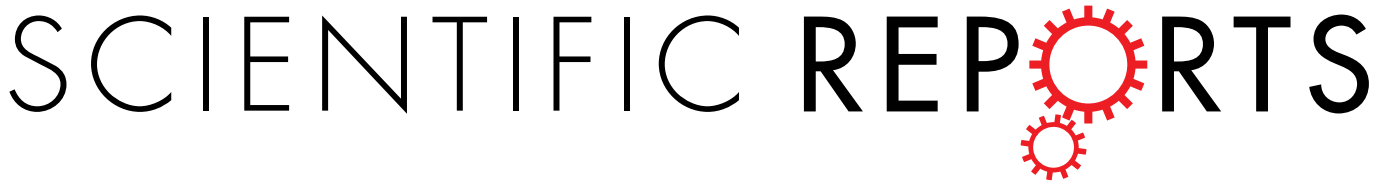

OPEN

Impact of Degree Heterogeneity on Attack Vulnerability of Interdependent Networks

Received: 30 January 2016
Accepted: 15 August 2016
Published: 09 September 2016

Shiwen Sun[1,2], Yafang Wu[1,2], Yilin Ma[1,2], Li Wang[1,2], Zhongke Gao[3] & Chengyi Xia[1,2]

The study of interdependent networks has become a new research focus in recent years. We focus on one fundamental property of interdependent networks: vulnerability. Previous studies mainly focused on the impact of topological properties upon interdependent networks under random attacks, the effect of degree heterogeneity on structural vulnerability of interdependent networks under intentional attacks, however, is still unexplored. In order to deeply understand the role of degree distribution and in particular degree heterogeneity, we construct an interdependent system model which consists of two networks whose extent of degree heterogeneity can be controlled simultaneously by a tuning parameter. Meanwhile, a new quantity, which can better measure the performance of interdependent networks after attack, is proposed. Numerical simulation results demonstrate that degree heterogeneity can significantly increase the vulnerability of both single and interdependent networks. Moreover, it is found that interdependent links between two networks make the entire system much more fragile to attacks. Enhancing coupling strength between networks can greatly increase the fragility of both networks against targeted attacks, which is most evident under the case of max-max assortative coupling. Current results can help to deepen the understanding of structural complexity of complex real-world systems.

Complex network is an important tool used to describe and analyze the structure and dynamical behaviors of complex systems[1–3]. Since real-world complex systems are becoming increasingly dependent on one another, the study of interdependent networks has become another new active topic in network science[4,5]. Modern critical infrastructures are representative examples of interdependent systems, such as water supply, power stations, fuel supply, transportation, communication, etc. For example, considering the interdependence between power grids and communication networks, power grids need communication networks to transmit control signals and communication networks need power grids to provide power supply. The investigation of interdependent networks has led to new discoveries that cannot be explained using a single-network framework[6–14].

We focus on one fundamental property of interdependent networks: attack vulnerability. Albert *et al.*[15] raised the study of complex networks under attacks, they found the "*robust yet fragile*" generic property of scale-free networks: scale-free networks display an unexpected degree of robustness to random failures, however, these networks are extremely vulnerable to intentional attacks. Their research has triggered numerous theoretical and experimental works in this topic[16–25]. However, most previous studies mainly focused on single, isolated networks. Based on percolation theory, recently, Buldyrev *et al.* proposed a general framework to investigate the attack resilience of a system composed of two networks whose nodes are mutually dependent[26,27]. In this model, attack on nodes is simulated by random node removal from one network. Due to the existence of interdependent links, an initial failure of only a small fraction of nodes in one network can lead to an iterative cascade of failures that cause both networks to become fragmented. Moreover, interdependent systems can react to random failures in a manner that is totally different from single networks, i.e., an interdependent system can exhibit a first-order (discontinuous) phase transition instead of the second-order (continuous) phase transition which is typical for single networks[16,18].

[1]Tianjin Key Laboratory of Intelligence Computing and Novel Software Technology, Tianjin University of Technology, Tianjin, 300384, China. [2]Key Laboratory of Computer Vision and System (Tianjin University of Technology), Ministry of Education, Tianjin, 300384, China. [3]School of Electrical Engineering and Automation, Tianjin University, Tianjin, 300072, China. Correspondence and requests for materials should be addressed to S.S. (email: sunsw80@126.com) or C.X. (email: xialooking@163.com) or Z.G. (email: zhongkegao@tju.edu.cn)

In reality, the topological features should be taken into account for a complete description of the networks. Thus it is of great importance to explore the effects of the structural properties of networks on attack vulnerability of interdependent systems. Several recent papers focused on the influence of clustering[28–31]. Huang *et al.*[28] established a fully interdependent system of two networks with tunable clustering and found that clustering significantly increases the vulnerability. The impact of clustering on partially interdependent systems is also investigated[29] and the percolation behaviors of clustered networks with partial support-dependence relations are analyzed based on the percolation theory[30]. Clustering coefficient is found to have a significant impact on robustness of the system particularly with strong coupling strength, however weak coupling strength can induce little influence[31]. The degree distribution is one of the most fundamental and important properties of complex networks. For example, single network with a broader degree distribution can be more robust to random failures, however, for interdependent networks, the broader the distribution is, the more vulnerable the networks become to random failures[32,33]. Zhou *et al.*[34] found that the internal node correlations in each of the two interdependent networks significantly changes the critical density of failures that triggers the total disruption of the two-network system. In particular, the assortativity, i.e., the likelihood of nodes with similar degree to be connected within a single network, decreases the robustness of the entire system[35,36]. Additionally, Yuan *et al.*[37] study the effect of the breadth of the degree distributions on network robustness by comparing two different attacking strategies: localized attack and random attack.

In this study, we continually focus on the effect of degree distribution on attack vulnerability of single and interdependent networks. An typical evolving network model, named extended Barabási-Albert model (*eBA*)[38], is employed as network component of an interdependent system. *eBA* model is one of the variants of *BA* model[39] with a parameter $p (p \in [0, 1])$. By varying p, the heterogeneity of degree distributions of corresponding networks can be controlled. Considering that in real-world coupled systems not every node in one network depends on another network, thus a parameter named coupling strength q, defined here as the fraction of network nodes that are dependent on the other network, is introduced in the interdependent network model. Furthermore, other than random interdependency between networks, coupling preference is also taken into consideration on the performance of interdependent systems. Additionally, previous studies mainly focused on the impact of degree distribution on interdependent networks under random attacks, while we extend the study to the case of the more realistic attacking strategy, targeted attack on high-degree nodes.

