SCIENTIFIC REPORTS

OPEN

The robustness of multiplex networks under layer node-based attack

Received: 01 October 2015
Accepted: 11 March 2016
Published: 14 April 2016

Da-wei Zhao[1], Lian-hai Wang[1], Yong-feng Zhi[2], Jun Zhang[2] & Zhen Wang[2,3]

From transportation networks to complex infrastructures, and to social and economic networks, a large variety of systems can be described in terms of multiplex networks formed by a set of nodes interacting through different network layers. Network robustness, as one of the most successful application areas of complex networks, has attracted great interest in a myriad of research realms. In this regard, how multiplex networks respond to potential attack is still an open issue. Here we study the robustness of multiplex networks under layer node-based random or targeted attack, which means that nodes just suffer attacks in a given layer yet no additional influence to their connections beyond this layer. A theoretical analysis framework is proposed to calculate the critical threshold and the size of giant component of multiplex networks when nodes are removed randomly or intentionally. Via numerous simulations, it is unveiled that the theoretical method can accurately predict the threshold and the size of giant component, irrespective of attack strategies. Moreover, we also compare the robustness of multiplex networks under multiplex node-based attack and layer node-based attack, and find that layer node-based attack makes multiplex networks more vulnerable, regardless of average degree and underlying topology.

Robustness of networks refers to the ability of preserving their functional integration when they are subject to failures or attacks[1,2]. Understanding the robustness of networks is thus useful for evaluating the resilience of systems and constructing more efficient architectures. During the past decades, there have been a great number of works contributing to this topic. But the majority of these achievements mainly focus on the vulnerability of single-layer networks[3–9], which seems inconsistent with the well-recognized fact that nodes can simultaneously be the elements of more than one network in most, yet not all, natural and social systems[10–12]?. Recently, Buldyrev *et al.* studied the robustness of interdependent networks, where two networks were coupled in one-to-one interdependence way[13]. Following the failure of one node, a cascading crash took place in both networks (namely, interdependent networks are intrinsically more fragile than traditional single-layer networks), which was accurately validated by the theoretical analysis as well. After this interesting finding, the research of network science is fast extended to multilayer framework[14–17], where systems are usually composed of several network layers, including interdependent networks[18–26], interconnected networks[27–32] and multiplex networks[33–44]. Thus far, the topological characteristics of multilayer networks and dynamical process (such as evolutionary game theory[22,24], disease spreading[28,31,37,43,45], random diffusion[33] and synchronization[39]) upon them have attracted great attention in both theoretical and empirical areas (for a recent review see[14]).

Different from interdependent netowrks, multiplex networks, as a typical kind of topology structures, can be regarded as the combination of several network layers which contain the same nodes yet different intra-layer connections. In this sense, many real-world systems like online social networks[46], technological networks[47], transportation networks[48] can be further studied with the viewpoint of multiplex networks. Figure 1 gives an illustration of multiplex framework: six people are connected via two kinds of relationship, for example Facebook connections (blue links) and Twitter connections (black links) (panel (a)). Such systems can be well embedded into the framework of multiplex networks with two types of links. Each link type in the system defines a network layer, and the nodes of each network layer are the same (see panel (b)). To distinguish the node of multiplex networks and its

[1]Shandong Provincial Key Laboratory of Computer Networks, Shandong Computer Science Center (National Supercomputer Center in Jinan), Jinan 250014, China. [2]School of Automation, Northwestern Polytechnical University, Xian 710072, China. [3]Interdisciplinary Graduate School of Engineering Sciences, Kyushu University, Kasuga-koen, Kasuga-shi, Fukuoka 816-8580, Japan. Correspondence and requests for materials should be addressed to D.-W.Z. (email: zhaodw@sdas.org) or Z.W. (email: zhenwang0@gmail.com)

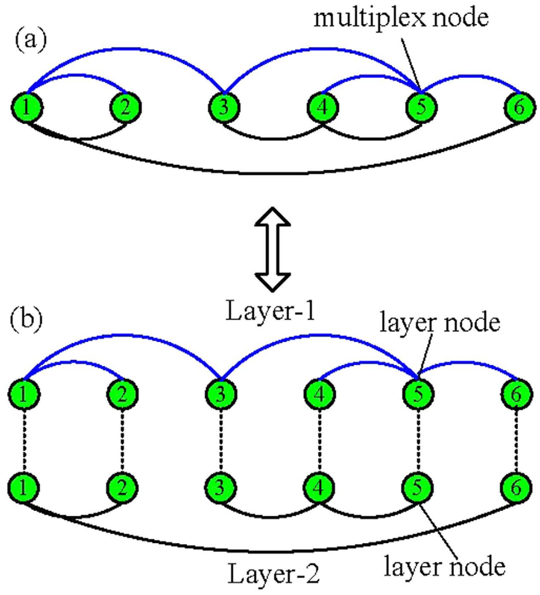

Figure 1. Schematic illustration of multiplex networks. (**a**) Six nodes are connected via two kinds of links (blue link and black link). (**b**) Such a system can also be embedded into the framework of multiplex networks, where each link type defines a network layer. Besides, we also define the terminology: multiplex node and layer node in the total architecture and each layer, respectively.

replica in each network layer, we term them as multiplex node and layer node, respectively. The former points to the node which connects its neighbors via all the types of links, like node 3 of Fig. 1(a), whose neighbors are 1, 5 and 4 via blue and black links. While the latter is the partial case of multiplex node and just considers the local connection topology of a given node on one layer. For example, if we only consider blue (black) links in Fig. 1(b), node 3 is the layer node of Layer-1 (Layer-2). Now, it is thus clear that multiplex node means the joint element of all the layers, and layer node just belongs to the element of one given layer.

