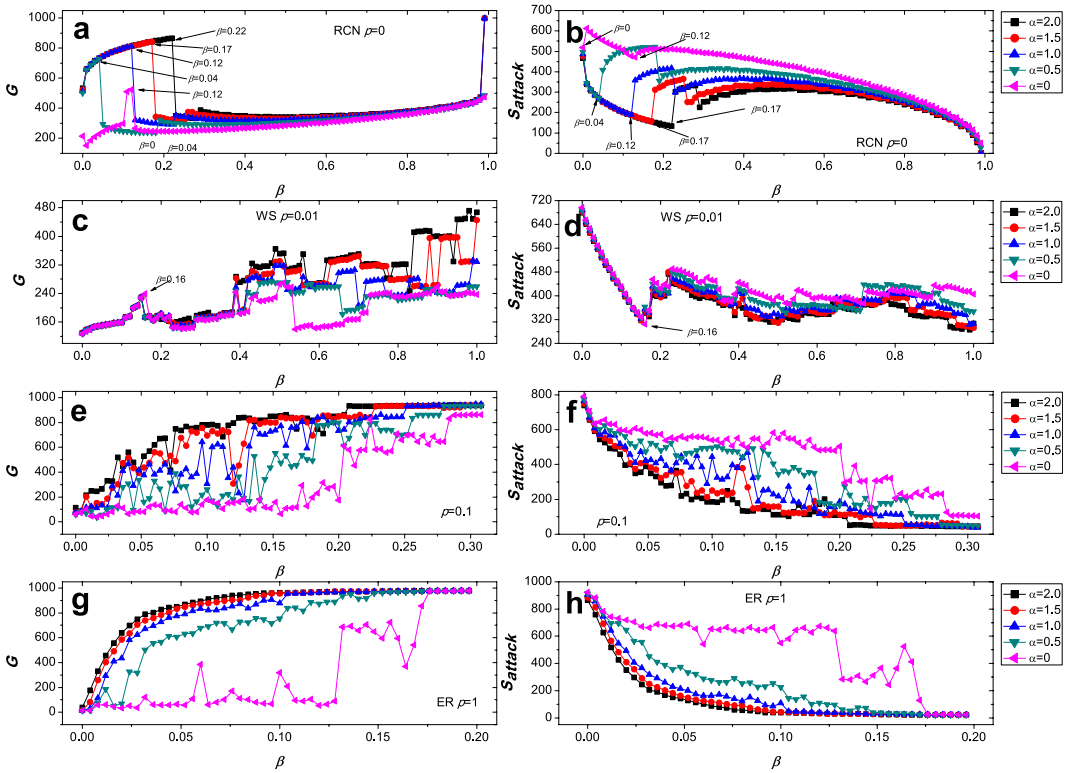

Figure 8. Cascading failures in four types of networks, initially constructed by a ring-coupled network (RCN) with 1000 nodes.

the cascading propagation might shed some new light on the analysis and control of cascading failures in real-world networks.

Conclusion

In summary, we introduce a new method to assign the initial load on each node in a network and proposed a cascading model. By investigating the cascades of overload failures triggered by attacks on or failures of highly loaded nodes, we focus on two fundamental and practically important questions: in the same network, how the weight parameter on a node affects the robustness of a network against cascading failures and, under the disturbance of the global shortest paths, whether the enhanced capability on each node in a network must improve the robustness of the network against cascading failures. In some man-made networks and infrastructure networks, we investigate the cascading propagation induced by attacks on a single node with the highest load by two measures of the largest connected component and the number of the failed nodes. We have shown that the size of the cascade can be reduced by increasing the value of the weight parameter on the node in those networks. Specially, in two networks (BA scale-free networks and the US airport) induced by the network structure, the bigger the value of the weight parameter on a node, the stronger the robustness of these networks, however, in some networks (networks generated by a coupled-ring network and two power grids) induced by the network structure, we observe an interesting phenomenon about the ability paradox of our model, i.e., investing more protecting resources to protect the network may not be able to improve the robustness of the network against cascading failures. By carefully analyzing this phenomenon and the cascading dynamics of our model, we give an explanation that the topological structure of the ring with many nodes due to some resurrection nodes may lead to the invalid investment strategy. These results should be useful in furthering studies in the analysis and control of cascade failures in real-world networks.