Results

Vulnerability of single networks. Firstly, numerical simulations are performed to investigate the effect of degree heterogeneity on single complex networks. The responses of single *eBA* networks under targeted node removal are exhibited in Fig. 1. All the initial networks ($N = 10{,}000$ and $\langle k \rangle = 6$) are constructed by *eBA* model with $m = 3$. Each point is averaged over 10 independent realizations.

The relative size S of the giant connected component is usually used to probe the functional integrity of networks after attack. S is defined to be $S = N'/N$ where N' and N denotes the number of nodes in the largest connected component and that in the initial network, respectively. Obviously, the larger S is, the more nodes remain in the largest component, which indicates the system is more robust under attacks. Figure 1(a) shows the relative size S of the giant connected components of single *eBA* networks with different parameter p after a fraction f of nodes removed from the networks. S decreases from $S = 1$ as f increases. At critical point $f = f_c$, $S \approx 0$, indicating that the network breaks into tiny isolated clusters. It can be observed from Fig. 1(a) that *eBA* networks with higher values of p are more vulnerable resisting targeted attack on high-degree nodes.

Also, considering the efficiency loss caused by the removal of nodes and links, efficiency loss *el* of the residual network after attack monotonically increases with f (Fig. 1(b)). Different changes of *el* with f can demonstrate the transitional behaviors of the vulnerability of *eBA* networks with different p against attacks. As observing from Fig. 1(b), removing the same percent of high-degree nodes from the networks will bring more efficiency loss on networks with higher values of p. The results demonstrate that targeted attack can bring more damage to the networks which are more heterogenous in connectivity.

In order to describe the fragment process of networks after attack in more detail, *Ns*, the number of isolated components breaking off from the main body, and $\langle s \rangle$, the average size of these isolated components, can be examined. For *eBA* networks with different parameter p, Fig. 1(c) shows the the changes of *Ns* as functions of f. As more nodes are removed from the networks, more and more nodes breaking off from the giant connected components, thus, *Ns* increases with f. It can be observed that with the same value of f, *Ns* of networks with higher values of p are larger. For example, when $f = 0.25$, $Ns \approx 250$ for *eBA* network with $p = 0.0$, while *Ns* increases with p, and for network with $p = 1.0$, *Ns* is increased to $Ns \approx 2600$.

Meanwhile, as shown in Fig. 1(d), there exits a critical threshold value f_c at which $\langle s \rangle$ reaches its maximum value and the phase transition occurs according to the percolation theory[2,16–18]. During network fragmentation process, for small f, single nodes break off from the main body, so $\langle s \rangle \approx 1$. With the increase of f, the size of the fragments that fall off the main body increases, thus $\langle s \rangle$ increases. At $f = f_c$, the giant component breaks into small pieces quickly $S \approx 0$, and the size of fragments $\langle s \rangle$ peaks. As the continue removal of nodes $f > f_c$, isolated components breaks apart continually resulting to a decreasing $\langle s \rangle$. As shown in Fig. 1(d), as p is increased, f_c becomes smaller, which indicates that corresponding network become more fragile. For example, when $p = 0.0$, $f_c \approx 0.44$, however, f_c is observed to be about 0.26 when $p = 1.0$. Moreover, $\langle s \rangle$ increases more drastically with increasing p.

To conclude, the numerical results in Fig. 1 show that, under intentional attacks, the fragility of the *eBA* networks also show a transition between that of the scale-free network ($p = 1.0$) and of the exponential network ($p = 0.0$). Moreover, heterogenous networks, that is, networks with higher values of p, are found to be more fragile resisting targeted attack on high-degree nodes.