Looking back to the early topic, the research of robustness of multiplex networks thus becomes a very interesting and crucial challenge. In[44], Min *et al.* explored the robustness of multiplex networks when multiplex nodes were removed randomly or intentionally (here the removal of a multiplex node means all its replicas in network layers are pruned). They showed that correlated coupling would affect the structural robustness of multiplex networks in diverse fashion. In some realistic cases, however, the failure unites or attack targets may be just the layer nodes. For example, on multiplex transport networks where nodes are cities and network layers are airplane network, highway network and railway network, the failures may take place in one or some, yet not all the layers. Similarly, prohibiting the use of some social network accounts, people may still connect with each other via other available social network accounts. In this sense, an interesting question naturally poses itself, which we aim to address in this work. Namely, how does the removal of layer node affect the robustness of multiplex networks?

Aiming to answer this issue, we consider the robustness of multiplex networks under layer node-based attack, which can be further divided into random and targeted scenarios. With the framework of generating function method[49], we propose theoretical method to calculate the critical threshold of network crash and the size of giant component when a fraction of layer nodes are removed. Furthermore, we also compare the robustness of multiplex networks under multiplex nodes-based attack and layer node-based attack.

Results

Model definition and theoretical analysis.

As mentioned in previous literatures[13,21,23], the robustness of networks is usually evaluated by one critical threshold value and the size of giant component after the removal of nodes. If the fraction of removed nodes exceeds this critical threshold, the giant component becomes null. Here it is worth mentioning that the accurate definition of giant component of multiplex networks should be mutually connected giant component (MCGC), which is the largest component that remains after the removal propagates back and forth in the different layers. The giant component naturally consists of a set of connected multiplex nodes. A pair of multiplex nodes are regarded to have connection if there exists at least one type of link between them. Therefore, attacking some layer nodes may not destroy their connection with other nodes, and the set of nodes that remains at the end of damage is the mutually connected giant component (see Fig. 2 for schematic illustration). In the following, we will focus on theoretical method of calculating the critical threshold value and the size of giant component of the multiplex networks under layer node-based attack.

For simplicity (yet without loss of generality), we refer to previous treatment[2,44,49]. For a multiplex network composing of N multiplex nodes and m network layers, the generating function for the joint degree distribution $p(\vec{k}_j)$, where $\vec{k}_j = (k_{j_1},\ k_{j_2},\ \ldots, k_{j_m})$ denotes the degrees of a multiplex node j in each layer, can be written in the form of a finite polynomial

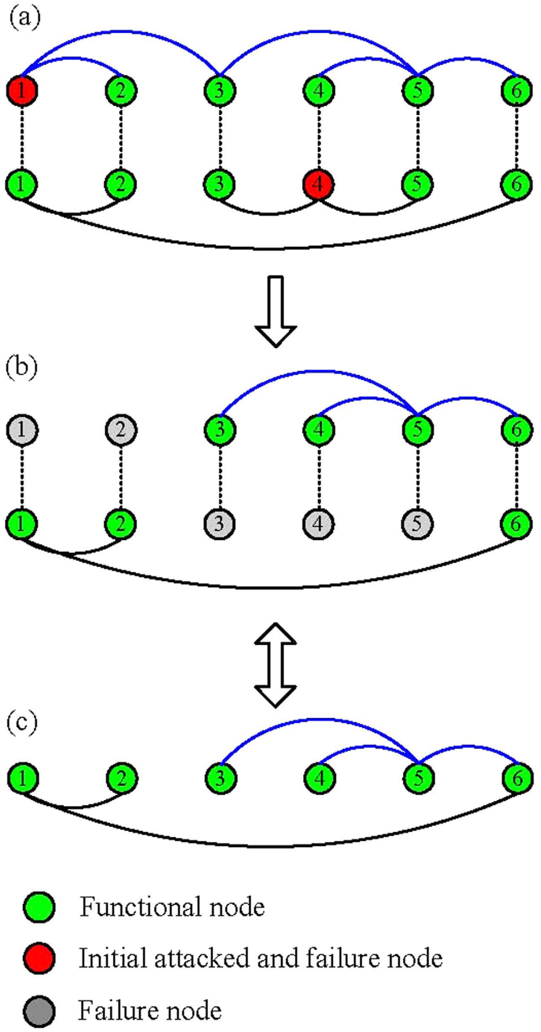

Figure 2. Schematic illustration of layer node-based attack and giant component of multiplex networks. (**a**) Layer node 1 of Layer-1 and layer node 4 of Layer-2 are initially attacked. (**b**) Soon layer nodes 1,2 of Layer-1 and 3,4 and 5 of Layer-2 become failure nodes since they do not belong to the giant component of corresponding layers. (**c**) However, multiplex nodes 1–6 still belong to the mutually connected giant component of the multiplex networks since they connect to the largest component through at least one type of links after damage.

$$G_0(\vec{x}) = \sum_{\vec{k}_j} p(\vec{k}_j) \prod_{i=1}^{m} x_i^{k_{j_i}}, \tag{1}$$

where $\vec{x} = (x_1, \ x_2, \ \ldots, x_m)$ represents the auxiliary variable coupled to $\vec{k}_j$. Here, it is of particular value to emphasize give that the key parameter, joint degree distribution $p(\vec{k}_j)$, contains the general information of degree correlation between network layers, the following derivations will be universal for (un)correlated multiplex networks. Then the generating function of remaining joint degree distribution by following a randomly chosen link of network layer i is given by

$$G_1^{(i)}(\vec{x}) = \frac{1}{z_i}\frac{\partial}{\partial x_i} G_0(\vec{x}), \tag{2}$$

where z_i is the average degree of layer i.

