Research Article
Interdependency and Vulnerability of Multipartite Networks under Target Node Attacks

Qing Cai, 1 Mahardhika Pratama, 1 and Sameer Alam 2
1 School of Computer Science and Engineering, Nanyang Technological University, Singapore
2 School of Mechanical and Aerospace Engineering, Nanyang Technological University, Singapore

Correspondence should be addressed to Mahardhika Pratama; pratama@ieee.org and Sameer Alam; sameeralam@ntu.edu.sg

Received 12 March 2019; Accepted 4 November 2019; Published 20 November 2019

Academic Editor: Diego R. Amancio

Copyright © 2019 Qing Cai et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Complex networks in reality may suffer from target attacks which can trigger the breakdown of the entire network. It is therefore pivotal to evaluate the extent to which a network could withstand perturbations. The research on network robustness has proven as a potent instrument towards that purpose. The last two decades have witnessed the enthusiasm on the studies of network robustness. However, existing studies on network robustness mainly focus on multilayer networks while little attention is paid to multipartite networks which are an indispensable part of complex networks. In this study, we investigate the robustness of multipartite networks under intentional node attacks. We develop two network models based on the largest connected component theory to depict the cascading failures on multipartite networks under target attacks. We then investigate the robustness of computer-generated multipartite networks with respect to eight node centrality metrics. We discover that the robustness of multipartite networks could display either discontinuous or continuous phase transitions. Interestingly, we discover that larger number of partite sets of a multipartite network could increase its robustness which is opposite to the phenomenon observed on multilayer networks. Our findings shed new lights on the robust structure design of complex systems. We finally present useful discussions on the applications of existing percolation theories that are well studied for network robustness analysis to multipartite networks. We show that existing percolation theories are not amenable to multipartite networks. Percolation on multipartite networks still deserves in-depth efforts.

1. Introduction

Complex systems are ubiquitous in our daily lives. The form of a complex system ranges from the macroscopic level like the power grid systems [1] to the microscopic level like the metabolic systems [2]. In order to better understand and control complex systems, a widely adopted method is to model a complex system as a network that is composed of a set of nodes and edges with the nodes denoting the network’ components and the edges denoting the relations between components [3]. It has been proved that complex network modelling and analysis are a promising instrument for not only control science [4–7] but also data science [8–10].

Note that a complex network in reality is likely to suffer from attacks and failures of network components [11–13]. Because the components of a complex network are interconnected [14, 15], therefore the failures of some components are likely to trigger the failures of other components that depend on those failed components and cascading failures occur [16, 17]. As a result, a small fraction of component failures may lead to the breakdown of the whole network [18–21]. In order to evaluate the robustness of complex networks under perturbations, studies on network robustness emerged and have gained a great popularity in the past two decades [22–26]. In the literature, a large body of work has been done towards network robustness [27–31].

Network robustness has long been studied [32–36]. During a long period of time, robustness studies mainly exploit the robustness of single networks [37]. It has been widely reported that the robustness of single networks normally displays a continuous phase transition phenomenon [17, 38, 39], which indicates that single networks are robust to perturbations. Note that networks in reality are not...
independent but on the contrary interact with one another, forming multilayer networks [40–44]. A small fraction of component failures in a multilayer network can elicit cascading failures [45, 46]. It has been disclosed that the robustness of multilayer networks normally exhibits a discontinuous phase transition phenomenon [14, 45, 47], which indicates that multilayer networks are vulnerable to perturbations [15, 18, 24].

The seminal work in [45] has sparked the research enthusiasm on the robustness of multilayer networks. An enormous amount of outstanding work has been done by researchers towards network robustness analysis [48–53]. Existing studies can be roughly categorised into three groups, i.e., studies on network robustness to node failures [54–59], studies on network robustness to edge failures [46, 60–62], and studies on network robustness to community failures [63–66]. A community is generally referred to as a subgraph of a network that has dense interconnections but sparse connections with the rest of the network [67–73]. It should be pointed out that, apart from multilayer networks, there exists another kind of network called multipartite networks, which are an indispensable part of complex networks [3, 74]. A multipartite network generally refers to a network whose nodes can be divided into several sets or layers while its edges only occur between two neighbouring node sets or layers (see Section 2.2 for the mathematical definition). A handful of complex networks such as service supplier-user networks [75], economic networks [76], ecological networks [77], and biological networks [78] could be modeled as multipartite networks.