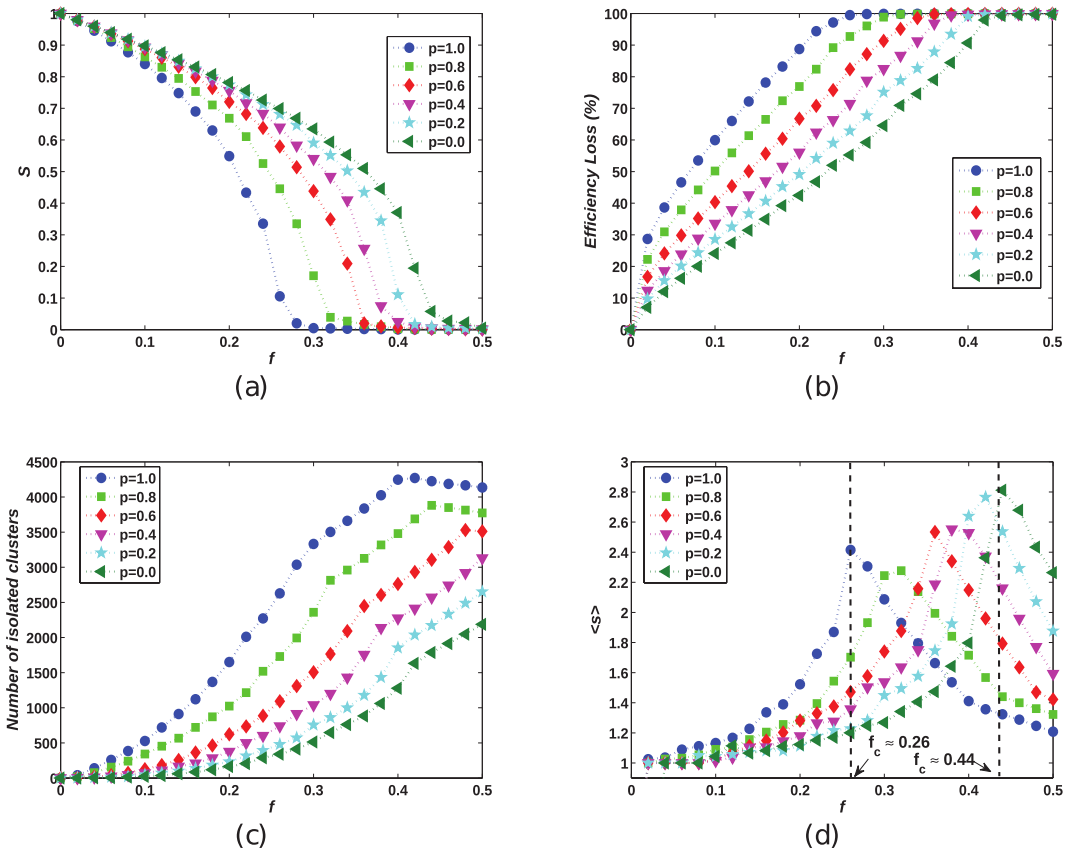

Figure 1. Vulnerability of single *eba* networks with different *p* after a fraction *f* of nodes removed from the networks. (**a**) The relative size *S* of the giant connected component; (**b**) Efficiency loss (*el*); (**c**) Number of isolated connected components (*Ns*); (**d**) Average size of isolated connected components ($\langle s\rangle$). All the networks are with $N = 10000$ and $\langle k\rangle = 6$. Each point is averaged over 10 independent realizations.

Vulnerability of fully interdependent networks. Next, we explore the influence of both degree heterogeneity and interdependency on the fully interdependent *eBA* networks, which corresponds to the case of coupling strength $q = 1.0$. According to the interdependent system model mentioned above, an interdependent system are constructed firstly in the numerical simulation. Two different networks, network *A* and network *B*, are separately constructed according to *eBA* model with parameters $m = 3$ and $N = 2000$. Meanwhile, the degree heterogeneity of each network can be controlled by parameter *p*, as *p* is changed from 0 to 1, the extent of degree heterogeneity of each network is enhanced greatly.

Additionally, different types of interdependency links are taken into account in the construction of interdependent networks. As for random coupling, after the construction of two networks *A* and *B*, randomly choose a node in network *A* and a node in network *B* and set up an interdependent link between them, repeat this process until *N* interdependent links are added. Meanwhile, two kinds of coupling preference are also investigated. The first one, which is referred to as assortative coupling, means sorting nodes in network *A* and *B* in the descending order of node degree and connecting the nodes in *A* and *B* one by one. The other one, referred to as *disassortative coupling*, means sorting nodes in network *A*(*B*) in the descending(ascending) order of node degree and connecting them one by one.

Figure 2 show the responses of fully interdependent *eBA* networks under targeted attacks on high-degree nodes with random (Fig. 2(a)), assortative (Fig. 2(b)) and disassortative (Fig. 2(c)) coupling, respectively. Considering the impact of degree heterogeneity of interdependent networks, as shown in Fig. 2, with all the three kinds of coupling, efficiency loss *el* of networks increases more rapidly with higher value of *p*, which demonstrates that corresponding networks are more vulnerable to attacks in targeted ways. Note that, this behavior is consistent with that of isolated *eBA* networks (Fig. 1).

Previous study has found that due to the existence of dependency links, a system composed of two interdependent networks is much more fragile than each network in isolation[26,27]. For isolated *eBA* networks, curves in Fig. 1(b) show the efficiency losses with increasing *f*. At the critical values f_c the communication efficiency is totally lost (i.e., $el \approx 100\%$) and the whole network collapses. It can be clearly observed that as parameter *p* is changed from 0 to 1, $fc \in [0.26, 0.44]$. However, in Fig. 2(a), the responses of interdependent networks are different, that is, $f_c \approx 0.32$ when $p = 0.0$ and $f_c \approx 0.17$ when $p = 1.0$. The decrease of f_c indicates that dependency links between networks make both networks become more vulnerable with respect to attacks on nodes.

Coupling preference can also greatly affect the properties and behaviours of complex interdependent networks. Rather than random coupling (Fig. 2(a)), attack vulnerabilities of networks with assortative and disassortative