References

1. R. Albert, H. Jeong & A.-L. Barabási. Attack and error tolerance in complex networks. Nature **406,** 378–382 (2000).
2. L. K. Gallos, C. M. Song & H. A. Makse. A review of fractality and self-similarity in complex networks *Physica A* **386,** 686–691 (2007).
3. P. Holme, B. J. Kim, C. N. Yoon & S. K. Han. Attack vulnerability of complex networks. *Phys. Rev. E* **65,** 056109 (2002).
4. J. M. Carlson & J. Doyle. Highly optimized tolerance: robustness and design in complex systems. *Phys. Rev. Lett.* **84,** 2529–2532 (2000).
5. D. S. Callaway, M. E. J. Newman, S. H. Strogatz & D. J. Watts. Network Robustness and Fragility: Percolation on Random Graphs. *Phys. Rev. Lett.* **85,** 5468–5471 (2000).

6. R. Cohen, K. Erez, D. ben-Avraham & S. Havlin. Resilience of the Internet to Random Breakdowns. *Phys. Rev. Lett.* **85,** 4626–4628 (2000).
7. P. Holme, B. J. Kim, C. N. Yoon & S. K. Han. Attack vulnerability of complex networks. *Phys. Rev. E* **65,** 056109 (2002).
8. C. Liu, W. B. Du & W. X. Wang. Particle swarm optimization with scale-free interactions. *Plos One* **9,** e97822 (2014).
9. W. B. Du, Z. X. Wu & K. Q. Cai. Effective usage of shortest paths promotes transportation efficiency on scale-free networks. *Physica* A392, 3505–3512 (2014).
10. M. Perc. Evolution of cooperation on scale-free networks subject to error and attack. *New J. Phys.* **11,** 033027 (2009).
11. T. Zhou & B. H. Wang. Catastrophes in Scale-Free Networks. *Chin. Phys. Lett.* **22,** 1072–1075 (2005).
12. J. Glanz & R. Perez-Pena. 90 Seconds That Left Tens of Millions of People in the Dark. *New York Times*, August **26**, 2003.
13. M. L. Sachtjen, B. A. Carreras & V. E. Lynch. Disturbances in a power transmission system. *Phys. Rev. E* **61,** 4877–4882 (2000).
14. R. Pastor-Satorras, A. Vázquez & A. Vespignani. Dynamical and correlation properties of the Internet. *Phys. Rev. Lett.* **87,** 258701 (2001).
15. K. I. Goh, B. Hahng & D. Kim. Fluctuation-driven dynamics of the Internet topology. *Phys. Rev. Lett.* **88,** 108701 (2002).
16. X. Q. Huang, I. Vodenska, S. Havlin & H. E. Stanley. Cascading failures in bi-partite graphs: model for systemic risk propagation. *Sci. Rep.* **3,** 1219 (2013).
17. D. Q. Li, Y. N. Jiang, R. Kang & S. Havlin. Spatial correlation analysis of cascading failures: congestions and blackouts. *Sci. Rep.* **4,** 538.
18. B. Mirzasoleiman, M. Babaei, M. Jalili & M. Safari. Cascaded failures in weighted networks. *Phys. Rev. E* **84,** 046114 (2011).
19. Z. X. Wu, G. Peng, W. X. Wang, S. Chan & E. E. M. Wong. Cascading failure spreading on weighted heterogeneous networks. *J. Stat. Mech.* **5,** P05013, (2008).
20. W. X. Wang & G. R. Chen. Universal robustness characteristic of weighted networks against cascading failure. *Phys. Rev. E* **77,** 026101 (2008).
21. X. F. Wang & J. Xu. Cascading failures in coupled map lattices. *Phys. Rev. E* **70,** 056113 (2004).
22. W. X. Wang, Y. C. Lai & A. Dieter. Cascading failures and the emergence of cooperation in evolutionary-game based models of social and economical networks. *Chaos.* **21,** 033112 (2011).
23. Z. J. Bao, Y. J. Cao, L. J. Ding, Z. X. Han & G. Z. Wang. Dynamics of load entropy during cascading failure propagation in scale-free networks. *Phys. Lett. A* **372,** 5778 (2008).
24. J. W. Wang, C. Zhang, Y. Huang & C. Xin. Attack robustness of cascading model with node weight. *Nonlinear Dyn*. **78,** 37–48 (2014).
25. A. E. Motter. Cascade Control and Defense in Complex Networks. *Phys. Rev. Lett.* **93** (2004) 098701.
26. A. Ash & D. Newth. Optimizing complex networks for resilience against cascading failure. *Physica A* **380,** 673–683 (2007).
27. B. Wang & B. J. Kim. A high-robustness and low-cost model for cascading failures. *Europhys. Lett.* **78,** 48001 (2007).
28. I. Simonsen, L. Buzna, K. Peters, S. Bornholdt & D. Helbing. Transient dynamics increasing network vulnerability to cascading failures. *Phys. Rev. Lett.* **100,** 218701 (2008).