Then, on locally-tree like networks, if u_i ($i = 1, 2, \ldots, m$) is defined as the probability that a multiplex node reached by following a random chosen link of network layer i does not belong to the giant component, it can be derived by the coupled self-consistency equation

$$u_i = G_1^{(i)}(\vec{u}), \tag{3}$$

where $\vec{u} = (u_1, u_2, \ldots, u_m)$. Furthermore, the size of the (mutually connected) giant component can be calculated according to

$$R = 1 - G_0(\vec{u}). \tag{4}$$

Along this framework, we can now turn to the layer node-based attack on multiplex networks. If $\phi_i(k_{j_i})$ is used to denote the probability that a layer node with degree k_{j_i} is removed from network layer *i*, then the generating function of the joint degree distribution after the removal of layer nodes can be expressed as

$$H_0(\vec{x}) = \sum_{\vec{k}_j} p(\vec{k}_j) \prod_{i=1}^{m} \left\{ \phi_i(k_{j_i}) + [1 - \phi_i(k_{j_i})] x_i^{k_{j_i}} \right\}. \tag{5}$$

Correspondingly, the generating function of remaining joint degree distribution after the removal of layer nodes by following a randomly chosen link of network layer *i* is given by

$$H_1^{(i)}(\vec{x}) = \frac{1}{z_i} \frac{\partial}{\partial x_i} H_0(\vec{x}). \tag{6}$$

In the case of layer node removal, the probability v_i that a multiplex node reached by following one random chosen link of network layer *i* does not belong to the giant component can be written as

$$\begin{aligned} v_i &= \frac{1}{z_i} \sum_{\vec{k}_j} k_{j_i} p(\vec{k}_j) \left\{ \phi_i(k_{j_i}) + [1 - \phi_i(k_{j_i})] v_i^{k_{j_i}-1} \prod_{s \neq i} \{\phi_s(k_{j_s}) + [1 - \phi_s(k_{j_s})] v_s^{k_{j_s}}\} \right\} \\ &= \frac{\langle k_{j_i} \phi_i(k_{j_i}) \rangle}{z_i} + H_1^{(i)}(\vec{v}). \end{aligned} \tag{7}$$

Then, after the removal of nodes from layers, the size of giant component is given as follows

$$R = 1 - H_0(\vec{v}). \tag{8}$$

The existence of giant component under layer node-based attack requires the largest eigenvalue Λ of the Jacobian matrix **J** of Eq. (7) at $(1, 1, \ldots, 1)$ to be larger than unity[44]. In this work, we mainly focus on multiplex networks composed of two Erdös-Rényi (ER) random[50] or Barabási-Albert scale-free (SF)[51] network layers (namely, $m = 2$), **J** thus can be written as

$$\mathbf{J} = \begin{pmatrix} \kappa_1 & \mathcal{K}_1 \\ \mathcal{K}_2 & \kappa_2 \end{pmatrix}, \tag{9}$$

where $\kappa_i = (\langle k_{j_i}^2 (1 - \phi_i(k_{j_i})) \rangle - \langle k_{j_i}(1 - \phi_i(k_{j_i})) \rangle)/z_i$ and $\mathcal{K}_i = \langle k_{j_1} k_{j_2} (1 - \phi_1(k_{j_1}))(1 - \phi_2(k_{j_2})) \rangle / z_i$. The largest eigenvalue Λ is given by

$$\Lambda = \frac{1}{2}[\kappa_1 + \kappa_2 + \sqrt{(\kappa_1 - \kappa_2)^2 + 4\mathcal{K}_1\mathcal{K}_2}]. \tag{10}$$

Before computation simulations, it is worth mentioning that the above derived theoretical framework (of generating function) is even effective in the thermodynamic limit $N \rightarrow \infty$. Aiming to validate its accuracy, we will pay our main attention to middle-size networks in the following simulations.

Layer node-based random attack. For layer node-based random attack, which is characterized by random removal of layer nodes from network layers, there exists the removal probability $\phi_i(k_{j_i}) = \phi_i^{LR}$ $(i = 1, 2; j = 1, 2, \ldots N)$. According to the above analysis, the critical threshold and the size of giant component of multiplex networks under layer node-based random removal can be respectively expressed as

$$(\phi_1^{LR}, \phi_2^{LR})_c = \{(\phi_1^{LR}, \phi_2^{LR}) | \Lambda = 1\} \tag{11}$$

and

$$R^{LR} = 1 - H_0(\vec{v}), \tag{12}$$

where $\phi_i(k_{j_i}) = \phi_i^{LR}$. It is worth mentioning that above $(\phi_1^{LR}, \phi_2^{LR})_c$ there is no giant component, whereas below $(\phi_1^{LR}, \phi_2^{LR})_c$ a giant connected cluster exists.