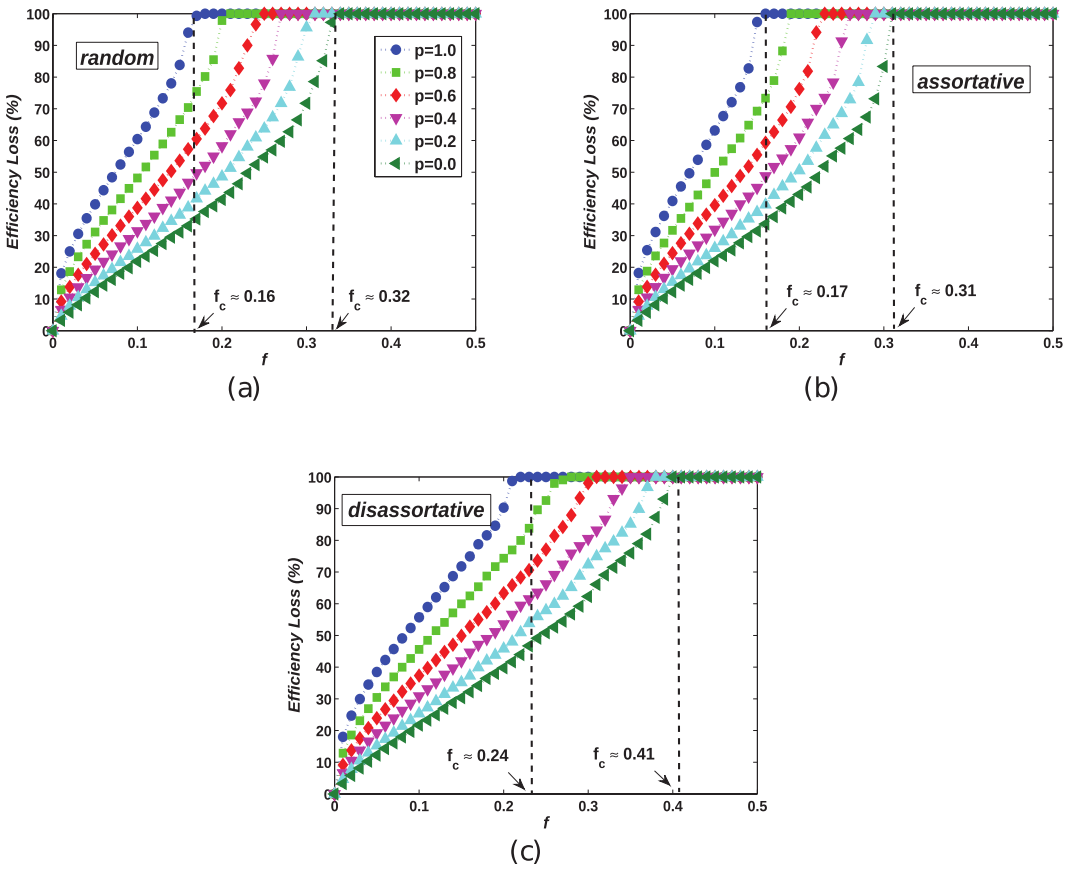

Figure 2. Vulnerability of interdependent *eba* networks with different *p* after a fraction *f* of nodes removed from the networks with coupling strength $q = 1.0$. Different coupling types are considered separately: (**a**) random coupling; (**b**) assortative coupling; (**c**) disassortative coupling. All the networks are with $N = 2000$ and $\langle k \rangle = 6$. Each point is averaged over 10 independent realizations. The legends in (**b**,**c**) are the same as those of (**a**).

coupling are presented in Fig. 2(b,c) respectively. Assortative coupling can bring more efficiency loss caused by the same number of removed nodes compared with disassortative coupling. For example, at $f = 0.1$, for networks with $p = 1.0$, the efficiency loss is 60% in Fig. 2(b), however, for the same network with disassortative coupling (Fig. 2(c)), at $f = 0.1$, the efficiency loss is deceased to 50%. Moreover, compared with disassortative coupling, the values of f_c are observed to be smaller than those of networks with the same parameters of m, N and p under assortative coupling. For example, when $p = 0.0$, $f_c \approx 0.32$ for assortative coupling (see Fig. 2(b)) but $f_c \approx 0.41$ under the case of disassortative coupling (see Fig. 2(c)). All the simulation results strongly demonstrate that assortative coupling makes interdependent networks more vulnerable compared with disassortative coupling.

Vulnerability of partially interdependent networks. As for partially interdependent networks, a parameter $q (0.0 \leq q \leq 1.0)$ is employed to control the coupling strength between two networks. Moreover, different coupling types are considered separately including random, *max-max*, *min-min*, *max-min* and *min-max* coupling.

The critical values f_c of removed nodes from the networks, at which the efficiency loss is almost 100%, is used as an important quantity to measure the vulnerability of corresponding systems. Obviously, the smaller the value of f_c is, the more vulnerable the network is, and *vice visa*.

In order to explore the influence of both degree heterogeneity and interdependency, numerical simulations are performed to examine the responses of partially interdependent networks. Figure 3 presents the values of f_c as functions of coupling strength q and parameter p of interdependent networks with different coupling types: random coupling (Fig. 3(a)), *max-max* coupling (Fig. 3(b)), *min-min* coupling (Fig. 3(c)), *max-min* coupling (Fig. 3(d)), *min-max* coupling (Fig. 3(e)). All the networks are with $N = 2000$ and $\langle k \rangle = 6$. Each point is averaged over 10 independent realizations.

From Fig. 3, when p is fixed, that is, the two interdependent networks are with the same extent of degree heterogeneity, with the increase of coupling strength q, f_c is observed to decrease. The most evident decrease of f_c can be observed under the case of *max-max* coupling (Fig. 3(b)). Since a smaller value of f_c indicates that corresponding network become more vulnerable against node attacks, the results demonstrate that strong interdependency between networks induces more vulnerability. Thus, due to the existence of dependency links, a system composed of two interdependent networks is much more fragile than each network in isolation no matter what kind of coupling preference is.