29. J. W. Wang. Mitigation of cascading failures on complex networks [J]. *Nonlinear Dyn* **70,** 1959–1967 (2012).
30. J. W. Wang. Mitigation strategies on scale-free networks against cascading failures. *Physica A* **392,** 2257–2264 (2013).
31. J. W. Wang. Optimized scale-free networks against cascading failures. *Int. J. Mod. Phys. C* **23,** 1250075 (2012).
32. X. B. Cao, C. Hong, W. B. Do & J. Zhang. Improving the network robustness against cascading failures by adding links. *Chao. Soliton. Fract* **57,** 35–40 (2013).
33. L. Buzna, K. Peters, H. Ammoser, C. Kühnert & D. Helbing. Efficient response to cascading disaster spreading. *Phys. Rev. E* **75,** 056107 (2007).
34. S. Pahwa, M. Youssef, P. Schumm, C. Scoglio & N. Schulz. Optimal intentional islanding to enhance the robustness of power grid networks. *Physica A* **392,** 3741–3754 (2013).
35. R. Yang, W. X. Wang, Y. C. Lai & G. R. Chen. Optimal weighting scheme for suppressing cascades and traffic congestion in complex networks. *Phys. Rev. E* **79,** 026112 (2009).
36. X. B. Cao, C. Hong, W. B. Du & J. Zhang. Improving the network robustness against cascading failures by adding links. *Chaos Soliton Fract* **57,** 35C40 (2013)
37. A. A. Moreira, J. S. Andrade Jr, H. J. Herrmann & J. O. Indekeu. How to Make a Fragile Network Robust and Vice Versa. *Phys. Rev. Lett.* **102,** 018701 (2009).
38. S. D. Li, L. X. Li, Y. X. Yang & Q. Luo. Revealing the process of edge-based-attack cascading failures. *Nonlinear Dyn* **69,** 837–845 (2012).
39. L. Zhao, K. Park & Y.C. Lai. Attack vulnerability of scale-free networks due to cascading breakdown. *Phys. Rev. E* **70,** 035101(R) (2004).
40. L. Zhao, K. Park, Y.C. Lai & N. Ye. Tolerance of scale-free networks against attack-induced cascades. *Phys. Rev. E* **72,** 025104 (2005).
41. A. Vespignani. The fragility of interdependency. *Nature* **464,** 984–985 (2010).
42. S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley & S. Havlin. Catastrophic cascade of failures in interdependent networks. *Nature* **464,** 1025–1028 (2010).
43. S. D. S. Reis, Y. Q. Hu, A. Babino, J. S. Andrade, S. Canals, M. Sigman & H. A. Makse. Avoiding catastrophic failure in correlated networks of networks *Nat. Phys.* **10,** 762–767 (2014).
44. D. Zhou, H. E. Stanley, G. D. Agostino & A. Scala. Assortativity decreases the robustness of interdependent networks. *Phys. Rev. E* **86,** 066103 (2012).
45. R. Parshani, S.V. Buldyrev & S. Havlin. Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition. *Phys. Rev. Lett.* **105,** 048701 (2010).
46. C. D. Brummitt, R. M. Dsouza & E. A. Leicht. Suppressing cascades of load in interdependent networks. *Proc. Natl. Acad. Sci. USA* **109,** E680 (2012).
47. J. Gao, S. V. Buldyrev, S. Havlin & H. E. Stanley. Robustness of a network of networks. *Phys. Rev. Lett.* **107,** 195701 (2011).
48. S. Pei, L. Muchnik, J. S. Andrade, Z. M. Zheng & H. A. Makse. Searching for superspreaders of information in real-world social media. *Sci. Rep*. **4,** 5547 (2014).
49. M. Schäfer, J. Scholz & M. Greiner. Proactive Robustness Control of Heterogeneously Loaded Networks. *Phys. Rev. Lett.* **96,** 108701 (2006).
50. J. W. Wang, C. Jiang & J. F. Qian. Robustness of interdependent networks with different link patterns against cascading failures. *Physica A* **393,** 535–541 (2014).
51. W. Li, A. Bashan, S. V. Buldyrev, H. E. Stanley & S. Havlin. Cascading Failures in Interdependent Lattice Networks: The Critical Role of the Length of Dependency Links. *Phys. Rev. Lett.* **108,** 228702 (2012).
52. S. V. Buldyrev, N. W. Shere & G. A. Cwilich. Interdependent networks with identical degrees of mutually dependent nodes. *Phys. Rev. E* **83,** 016112 (2011).
53. Y. Q. Hu, B. Ksherim, R. Cohen & S. Havlin. Percolation in interdependent and interconnected networks: Abrupt change from second- to first-order transitions. *Phys. Rev. E* **84,** 066116 (2011).