Investigating the robustness of multipartite networks is significantly pertinent to unravel system dynamics of multipartite networks. In the literature, studies on the robustness of multipartite networks only deal with the simplest scenarios, namely, bipartite networks. Although existing studies indicate that bipartite networks are robust to attacks [56, 79, 80], how multipartite networks behave in face of attacks is still unknown. Meanwhile, existing studies are primarily from specific domains like ecology [56, 64, 65], biology [79], and economy [80], i.e., the robustness analysis of bipartite networks depends on domain-specific knowledge. Albeit the nature of studies on the robustness of multilayer networks [15, 81], existing models and theories cannot be directly applied to multipartite networks. The key reason is that the structures of multipartite networks differ from that of multilayer networks.

In order to understand how multipartite networks behave in the presence of attacks, in this paper we present a simulation-based study to capture a fundamental comprehension of the robustness of multipartite networks. To do so, we first put forward two network models to mimic the dynamic processes on multipartite networks under target node attacks. Subsequently, we examine the robustness of multipartite networks under target node attacks with respect to eight widely investigated node centrality metrics, which are the Degree centrality, Betweenness centrality, Closeness centrality, EigenVector centrality, Coreness centrality, Subgraph centrality, PageRank centrality, and LocalRank centrality. Finally, we carry out extensive experiments on multipartite networks with Poisson degree distributions. The experiments indicate that the robustness of multipartite networks could display either discontinuous or continuous phase transitions, depending on the utilized network models. As a multipartite network could be regarded as a simplified multilayer network from the viewpoint of network structures, therefore we apply existing percolation theories that are developed for robustness analysis of multilayer networks to the case of multipartite networks. We show that existing percolation theories are not applicable to multipartite networks. It has been reported that the robustness of a multilayer network deteriorates sharply with the increase of the number of network layers. Surprisingly, we have experimentally found that the robustness a multipartite network does not vary too much with respect to the change of the number of its node sets. The experiments even show that the increase of the number of the node sets could increase the robustness of a multipartite network. Our study suggests that multipartite networks are more robust to attacks than multilayer networks do.

The remainder of this paper is structured as follows. Section 2 presents some preliminaries for better understanding of this work. Section 3 discusses the research motivations. Section 4 demonstrates our empirical method for exploring the robustness of multipartite networks under target node attacks. Section 5 displays the simulation experiments on multipartite networks with Poisson degree distributions and Section 6 concludes the paper.

2. Preliminary

2.1. Complex Network Notations. In the literature, a commonly used method for complex network analytics is to denote a network by a graph which is generally denoted by \( G = (V, E) \) with \( V \) representing the set of nodes and \( E \) the set of edges. The edges between the nodes of \( G \) can be reflected by the adjacency matrix \( A \) of \( G \). The entry \( a_{ij} \) of \( A \) is normally defined as follows:

\[
\begin{cases}
    a_{ij} = 1, & \text{if } e_{ij} \in E, \\
    a_{ij} = 0, & \text{if } e_{ij} \notin E.
\end{cases}
\]

Concerning complex network analytics, one of the most frequently discussed terms is degree. The degree \( d_i \) of node \( i \) is defined as \( d_i = \sum_j a_{ij} \), i.e., \( d_i \) equals the number of edges that have been attached to node \( i \).

2.2. Multipartite Networks. Given a network \( G = (V, E) \). Assume that \( V \) can be divided into \( L \) subsets, i.e., \( V = \{V_1, V_2, \ldots, V_L\} \). If \( \forall a, b \in [1, L], \) \( G \) satisfies the following conditions:

\[
\begin{align*}
    & V_a \cap V_b = \emptyset, & & \text{if } a \neq b, \\
    & a_{ij} \in [0, 1], & & \text{if } i \in V_a \land j \in V_b \land b = a - 1, \\
    & a_{ij} \in [0, 1], & & \text{if } i \in V_a \land j \in V_b \land b = a + 1, \\
    & a_{ij} \equiv 0, & & \text{if } i \in V_a \land j \in V_b, \forall k \in [2, L - 1], \\
    & a_{ij} \equiv 0, & & \text{if } i, j \in V_a,
\end{align*}
\]
then $G$ is called a multipartite network [19, 74].