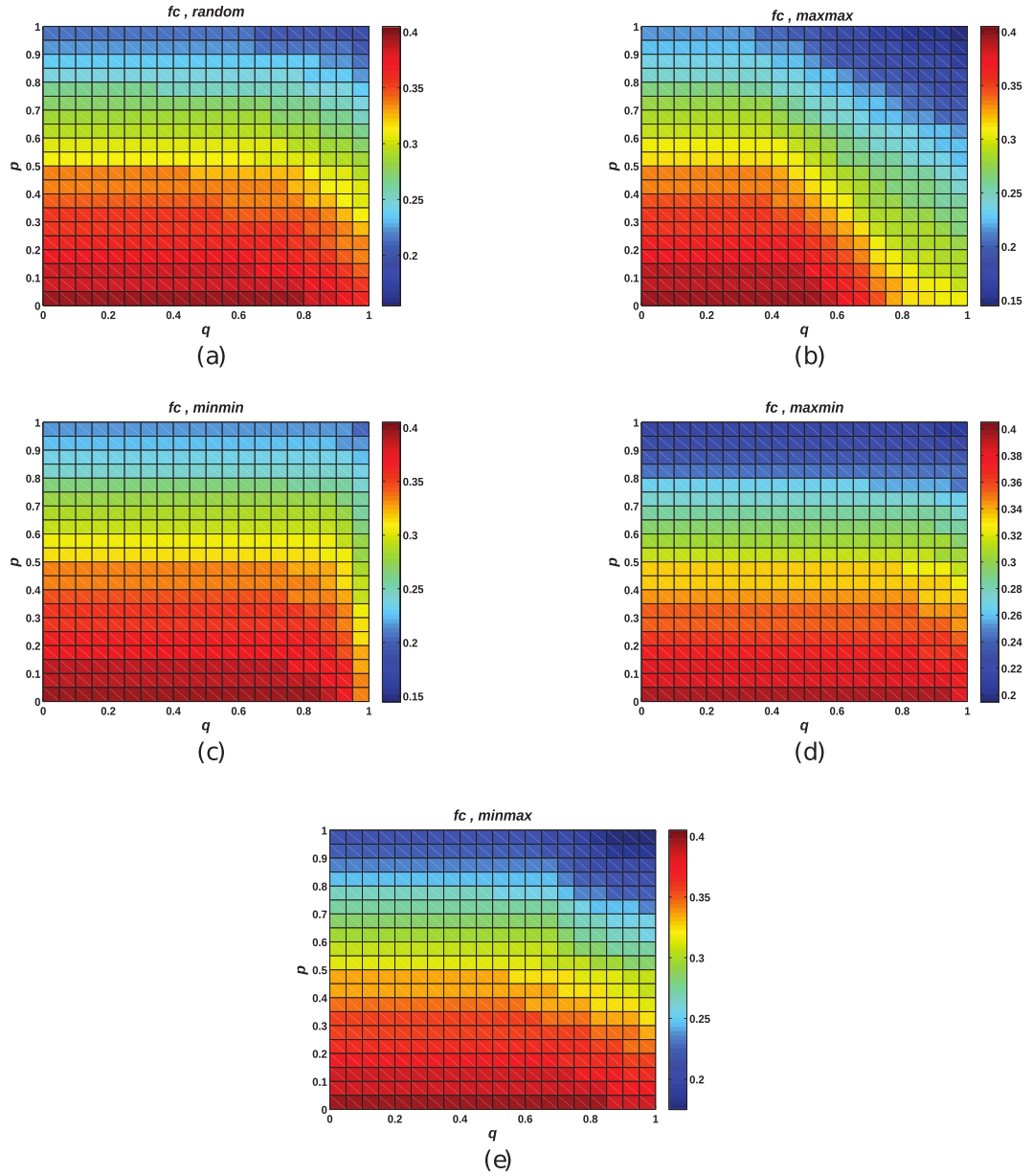

Figure 3. The critical values f_c as a function of the coupling strength q and model parameter p. Different coupling types are considered separately: (**a**) random coupling; (**b**) *max-max* coupling; (**c**) *min-min* coupling; (**d**) *max-min* coupling; (**e**) *min-max* coupling. All the networks are with $N = 2000$ and $\langle k \rangle = 6$. Each point is averaged over 10 independent realizations.

Additionally, with fixed q, f_c is observed to decrease as p is increased, thus confirming that for partially interdependent networks, when networks become more heterogenous in connectivity, they are also more vulnerable to resist node attacks. The vulnerability is basically rooted in the network's connectivity. For heterogenous networks ($p = 1.0$), the connectivity is ensured by a few high-degree nodes, whose removal drastically alters the network's topology and decrease the ability of the remaining nodes to communicate with each other. While in homogeneous network ($p = 0.0$), most nodes have approximately the same number of connections and contribute equally to the integrity of the topology. Due to the absence of nodes with large connections ($k \gg \langle k \rangle$), targeted removal of hub nodes does not affect the structure of remaining nodes as drastically as in heterogenous networks.

The most vulnerable case occurs under the case of $p = 1.0$, $q = 1.0$ with *max-max* coupling (see Fig. 3(b)). When targeted attack is initiated in one network, the *max-max* coupling makes node failures quickly propagate between high-degree nodes of each networks, thus leading to rapid collapse of both networks. Nevertheless, the interdependent system with two networks coupled in a *min-min* mode are more robust than *max-max* and *min-max* coupling in particular for strong coupling strength q (see Fig. 3(e)). Since with *min-min* coupling low-degree nodes in network A and B are connected to each other, the failure of low-degree nodes in network

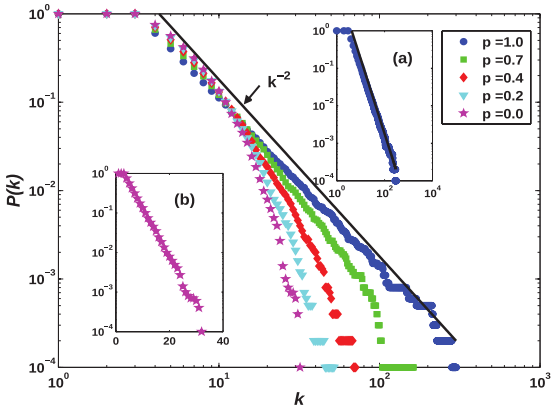

Figure 4. Cumulative degree distribution $P(k)$ of *eBA* evolving networks with $N = 10{,}000$ and $\langle k\rangle = 4$ for different parameter p. In panel (a) (log-log scale), $P(k)$ follows a power-law form, which corresponds to one special case of *eBA* networks ($p = 1.0$). Panel (b) (in semi-log scale) presents the other special case of *eBA* networks ($p = 0.0$), whose degree distribution follows a exponential form. A higher value of p makes corresponding network more heterogeneous in connectivity.

A can only affect low-degree nodes in network *B*, having little effects on high-degree nodes in *B*. While, in *max-max* and *min-max* coupling, the failures of low-degree nodes in network *A* can lead to the failures of all the high-degree nodes in *B*, thus, making cascading failures propagate more quickly between two networks.

Discussion

The attack vulnerability of networks can be greatly influenced by their degree distributions and in particular by degree heterogeneity. In order to deeply understand the role of degree heterogeneity upon interdependent networks, An typical evolving network model, named extended Barabási-Albert model, is employed as network component of an interdependent system. *eBA* model can generate networks displaying a transition from exponential to power-law form with respect to degree distributions. Also a parameter named coupling strength q, defined as the fraction of network nodes that are dependent on the other network, is introduced in the interdependent network model. Furthermore, other than random interdependency between networks, coupling preference is also taken into consideration on the performance of interdependent systems. In order to better describe the responses of interdependent networks after node removal, a new quantity concerning the communication efficiency is introduced.

Numerical simulation results demonstrate that degree heterogeneity can significantly increase the vulnerability of both single and interdependent networks. Networks with heterogenous degree distribution are more vulnerable against targeted attacks on high-degree nodes, and this result also holds for interdependent networks. Moreover, it is found that interdependent links between two networks make the entire system much more fragile to attacks. Enhancing coupling strength between networks can greatly increase the fragility of both networks against targeted attacks, which is most evident under the case of max-max assortative coupling. These results can improve the deep understanding of structural complexity of complex real-world systems, also give some insight to the guidance of designing resilient infrastructures.

Methods

Constructing Extended Barabási-Albert Networks. Network growth and preferential attachment(*PA*) are argued to the emergence of the power-law degree distribution (i.e., $p(k) \sim k^{-\gamma}$) in Barabási-Albert(*BA*) scale-free networks[39]. Extended BA model(*eBA*)[38] is one of the variants of *BA* model by introducing a parameter $p (p \in [0, 1])$. By varying p, the heterogeneity of degree distributions of corresponding networks can be controlled.