We start by inspecting how layer node-based random attack affects the robustness of multiplex networks. Figure 3 shows the size R^{LR} of giant component in dependence on the removal probability ϕ_1^{LR} and ϕ_2^{LR} for network layer 1 and network layer 2, respectively. Moreover, the black line indicates the theoretical critical threshold calculated according to Eq. (11). It is clear that when the removal probability $(\phi_1^{LR}, \phi_2^{LR})$ is above this black line, the size of giant component becomes negligible; whereas there exists one giant component if $(\phi_1^{LR}, \phi_2^{LR})$ is located below this black line. This implies that the theoretical critical threshold can accurately predict the impact of layer node-based attack on the robustness of multiplex networks. To further validate this fact, we also compare the

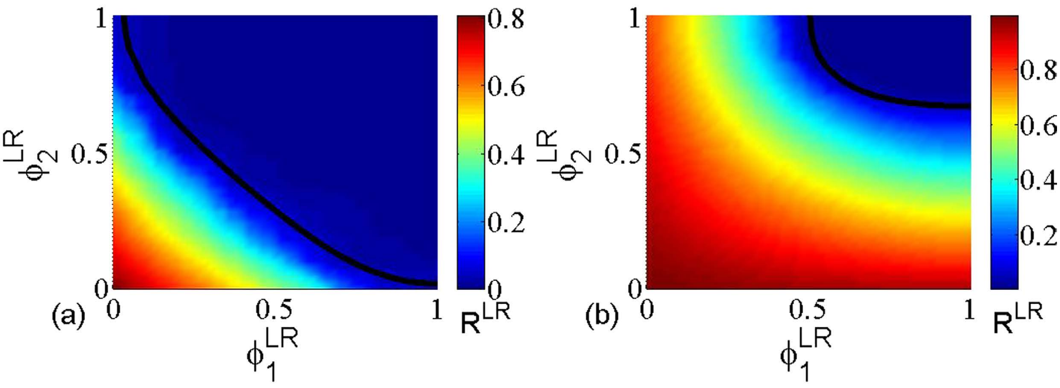

Figure 3. The size R^{LR} of giant component in dependence on removal probability ϕ_1^{LR} and ϕ_2^{LR} for layer node-based random attack. The black line indicates the theoretical critical threshold calculated according to Eq. (11). The networks used are multiplex ER network with average degree (**a**) $z_1 = z_2 = 1$, (**b**) $z_1 = 2$, $z_2 = 3$ and network size $N = 5000$. It is worth mentioning that the well agreement between theoretical prediction and simulation outcome is effective for larger networks as well (not shown here). For the convenience of simulations, we will focus on the same network size in the remaining figs.

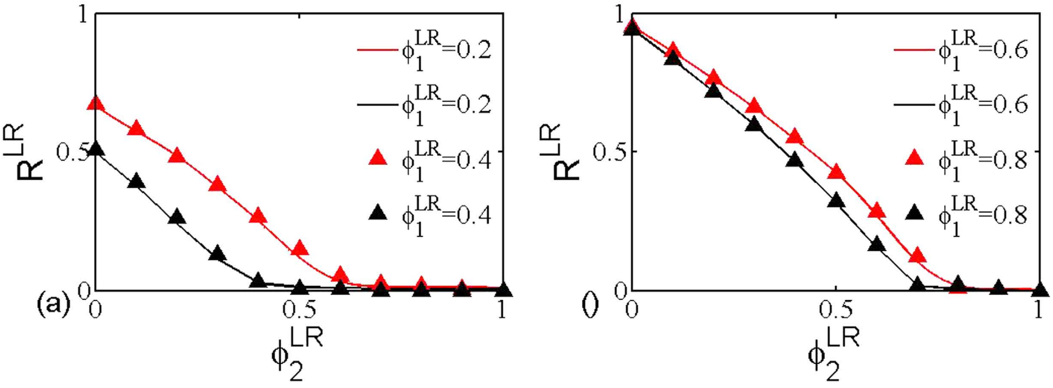

Figure 4. Theoretical (line) and numerical (point) results of the size R^{LR} of giant component as a function of ϕ_2^{LR} when ϕ_1^{LR} takes fixed values. The networks used are multiplex ER networks with average degree (**a**) $z_1 = z_2 = 1$, (**b**) $z_1 = 2$, $z_2 = 3$ and network size $N = 5000$.

theoretical prediction derived from Eq. (12) and simulation results for the size of giant component in Fig. 4. It can be observed that there is indeed good agreement between simulation and theoretical prediction.

Layer node-based targeted attack. Targeted attack, as a well-known attack strategy, usually aims to remove influential nodes, which can be identified by centrality measures, such as the degree centrality, eigenvector centrality, k-shell centrality and betweenness centrality[52]. In this work, we mainly pay attention to the viewpoint of degree centrality. For layer node-based targeted attack, the removal probability of a layer node with degree k_{j_i} is determined by its degree, and can be expressed as follows

$$\phi_i(k_{j_i}) = \begin{cases} 1, & \text{if } k_{j_i} > k_{c_i} \\ f_i, & \text{if } k_{j_i} = k_{c_i}, \\ 0, & \text{if } k_{j_i} < k_{c_i} \end{cases} \tag{13}$$

where k_{c_i} is the cutoff degree for attack on network layer i, and f_i denotes the removal probability of node with degree k_{c_i}. Consequently, the total fraction of removal nodes in network layer i is given by

$$\phi_i^{LT} = \sum_{k_{j_i}} p_i(k_{j_i})\phi_i(k_{j_i}), \tag{14}$$

where $p_i(k_{j_i})$ indicates the fraction of layer nodes with degree k_{j_i} in layer i.