Note that the subset $V_i$ also can be called a partite set [19, 74]. Thus, a multipartite network with $L$-partite sets is deemed an $L$-partite network. Especially, an $L$-partite network with $L = 2$ is normally termed as a bipartite network [19, 74].

Equation (2) indicates that there is no edge between nodes within the same node set. If we relax this condition, i.e., edges between nodes within the same node set are allowed, then a network with such kind of structure is normally called a multilayer network [43, 44, 82]. Mathematical definitions for multilayer networks can be found in [41, 42].

Figure 1(a) gives a graphical example of a three-layer network which is composed of three networks $G_1$, $G_2$, and $G_3$ (denoted by different colors), while Figure 1(b) presents a graphical example of a multipartite network with three partite sets, i.e., a tripartite network. From the perspective of network structures, we can observe from Figures 1(a) and 1(b) that a multipartite network can be regarded as a simplified multilayer network.

2.3. Network Robustness. Studies on network robustness aim at evaluating the endurance of a network in face of perturbations. In the literature, there are mainly two widely adopted methods for network robustness analysis. Figure 2 explains the main ideas of those two methods.

The method shown in Figure 2(a) pays attention to the fraction $r_{\eta}$ of nonzero degree nodes after removing $q$ fraction of nodes from a focal network. The method shown in Figure 2(b) focuses on the fraction $|\text{LCC}|/N$ of nodes in the largest connected component (LCC) after removing a given fraction $1 - p$ of nodes. The above two methods then, respectively, measure the robustness of a network as follows:

$$
\begin{align*}
R_n &= \sum_{\eta=0}^{1} r_{\eta}, \\
R^\infty &= \frac{|\text{LCC}|}{N},
\end{align*}
$$

where the symbols $R_n$ and $R^\infty$ quantify the robustness of a network. Normally, the larger the values of $R_n$ and $R^\infty$ are, the more robust the network is.

3. Motivations

Network robustness analysis is involved with network models which specify how cascading failures propagate on complex networks. In this paper, we have proposed two network models to explore the robustness of multipartite networks. The reason for developing new models is that existing models that are well studied for multilayer networks are not amenable to multipartite networks.

When exploiting the robustness of multilayer networks, a widely used network model is from [45] which is illustrated in Figure 3. Figure 3 exhibits the dynamic process on a three-layer network with one-to-one correlations, i.e., every node in one subnetwork exactly depends on one node in the other subnetwork. Initially, node 2 of network $G_1$ shown in Figure 3 is attacked. Due to the interdependency, the removal of node 2 leads to the removal of nodes 6 and 10 together with the edges attached to them in step 1. The removal of nodes 6 and 10 further breaks network $G_2$ into two parts. It is assumed that only nodes in the LCC for each subnetwork of a multilayer network will be of interest. Putting it another way, the nodes that are not in the LCC will be regarded as dysfunctional and will be removed. Therefore, in step 2, node 5 together with nodes 1 and 9 (interdependency) is removed. As network $G_3$ fragments into two parts and based on the LCC theory, node 11 or node 12 will be removed (assume that node 11 is removed). Eventually, only nodes 4, 8, and 12 are remained.

In the literature, there are several variants [21, 83–85] of the model shown in Figure 3. However, those models cannot be applied to multipartite networks. The reason is apparent because in those models the focal multilayer network is one-to-one correlated. As we can see from Figure 1 that a multipartite network could be regarded as a special case of a multilayer network with one-to-many correlations.

In order to circumvent the deficiency of the model shown in Figure 3 so as to better characterize real-world networks, Shao et al. and Dong et al. [55, 86] proposed a model exhibited in Figure 4 for analyzing the robustness of multilayer networks with one-to-many correlations. In Figure 4, a node which has no connections with nodes from its coupled network is regarded as a dysfunctional node. Within a network, nodes that are not in the LCC will also be regarded as dysfunctional nodes. Cascading failures will continue on the network until no further failure is possible.