54. S. Pahwa, C. Scoglio & A. Scala. Abruptness of cascade failures in power grids. *Sci. Rep*. **4,** 3694 (2014).
55. Z. Su, L. X. Li, H. P. Peng, J. Kurths, J. H. Xiao & Y. X. Yang. Robustness of interrelated traffic networks to cascading failures. *Sci. Rep.* **4,** 5413 (2014).
56. R. Pastor-Satorras, A. Vázquez & A. Vespignani. Dynamical and correlation properties of the Internet. *Phys. Rev. Lett.* **87,** 258701 (2001).
57. V. S. Ricard, R. C. Martí, C. M. Bernat & V. Sergi. Robustness of the European power grids under intentional attack. *Phys. Rev. E* **77,** 026102 (2008).
58. J. W. Wang & L. L. Rong. Cascade-based attack vulnerability on the U.S. power grid. *Safety Sci.* **47,** 1332–1336 (2009).
59. D.-O. Leonardo & M. V. Srivishnu. Cascading failures in complex infrastructure systems. *Struct. Safety* **31,** 157–167 (2009).
60. G. D. Zhang, Z. Li, B. Zhang & W. A. Halang. Understanding the cascading failures in Indian power grids with complex networks theory. *Physica A* **392,** 3273–3280 (2013).
61. R. Albert, I. Albert & G. L. Nakarado. Structural vulnerability of the North American power grid. *Phys. Rev. E* **69,** 025103 (2004).
62. J. W. Wang & L. L. Rong. Robustness of the western United States power grid under edge attack strategies due to cascading failures. *Safety Sci.* **49,** 807–812 (2011).
63. L. Chang & Z. G. Wu. Performance and reliability of electrical power grids under cascading failures. *Int. J. Elec. Power* **33,** 1410–1419 (2011)
64. A. E. Motter & Y. C. Lai. Cascade-based attacks on complex networks. *Phys. Rev. E* **66,** 065102(R) (2002).
65. P. Crucitti, V. Latora, M. Marchiori. Model for cascading failures in complex networks. *Phys. Rev. E* **69,** 045104 (2004).
66. A.-L. Barabási & R. Albert. Emergence of Scaling in Random Networks. *Science* **286,** 509–512 (1999).
67. D. J. Watts & S. H. Strogatz. Collective dynamics of 'small-world' networks. *Nature* **393,** 6684, 440–442 (1998).
68. V. Colizza, R. Pastor-Satorras & A. Vespignani. Reaction-diffusion processes and metapopulation models in heterogeneous networks. *Nat. Phys.* **3,** 276–282 (2007).

Aknowledgement

This work was supported by the National Natural Science Foundation of China under Grant No. 71101022, the Fundamental Research Funds for the Central Universities under Grant No. N140604005, and the Program for New Century Excellent Talents in University under Grant No. NCET-12-0100.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Wang, J. *et al.* Ability paradox of cascading model based on betweenness. *Sci. Rep.* **5**, 13939; doi: 10.1038/srep13939 (2015).