Similar to Eqs (11) and (12), we can get the critical threshold

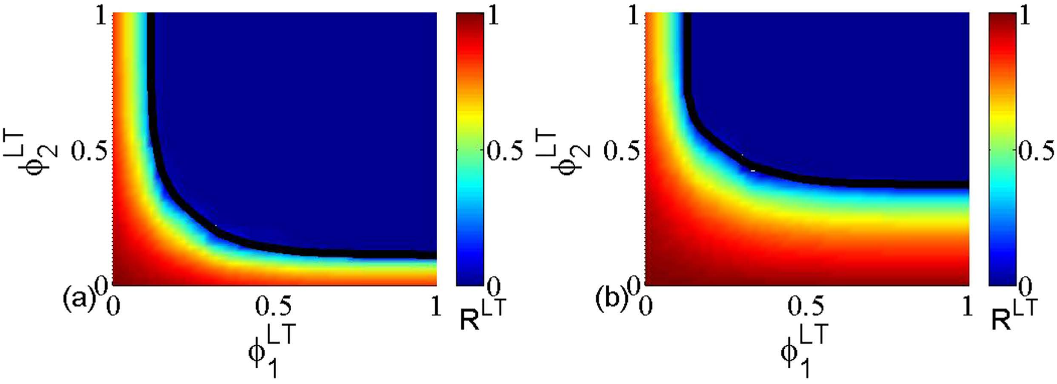

Figure 5. The size R^{LT} of giant component in dependence on removal probability ϕ_1^{LT} and ϕ_2^{LT} for layer node-based targeted attack. The black line indicates the theoretical critical threshold calculated according to Eq. (15). The networks used are multiplex ER networks with average degree (**a**) $z_1 = z_2 = 2$, (**b**) $z_1 = 2$, $z_2 = 4$ and network size $N = 5000$.

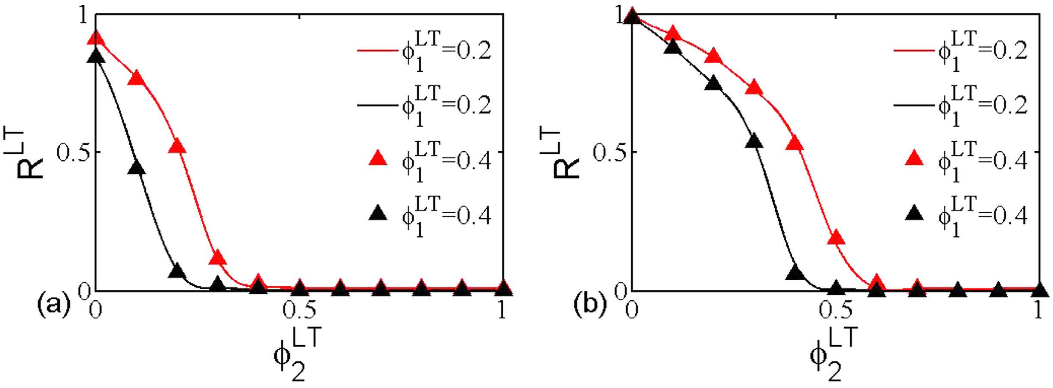

Figure 6. Theoretical (line) and numerical (point) results of the size R^{LT} of giant component as a function of ϕ_2^{LT} when ϕ_1^{LT} takes fixed values. The networks used are multiplex ER networks with average degree (**a**) $z_1 = z_2 = 2$, (**b**) $z_1 = 2$, $z_2 = 4$ and network size $N = 5000$.

$$(\phi_1^{LT}, \phi_2^{LT})_c = \{(\phi_1^{LT}, \phi_2^{LT}) | \Lambda = 1\}, \tag{15}$$

and the size of giant component

$$R^{LT} = 1 - H_0(\vec{v}), \tag{16}$$

where $\phi_i(k_{j_i})$ is defined as Eq. (13), for layer node-based targeted attack on multiplex networks consisting of two network layers.

In Fig. 5, the color code represents the size R^{LT} of the giant component as a function of the removal probability ϕ_1^{LT} and ϕ_2^{LT} under layer node-based targeted attack, and the black line indicates the theoretical critical threshold calculated according to Eq. (15). Similar to Fig. 3, the theoretical prediction fully agrees with the simulation results. Moreover, Fig. 6 provides the further comparison between the theoretical prediction and simulation for the size of giant component, which also validates the accuracy of theoretical method. Combining with all the above phenomena, it is clear that the proposed theoretical framework can allow us to accurately calculate the critical threshold and the size of giant component under the layer node-based attack.

Comparison of robustness of multiplex networks. Based on the above framework, multiplex node-based attack proposed in[44], can be regarded as a special case of layer node-based attack when all the removed nodes or replicas are the same in each network layer. From the economic viewpoint, the cost of removing p fraction of multiplex nodes seems approximately equal to that of removing p fraction of layer nodes in each network layer. However, the damage of both scenarios on the multiplex networks may be greatly different. In this sense, it becomes very instructive to compare the robustness of multiplex networks under multiplex node-based attack and layer node-based attack. For simplicity of comparison, we assume that layer node-based attack means to remove the same proportion of layer nodes in each network layer in what follows. The removal probability

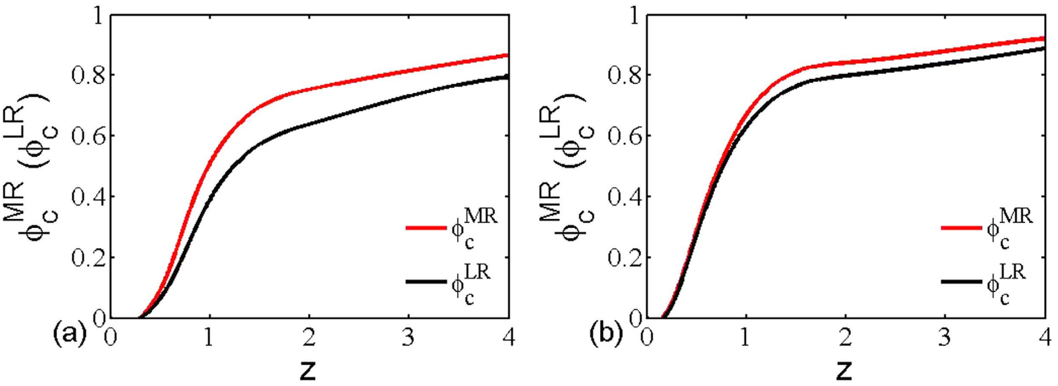

Figure 7. The critical threshold of multiplex networks in dependence on the network average degree under multiplex node-based random attack (red dash line) and layer node-based random attack (black solid line). The networks used are (**a**) multiplex ER networks with average degree $z_1 = z_2 = z$ and (**b**) multiplex SF networks with average degree $z_1 = z_2 = z$. The size of all the networks is $N = 5000$.