The iterative algorithm of *eBA* model is outlined as follows. Starting from m_0 fully connected nodes, at each step t, a new node is added to the network with $m (m \leq m_0)$ edges that link to m different nodes already existing in the network. The m links are attached in two different ways: i) with probability p, the *PA* rule is used, that is, the new node is connected to an existing node i according to the probability $\Pi_i = k_i/\sum_j k_j$; ii) with probability $(1 - p)$, the new node is connected to a randomly chosen node.

The cumulative degree distributions, defined as $P(k) = \sum_{k>k'}^{+\infty} p(k')$, of *eBA* networks are shown in Fig. 4. It can be observed that the probability p in *eBA* model has great effect on the network's degree distributions. Here, two special cases exist. If $p = 1.0$, the model reduces to the standard *BA* network with a degree distribution following a power-law form (see panel (a) in Fig. 4). On the other hand, if $p = 0.0$, the preferential attachment mechanism does not take effect and the model results in a network with a degree distribution following an exponential form: $p(k) \sim e^{-k/m}$ (see panel (b) in Fig. 4). In addition, noticeably, as p is changed from 0 to 1, corresponding networks display transitional behaviors from exponential to power-law form with respect to degree distributions.

In order to further study the effects of p on degree heterogeneity, two important indicators, σ_k^2 and k_{max} of the resultant networks are examined. k_{max} means the maximal value of the node degree in the whole network. σ_k^2 is

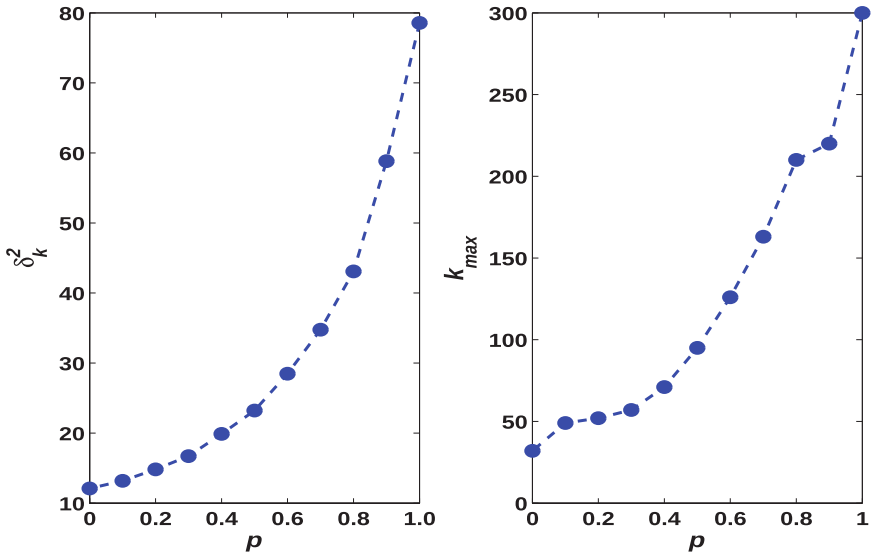

Figure 5. The dependencies of σ_k^2 and k_{max} on parameter p of *eBA* networks with $N = 10{,}000$ and $\langle k \rangle = 4$.

defined to be the variance of node degree sequence, i.e., $\sigma_k^2 = \langle k \rangle^2 - \langle k^2 \rangle$. Figure 5 shows the dependencies of σ_k^2 and k_{max} on p. For $0 \leq p \leq 1$, as p increases, σ_k^2 is observed to increase monotonously, implying the increase of degree heterogeneity (see Fig. 5(a)). Meanwhile, with increasing p, k_{max} also becomes larger (see Fig. 5(b)). The increase of k_{max} with increasing p indicates the emergence of hub nodes, which have much more connections than the others. These results verify that a higher value of p makes corresponding *eBA* network more heterogeneous in connectivity.

Establishing Interdependent Network System. Following the framework established by Buldyrev *et al.*[26], A partially interdependent system composed of two networks is proposed. Let network A and B be *eBA* networks with the same size $N_A = N_B = N$ and the same average node degree $\langle k_A \rangle = \langle k_B \rangle = \langle k \rangle$. Also, A and B are with the same parameter p, i.e. $p_A = p_B = p$. Apparently, as p is changed from 0 to 1, the extent of heterogeneity of degree distributions of each network is changed greatly, i.e. a higher p makes corresponding network become more heterogeneous concerning degree distribution. Note that only one-to-one and symmetric interdependency is considered, which means that node a_i in network A only depends on one node b_j in B and vice visa. For partially coupling, only a fraction q of nodes in network A and B depends on each other. $0 \leq q \leq 1$ and $q = 1$ corresponds to the case of fully coupling.

A simple example of an interdependent system consisting of two networks A and B is shown in Fig. 6(a). Nodes in network A are represented by blue circles ($\{a_i | 1 \leq i \leq 6\}$) and nodes in network B are represented by red squares ($\{b_j | 1 \leq j \leq 6\}$). The intra-links in each network are represented as solid lines and the interdependent links between networks are represented as dashed lines. Figure 6(b–e) illustrate the iterative process of a cascade of failures induced by an initial attack on a single node a_5 in network A. When a_5 fails, all the intra-links (a_3-a_5),(a_4-a_5) and (a_6-a_5) in network A fail (Fig. 6(b)). This disconnects nodes a_4 and a_6 from the largest connected component of network A and therefore a_4 and a_6 fail. Due to the interdependency between nodes a_4 and b_4, the failure of a_4 triggers the failures of b_4 and all its direct links (b_3-b_4) and (b_4-b_5) (Fig. 6(c)), which makes node b_3 disconnected from the largest connected component of network B, hence b_3 fails. The failure of b_3 leads to the failures of the interdependent link (a_3-b_3), node a_3 and two links (a_1-a_3), (a_2-a_3) (Fig. 6(d)). This procedure will not stop until no further node elimination occurs. The system eventually stabilises with the largest connected component (a_1, a_2) in network A and (b_1, b_2, b_5, b_6) in network B (Fig. 6(e)).