This model displayed in Figure 4 seems very promising for multipartite networks if we neglect the directions of the edges. However, this model is still not applicable to multipartite networks. The reason is that this model shares the same idea with the model presented in Figure 3. More specifically, they consider the LCC for each layer of a multilayer network as each single layer is an independent subnetwork which has its own network structure. By contrast, each “layer” of a multipartite network is not an independent subnetwork as nodes in each “layer” are disconnected from each other. For the models surveyed in
In this paper, we first develop two network models for multipartite networks. Based on the developed models, we then adopt the simulation-based method instead of theoretical methods, especially those represented by percolation theories, to plumb the robustness of multipartite network. The main reason is that existing models for multilayer networks are not amenable to multipartite networks which directly elicits the infeasibility of the applications of the corresponding theoretical methods to multipartite networks, since those theoretical methods are developed based on the corresponding network models.

4. Methodology

4.1. Framework of Robustness Evaluation Method. For a given $L$-partite network $G$, we define $n_i = |V_i|$ as the number of nodes in partite set $V_i$. We utilize Algorithm 1 to evaluate its robustness under target node attacks.

In step 2 of Algorithm 1, for a given centrality metric, we sort the nodes in $V_i$ in a descend order based on their centralities. In case one needs to analyze the robustness of an $L$-partite network under target node attacks that occur to every partite set, then the three variables, i.e., $V^c$, $V$, and $N$, as given in Algorithm 1 should be replaced as $V^c$, $V$, and $N$, respectively.

4.2. Proposed Model M1 for Multipartite Networks. We have illustrated in Section 3 that existing network models are not applicable to analyze the robustness of multipartite networks due to the special structure of multipartite networks. With regard to this, here we first propose network model M1 for multipartite networks.

Figure 5 describes our proposed model M1 for robustness analysis of multipartite networks. For the tripartite network displayed in Figure 5, node 2 is initially attacked. Model M1 takes a multipartite network as a whole. Model
M1 cares about the LCC of a multipartite network after node attacks happened. In step 1, the removal of node 2 breaks the whole network into two parts. Based on the LCC concept, in step 2, all the nodes in red will be removed, and in the end, only the nodes that belong to the LCC of the focal multipartite network are remained.

### 4.3. Proposed Model M2 for Multipartite Networks

Model M2 considers the LCC of each bipartite network contained in a multipartite network. Model M2 eventually calculates the LCC that contains nodes from every partite set of a multipartite network.

Input: an \( L \)-partite network \( G \); index \( i \in [1, L] \)

Output: the robustness curves

1. Implement \( P'_{\infty j} = [\ ] \) for all \( j \in [1, L] \); //memory allocation
2. \( V'_i = \text{NodeRanking}(V_i, \text{centrality}, \text{descend}); //\) see Section 4.4.
3. For \( p = 0 : \text{interval} : 1 \) do
   a. \( G' = \text{NodeRemove}(G, V'_j \cdot (1 - p)n_j); //\) remove the former \( (1 - p)n_j \) nodes from \( V'_j \).
   b. \( G' \leftarrow \text{CascadingFailure}(G', \text{model}); //\) see Sections 4.2 and 4.3.
   c. \( \text{LCC} = \text{LargestConnectedComponent}(G'); \)
   d. Implement \( P'_{\infty j} \leftarrow |V_j \cap \text{LCC}|/n_j \) for all \( j \in [1, L] \); //in the final LCC, calculate the fraction of nodes remained in each node set.
4. End
5. Go to step 2 and repeat the above processes for \( T \) times. Calculate the average values of \( P'_{\infty j} \).
6. Plot \( P'_{\infty j} \) with respect to \( p \).

**Algorithm 1:** Framework of the method for analyzing the robustness of an \( L \)-partite network under target node attacks.

M1 treats a multipartite network as a whole. Model M1 is straightforward and simple since it shares the basic idea with the model that is widely utilized for analyzing the robustness of single-layer networks. Inspired by the existing models established for analyzing the robustness of multilayer networks [16], here we put forward another model, i.e., M2, to describe the dynamic process of multipartite networks to perturbations. Different from model M1, model M2 considers the LCC of each bipartite network contained in a multipartite network. Model M2 eventually calculates the LCC that contains nodes from every partite set of a multipartite network.