correspondingly becomes $\phi_1^{LR} = \phi_2^{LR} = \phi^{LR}$ for layer node-based random attack and $\phi_1^{LT} = \phi_2^{LT} = \phi^{LT}$ for layer node-based targeted attack. While for multiplex node-based attack, the total fraction of removal multiplex nodes under random attack and targeted attack becomes ϕ^{MR} (all of the multiplex nodes are removed randomly with probability ϕ^{MR}) and

$$\phi^{MT} = \sum_{\vec{k}_j} p(\vec{k}_j)\phi^{MT}(\vec{k}_j), \tag{17}$$

where $p(\vec{k}_j)$ indicates the fraction of multiplex nodes with degree $\vec{k}_j = \{k_{j_1}, k_{j_2}\}$, and $\phi^{MT}(\vec{k}_j)$ is defined as the removal probability of multiplex nodes with degree $\vec{k}_j$ and given by

$$\phi^{MT}(\vec{k}_j) = \begin{cases} 1, & \text{if } k_{j_1} + k_{j_2} > k_c \\ f, & \text{if } k_{j_1} + k_{j_2} = k_c, \\ 0, & \text{if } k_{j_1} + k_{j_2} < k_c \end{cases} \tag{18}$$

where k_c is the cutoff degree and f denotes the removal probability of node which satisfies $k_{j_1} + k_{j_2} = k_c$.

Similar to the above treatment, we still use the critical threshold as a uniform evaluation index for multiplex node-based attack and layer node-based attack. In fact, the larger the value of critical threshold, the better the robustness of multiplex networks against attack. To get a more intuitive comparison, we consider the simple case of random attack on multiplex ER networks with $z_1 = z_2 = z$. Based on Eq. (9), we have $\kappa_1 = \kappa_2 = (z - 1)(1 - \phi^{LR})$ and $\mathcal{K}_1 = \mathcal{K}_2 = z(1 - \phi^{LR})^2$. The critical threshold of layer node-based random attack ϕ_c^{LR} thus becomes

$$\phi_c^{LR} = 1 - \frac{1}{z}. \tag{19}$$

Similarly, according to ref. 44, the critical threshold of multiplex node-based random attack ϕ_c^{MR} is

$$\phi_c^{MR} = 1 - \frac{1}{2z - 1}. \tag{20}$$

Obviously, there always exists $\phi_c^{MR} > \phi_c^{LR}$, which means multiplex networks are more robustness under the multiplex node-based random attack, irrespective of average degree. To attest this theoretical analysis, we will provide more comprehensive simulation comparisons in what follows. Figure 7 features how the the critical threshold of multiplex networks varies as a function of average degree under both multiplex node-based random attack (red line) and layer node-based random attack (black line). It is clear that the threshold of both cases rises with the increment of average degree, which means that multiplex networks are more robust for denser connections. Interestingly, another observation of utmost significance is that the threshold of multiplex node-based random attack is always higher than that of layer node-based random attack, irrespective of the average degree and underlying connection topology. This computation outcome completely agrees with the aforementioned theoretical prediction. This is to say, multiplex networks are more vulnerable under layer node-based attack, because it usually makes more multiplex nodes subject to attack and lose more connections with other multiplex nodes. Moreover, we can also obtain the similar observation for multiplex node-based targeted attack and layer node-based targeted attack in Fig. 8, which further supports the fact that layer node-based attack brings larger damage to multiplex networks. Along this seminal finding, it may shed new light into the research of protection or immunization of empirical multiplex topology[53,54].

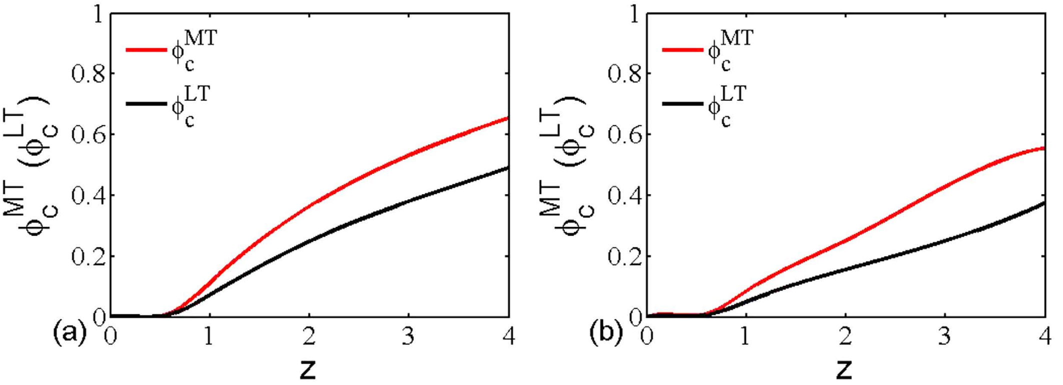

Figure 8. The critical threshold of multiplex networks in dependence on the network average degree under multiplex node-based targeted attack (red line) and layer node-based targeted attack (black line). The networks used are (**a**) multiplex ER networks with average degree $z_1 = z_2 = z$ and (**b**) multiplex SF networks with average degree $z_1 = z_2 = z$. The size of all the networks is $N = 5000$.