Furthermore, other than random interdependency between networks, coupling preference is also taken into consideration in our study:

- Random coupling. Randomly choose a node in network A and a node in network B and set up an interdependent link between them, Repeat this process until $N*q$ interdependent links are added.
- Assortative coupling. Two different kinds of assortative coupling, referred to as *max-max* and *min-min* coupling, respectively, are considered. Sort nodes in network A and B in the descending order of node degree, as for *max-max* coupling, connect the fraction q of nodes with the highest degree in A and the fraction q of nodes with the highest degree in B; while for *min-min* coupling, the fraction q of nodes with the lowest degree in A and the fraction q of nodes with the lowest degree in B are connected.
- Disassortative coupling. Also, Two different kinds of disassortative coupling, *max-min* (the fraction q of nodes with the highest degree in A connect the fraction q of nodes with the lowest degree in B) and *min-max* (the fraction q of nodes with the lowest degree in A connect the fraction q of nodes with the highest degree in B), are considered.

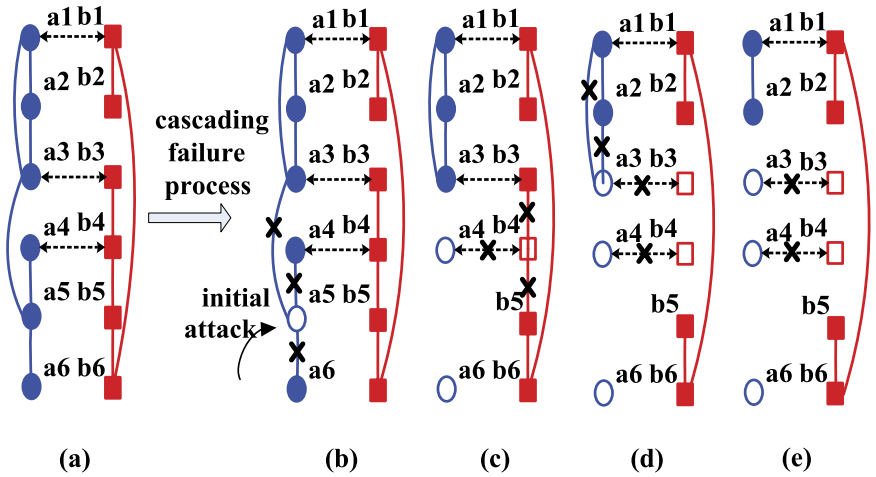

Figure 6. Illustration of an interdependent system composed of two networks and the cascading failure process caused by node removal from one network. The initial system is shown in (**a**). Nodes in network A are represented by blue circles ($\{a_i|1 \le i \le 6\}$) and nodes in network B are represented by red squares ($\{b_j|1 \le j \le 6\}$). The intra-links in each network are represented as solid lines and the interdependent links between networks are represented as dashed lines. (**b**–**e**) Illustrate the iterative process of a cascade of failures induced by an initial attack on a single node a_5 in network A.

A New Vulnerability Measure - *efficiency loss*(*el*). When nodes are gradually damaged due to random failures or targeted attacks, a network may be split into several unconnected components. Thus, the vulnerability of networks is mainly measured by the connectivity integrity of the networks. Several measures are commonly used including the relative size S of the giant connected component, the number of isolated connected components Ns, the average size $\langle s \rangle$ of connected components except the largest one, and the critical fraction f_c of nodes attacked at which the whole network collapses completely.

However, in realistic cases, these measures may overlooks situations in which the networks suffer from a big damage but they are not completely collapsing. Moreover, other than the study on the connectivity integrity, other properties of the residual nodes and links after attack should also be explored. Thus, in our study, a new quantity, aiming at measuring the communication efficiency of the residual network after attack, is introduced, which is used as an important vulnerability measure of interdependent networks.

Communication efficiency is one of the important quantities to measure how efficiently the information is exchanged over the whole network[21,40]. Suppose that information is exchanged between every pair of nodes and transmitted along the shortest path connecting them, communication efficiency ε_{ij} is assumed to be inversely proportional to the shortest distance: $\varepsilon_{ij} = 1/l_{ij}$, here, l_{ij} denotes the length of shortest path between nodes i and j. Thus, global communication efficiency ε of network G is defined as the average of ε_{ij} over all pair of nodes, i.e., $\varepsilon = \sum_{i \ne j} \varepsilon_{ij}/(N(N-1))$, where N is the total number of nodes in the network.

Once $\varepsilon(G)$ is defined as a measure of performance of network G, the damage caused by the removal of some components(node and/or edges) can be naturally evaluated by the a new measure, *efficiency loss*(*el*), which is defined as

$$el = \frac{\varepsilon(G_0) - \varepsilon(G_f)}{\varepsilon(G_0)}, \tag{1}$$

where $\varepsilon(G_0)$ is the efficiency of the initial network before any attack and $\varepsilon(G_f)$ is the final efficiency that is reached by the network due to the breakdown. Apparently, under the same level of damage, a larger value of *el* means that corresponding network is more vulnerable resisting attacks.

References

1. Albert, R. & Barabási, A. L. Statistical mechanics of complex networks. *Rev. Mod. Phys.* **74,** 47–97 (2002).
2. Newman, M. E. J. The structure and function of complex networks. *SIAM Rev.* **45(2),** 167–256 (2003).
3. Boccalettia, S., Latora, V., Moreno, Y., Chavez, M. & Hwang, D. U. Complex networks: structure and dynamics. *Phys. Rep.* **424,** 175–308 (2006).
4. Kivela, M. *et al.* Multilayer Networks. *J. of Comp. Net.* **2(3),** 203–271 (2014).
5. Boccaletti, S. *et al.* The structure and dynamics of multilayer networks. *Phys. Rep.* **544(1),** 1–122 (2014).
6. Wang, Z., Wang, L. & Perc, M. Degree mixing in multilayer networks impedes the evolution of cooperation, *Phys. Rev. E* **89,** 052813 (2014).
7. Wang, Z., Szolnoki, A. & Perc, M. Self-organization towards optimally interdependent networks by means of coevolution. *New J. of Phys.* **16,** 033041 (2014).
8. Jesus, G. G., Carlos, G. L., Luis, M. F. & Moreno, Y. Evolutionary dynamics on interdependent populations. *Phys. Rev. E* **86,** 056113 (2012).
9. Tan, F., Xia, Y. X., Zhang, W. & Jin, X. Cascading failure of loads in interconnected networks under intentional attack. *EPL* **102,** 28009 (2013).
10. Tan, F., Wu, J. J., Xia, Y. X. & Tse, C. K. Traffic congestion in interconnected complex networks, *Phys. Rev. E* **89,** 062813 (2014).