Summary

To sum, we have studied the robustness of multiplex networks under layer node-based attack. Under this framework, the layer nodes can be removed randomly or intentionally, which corresponds to layer node-based random attack or layer node-based targeted attack. A theoretical method is proposed to evaluate the robustness of multiplex networks when a fraction of layer nodes are removed. Through numerous simulations, this method can accurately calculate the threshold and size of giant component, irrespective of the removal case. In addition, we also compare the robustness of multiplex networks under multiplex node-based attack and layer node-based attack. An interesting finding is that multiplex networks will be more robust under multiplex node-based attack, which is universal for different average degree and underlying topology. With regard to the reason, it may be related with the fact that layer node-based attack usually brings damage to more multiplex nodes, which will directly break the remaining joint component of networks.

Since multiplex framework is ubiquitous in realistic social and technological networks, we hope that the present outcomes can inspire further research of the robustness of multiplex networks, especially combining with the novel properties of multiplex networks, like the clustering characteristic[25], degree-degree correlation between network layers[37]. In addition, the targeted attack can also be incorporated into other centrality measures, such as the eigenvector centrality, *k*-shell centrality and betweenness centrality[52]. Along this line, we may get new understanding for the protection of multiplex network.

References

1. Cohen, R. & Havlin, S. *Complex networks: structure, robustness and function* (Cambridge University Press, 2010).
2. Callaway, D. S., Newman, M. E., Strogatz, S. H. & Watts, D. J. Network robustness and fragility: Percolation on random graphs. *Phys. Rev. Lett.* **85,** 5468 (2000).
3. Albert, R., Jeong, H. & Barab¢si, A. L. Error and attack tolerance of complex networks. *Nature* **406,** 378–382 (2000).
4. Motter, A. E. & Lai, Y. C. Cascade-based attacks on complex networks. *Phys. Rev. E* **66,** 065102 (2002).
5. Perc, M. Evolution of cooperation on scale-free networks subject to error and attack. *New J. Phys.* **11,** 033027 (2009).
6. Shargel, B., Sayama, H., Epstein, I. R. & Bar-Yam, Y. Optimization of robustness and connectivity in complex networks. *Phys. Rev. Lett.* **90,** 068701 (2003).
7. Xiao, S. *et al.* Robustness of scale-free networks under rewiring operations. *EPL* **89,** 38002 (2010).
8. Radicchi, F. Predicting percolation thresholds in networks. *Phys. Rev. E* **91,** 010801 (2015).
9. Zhao, D., Peng, H., Li, L., Yang, Y. & Li, S. An efficient patch dissemination strategy for mobile networks. *Mathematical Problems in Engineering* **2013,** 896187 (2013).
10. Kivelä, M. *et al.* Multilayer networks. *J. Comp. Net.* **2,** 203–271 (2014).
11. Cardillo, A. *et al.* Modeling the multi-layer nature of the European Air Transport Network: Resilience and passengers re-scheduling under random failures. *Euro. Phys. J. ST* **215,** 23–33 (2013).
12. Yuan, H. & Wang, X. Vortex-assisted domain wall depinning and propagation in notched nanowires. *Euro. Phys. J. B* **88,** 1–5 (2015).
13. Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E. & Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **464,** 1025–1028 (2010).
14. Boccaletti, S. *et al.* The structure and dynamics of multilayer networks. *Phys. Rep.* **544,** 1–122 (2014).
15. De Domenico, M. *et al.* Mathematical formulation of multilayer networks. *Phys. Rev. X* **3,** 041022 (2013).
16. Salehi, M. *et al.* Spreading processes in Multilayer Networks. *Network Science and Engineering, IEEE Transactions on* **2,** 53–64 (2015).
17. Zhao, D., Wang, L., Xu, L. & Wang, Z. Finding another yourself in multiplex networks. *App. Math. Comput.* **266,** 599–604 (2015).
18. Radicchi, F. Percolation in real interdependent networks *Nat. Phys.* **11,** 597C–602 (2015).
19. Gao, J., Buldyrev, S. V., Stanley, H. E. & Havlin, S. Networks formed from interdependent networks. *Nat. Phys.* **8,** 40–48 (2012).
20. Dong, G. *et al.* Robustness of network of networks under targeted attack. *Phys. Rev. E* **87,** 052804 (2013).
21. Gao, J., Buldyrev, S. V., Havlin, S. & Stanley, H. E. Robustness of a network of networks. *Phys. Rev. Lett.* **107,** 195701 (2011).
22. Wang, Z., Szolnoki, A. & Perc, M. Interdependent network reciprocity in evolutionary games. *Sci. Rep.* **3,** 1183 (2013).
23. 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).
24. Wang, Z., Szolnoki, A. & Perc, M. Optimal interdependence between networks for the evolution of cooperation. *Sci. Rep.* **3,** 2470 (2013).
25. Parshani, R., Rozenblat, C., Ietri, D., Ducruet, C. & Havlin, S. Inter-similarity between coupled networks. *EPL* **92,** 68002 (2010).