11. Tan, F., Xia, Y. X. & Wei, Z. Robust-yet-fragile nature of interdependent networks. *Phys. Rev. E* **91,** 052809 (2015).
12. Sanz, J., Xia, C. Y., Meloni, S. & Moreno, Y. Dynamics of interacting diseases. *Phys. Rev. X* **4(4),** 041005 (2014).
13. Meng, X. K., Xia, C. Y., Wang, L. & Sun, S. W. Spatial prisoner's dilemma games with increasing neighborhood size and individual diversity on two interdependent lattices. *Phys. Lett. A* **379,** 767–773 (2015).
14. Meng, X. K. *et al.* Interdependency enriches the spatial reciprocity in prisoner's dilemma game on weighted networks. *Physica A* **442,** 388–396 (2016).
15. Albert, R., Jeong, H. & Barabási, A. L. The Internet's Achilles' Heel: Error and attack tolerance of complex networks. *Nature* **406,** 378–382 (2000).
16. Cohen, R., Erez, K., ben-Avraham, D. & Havlin, S. Resilience of the Internet to random breakdowns. *Phys. Rev. Lett.* **85(21),** 4626–4628 (2000).
17. Cohen, R., Erez, K., ben-Avraham, D. & Havlin, S. Breakdown of the Internet under intentional attack. *Phys. Rev. Lett.* **86,** 3682–3685 (2001).
18. Callaway, D. S., Newman, M. E. J. & Strogatz, S. H. Network robustness and fragility: percolation on random graphs. *Phys. Rev. Lett.* **85(25),** 5468–5471 (2000).
19. Holme, P., Kim, B. J. & Yoon, C. N. Attack vulnerability of complex networks. *Phys. Rev. E* **65,** 056109 (2002).
20. Motter, A. E., Nishikawa, T. & Lai, Y. C. Range-based attack on links in scale-free networks: Are long-range links responsible for the small-world phenomenon? *Phys. Rev. E* **66,** 065103 (2002).
21. Albert, R., Albert, I. & Nakarado, G. L. Structural vulnerability of the North American power grid. *Phys. Rev. E* **69,** 025103 (2004).
22. Solé, R. V., Casals, M. R. & Murtra, B. C. Robustness of the European power grids under intentional attack. *Phys. Rev. E* **77(2),** 026102 (2007).
23. Berche, B., von Ferber, C. & Holovatch, T. Resilience of public transport networks against attacks. *Europhys. J. B*, **71,** 125–137 (2009).
24. Iyer, S., Killingback, T., Sundaram, B. & Wang, Z. Attack robustness and centrality of complex networks. *Plos One* **8(4),** e59613 (2013).
25. Peng, G. S. & Wu, J. Optimal network topology for structural robustness based on natural connectivity. *Physica A* **443,** 212–220 (2016).
26. Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E. & Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **464,** 1025–1028 (2010).
27. Gao, G., Buldyrev, S. V., Stanley, H. E. & Havlin, S. Networks formed from interdependent networks. *Nature Phys*. **8,** 40–48 (2012).
28. Huang, X. *et al.* The robustness of interdepenent clustered networks. *EPL* **101,** 18002 (2013).
29. Shao, S., Huang, X., Stanley, H. E. & Havlin, S. Robustness of partially interdependent network formed of clustered networks. *Phys. Rev. E* **89,** 032812 (2014).
30. Dong, G. G., Tian, L., Du, R., Fu, M. & Stanley, H. E. Analysis of percolation behaviors of clustered networks with partial support-dependence relations. *Physica A* **394,** 370–378 (2014).
31. Tian, L., Huang, Y., Dong, G. G., Du, R. & Shi, L. Robustness of interdependent and interconnected clustered networks. *Physica A* **412,** 120–126 (2014).
32. Parshani, R., Buldyrev, S. V. & Havlin, S. Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition. *Phys. Rev. Lett.* **105,** 048701 (2010).
33. Zhou, D., Gao, J. X., Stanley, H. E. & Havlin, S. Percolation of partially interdependent scale-free networks. *Phys. Rev. E* **87,** 052812 (2013).
34. Zhou, D., Stanley, H. E., Agostino, G. D. & Scala, A. Assortativity decreases the robustness of interdependent networks. *Phys. Rev. E* **86,** 066103 (2012).
35. Buldyrev, S. V., Shere, N. W. & Cwilich, G. A. Interdependent networks with identical degrees of mutually dependent nodes. *Phys. Rev. E* **83,** 016112 (2011).
36. Parshani, R., Rozenblat, C., Ietri, D., Ducruet, C. & Havlin, S. Inter-similarity between coupled networks. *EPL* **92,** 68002 (2010).
37. Yuan, X., Shao, S., Stanley, H. E. & Havlin, S. How breadth of degree distribution influences network robustness: Comparing localized and random attacks. *Phys. Rev. E* **92,** 032122 (2015).
38. Liu, Z. H., Lai, Y. C., Ye, N. & Dasgupta, P. Connectivity distribution and attack tolerance of general networks with both preferential and random attachments. *Phys. Lett. A* **303,** 337–344 (2002).
39. Barabási, A. L. & Albert, R. Emergence of scaling in random networks. *Science* **286,** 509–512 (1999).
40. Latora, V. & Marchiori, M. Efficient behavior of small-world networks. *Phys. Rev. Lett.* **87(19),** 198701 (2001).

Acknowledgements

This work was partially supported by the National Natural Science Foundation of China under Grant Nos. 61203138, 61374169,61473203 and 61403280. SWS and CYX acknowledge the support from "131" Innovative Talents Program of Tianjin. CYX acknowledges the support from the Scientific Research Foundation for the Returned Overseas Chinese Scholars (Ministry of Education).

Author Contributions

S.S. and C.X. conceived the experiments, S.S., Y.M. and Y.W. conducted the experiments, S.S., L.W., Z.G. and C.X. analyzed the results. All authors reviewed the manuscript.

Additional Information

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

How to cite this article: Sun, S. *et al.* Impact of Degree Heterogeneity on Attack Vulnerability of Interdependent Networks. *Sci. Rep.* **6**, 32983; doi: 10.1038/srep32983 (2016).