26. Shao, J., Buldyrev, S. V., Havlin, S. & Stanley, H. E. Cascade of failures in coupled network systems with multiple support-dependence relations. *Phys. Rev. E* **83,** 036116 (2011).
27. Radicchi, F. & Arenas, A. Abrupt transition in the structural formation of interconnected networks. *Nat. Phys.* **9,** 717–720 (2013).
28. Dickison, M., Havlin, S. & Stanley, H. E. Epidemics on interconnected networks. *Phys. Rev. E* **85,** 066109 (2012).
29. De Domenico, M., Solé-Ribalta, A., Gómez, S. & Arenas, A. Navigability of interconnected networks under random failures. *Proc. Natl. Acad. Sci. USA* **111,** 8351–8356 (2014).
30. Wang, H. *et al.* Effect of the interconnected network structure on the epidemic threshold. *Phys. Rev. E* **88,** 022801 (2013).
31. Saumell-Mendiola, A. & Serrano, M. á. and Boguñá, M. Epidemic spreading on interconnected networks. *Phys. Rev. E* **86,** 026106 (2012).
32. Zhao, D., Li, L., Li, S., Huo, Y. & Yang, Y. Identifying influential spreaders in interconnected networks. *Phys. Scripta* **89,** 015203 (2014).
33. Serrano, M. Á., Buzna, Ľ. & Boguñá, M. Escaping the avalanche collapse in self-similar multiplexes. *New J. Phys.* **17,** 053033 (2015).
34. Bastas, N., Lazaridis, F., Argyrakis, P. & Maragakis, M. Static and dynamic behavior of multiplex networks under interlink strength variation. *EPL* **109,** 38006 (2015).
35. Sole-Ribalta, A. *et al.* Spectral properties of the Laplacian of multiplex networks. *Phys. Rev. E* **88,** 032807 (2013).
36. Granell, C., Gómez, S. & Arenas, A. Dynamical interplay between awareness and epidemic spreading in multiplex networks. *Phys. Rev. Lett.* **111,** 128701 (2013).
37. Zhao, D., Li, L., Peng, H., Luo, Q. & Yang, Y. Multiple routes transmitted epidemics on multiplex networks. *Phys. Lett. A* **378,** 770–776 (2014).
38. Zhao, D. *et al.* Immunization of epidemics in multiplex networks. *PloS One* **9,** e112018 (2014).
39. Gambuzza, L. V. & Frasca, M. Intra-layer synchronization in multiplex networks. *EPL* **110,** 20010 (2015).
40. Battiston, F., Nicosia, V. & Latora, V. Structural measures for multiplex networks. *Phys. Rev. E* **89,** 032804 (2014).
41. Kim, J. Y. & Goh, K. I. Coevolution and correlated multiplexity in multiplex networks *Phys. Rev. Lett.* **111,** 058702 (20201305).
42. Gómez-Gardeñes, J., Reinares, I., Arenas, A. & FlorÍa, L. M. Evolution of cooperation in multiplex networks. *Sci. Rep.* **2,** 620 (2012).
43. Buono, C., Alvarez-Zuzek, L. G., Macri, P. A. & Braunstein, L. A. Epidemics in partially overlapped multiplex networks. *PloS One* **9,** e92200 (2014).
44. Min, B., Do Yi, S., Lee, K. M. & Goh, K. I. Network robustness of multiplex networks with interlayer degree correlations. *Phys. Rev. E* **89,** 042811 (2014).
45. Wang, L. & Li, X. Spatial epidemiology of networked metapopulation: An overview. *Chin. Sci. Bull.* **59,** 3511–3522 (2014).
46. Dodds, P. S., Muhamad, R. & Watts, D. J. An experimental study of search in global social networks. *Science* **301,** 827–829 (2003).
47. Wang, W. X., Wang, B. H., Hu, B., Yan, G. & Ou, Q. General dynamics of topology and traffic on weighted technological networks. *Phys. Rev. Lett.* **94,** 188702 (2005).
48. Banavar, J. R., Maritan, A. & Rinaldo, A. Size and form in efficient transportation networks. *Nature* **399,** 130–132 (1999).
49. Newman, M. E., Strogatz, S. H. & Watts, D. J. Random graphs with arbitrary degree distributions and their applications. *Phys. Rev. E* **64,** 026118 (2001).
50. Erdös, R. On random graphs I. *Publ. Math. Debrecen* **6,** 290–297 (1959).
51. Barabási, A. L. & Albert, R. Emergence of scaling in random networks. *Science* **286,** 509–512 (1999).
52. Ren, X. L. & Lü, L. Y. Review of ranking nodes in complex networks (in Chinese). *Chin. Sci. Bull.* **59,** 1175–C1197 (2014).
53. Wang, Z., Zhao, D. W., Wang, L., Sun, G. Q. & Jin, Z. Immunity of multiplex networks via acquaintance vaccination. *EPL* **112,** 48002 (2015).
54. Wamg, Z., Wang, L., Szolnoki, A. & Perc, M. Evolutionary games on multilayer networks: a colloquium. *Euro. Phys. J. B* **88,** 124 (2015).

Acknowledgements

This work is supported by: The National Natural Science Foundation of China (Grant No. 61572297 and 61471300), Shandong Province Outstanding Young Scientists Research Award Fund Project (Grant No. BS2015DX006, BS2014DX007), Shandong Academy of Sciences Youth Fund Project (Grant No. 2015QN003) and Natural Science Foundation of Shandong Province (Grant No. ZR2014FM003, ZR2015YL018).

Author Contributions

D.W.Z., L.H.W., Y.F.Z., J.Z. and Z.W. designed the research, performed the simulations, analyzed the result and wrote the paper.

Additional Information

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

How to cite this article: Zhao, D.-w. *et al.* The robustness of multiplex networks under layer node-based attack. *Sci. Rep.* **6**, 24304; doi: 10.1038/srep24304 (2016).