Model M2 works in a bounce-forward-and-back manner and assumes that only nodes in the LCC are of concern. Given an \( L \)-partite network with \( V_i \) being its \( i \)-th partite set. Assume that nodes from \( V_i \) for \( i \in [1, L - 1] \) are under attack. Then, model M2 first works in a bounce-forward way. Specifically, model M2 first analyzes the LCC of the bipartite network composed of partite sets \( V_i \) and \( V_{i+1} \) and the edges between them. In the next step, model M2 moves to analyze the bipartite network that contains partite sets \( V_{i+1} \) and \( V_{i+2} \).

![Network model](image)

**Figure 4:** Network model for depicting the cascading failures on a two-layer network (networks A and B) with one-to-many correlations. The directed links are support links. The arrows point from the support nodes to the dependent nodes. (a) Nodes A1 and B6 are initially attacked. (b) Cascading failures on network A. Node A2 is removed because it is disconnected from network A. Node A7 is removed due to the lack of support. The removal of A7 further leads to the failure of node A6 as it is disconnected. (c) Cascading failures on network B. Nodes B1, B2, and B7 are removed as they have no supports. Node B3 is removed as it is disconnected from network B. (d) The LCC of the focal network in the final stable stage.
The above process moves forward until the bipartite network that contains partite sets \( V_{L-1} \) and \( V_L \) is reached and its LCC is identified. Then, model M2 starts to work in a bounce-back manner. Specifically, model M2 analyzes the LCC of the bipartite network composed of partite sets \( V_{L-2} \) and \( V_{L-1} \) and the edges between them. Then, model M2 moves to analyze the bipartite network that contains partite sets \( V_{L-3} \) and \( V_{L-2} \) and the bounce-back process continues until the bipartite network that contains partite sets \( V_L \) and \( V_2 \) is reached and the new start of the bounce-forward process is initiated. The aforementioned bounce-forward-and-back process repeats until a stable stage is reached in which no node and edge removals are possible. The remaining part of the network is then the LCC which model M2 aims to figure out. Note that in the case where nodes from \( V_i \) for \( i = L \) are under attack, then model M2 first implements the bounce-back procedure.

Figure 6 takes the same multipartite network shown in Figure 5 as an example to explain in detail how model M2 works. Initially, node 2 is attacked. The removal of node 2 breaks the bipartite network consisting of nodes in \( V_1 \) and \( V_2 \) into three parts, i.e., \( \{1, 5, 6\} \), \( \{3, 7\} \), and \( \{4, 8\} \). As mentioned earlier, model M2 considers the LCC of each bipartite network contained in a multipartite network, therefore nodes 3, 4, 7, and 8 will be removed in step 1 since they are not in the LCC of the bipartite network. Analogously, in step 2, the nodes that are not in the LCC of the second bipartite network are removed, and eventually, only nodes 1, 6, and 10 survive (also could be nodes 1, 5, and 9).

### 4.4. Node Centrality Metrics

Note that, for real-world complex networks, nodes with higher significance have higher probabilities to be attacked. When investigating the robustness of multipartite networks under target node attacks, one therefore may wish to rank the nodes of a multipartite network based on their significance such that one can choose the nodes to be removed. In network science domain, centrality metrics have been widely used to measure the significance of the nodes in a network. In the literature, there are a handful of node centrality metrics [87]. In this paper, we only choose eight of them. On the one hand, the adopted metrics are widely investigated in the literature. On the other hand, they are computationally friendly. The adopted centrality metrics are described below.

#### 4.4.1. Degree Centrality

The Degree centrality of node \( i \) is calculated as follows:

\[
C_{\text{deg}}(i) = d_i = \sum_{j=1}^{N} a_{ij}.
\]  

#### 4.4.2. Betweenness Centrality

The Betweenness centrality of node \( i \) is calculated as follows:

\[
C_{\text{btw}}(i) = \sum_{s \neq i \neq t} \frac{p_{st}}{p_{st}}.
\]
where $p_{it}$ denotes the number of shortest paths from two different nodes $s$ and $t$ in $G$ and $p^i_{st}$ represents the number of paths in $p_{st}$ that have passed through node $i$.

4.4.3. Closeness Centrality. The Closeness centrality of node $i$ is measured as follows:

$$C_{cl}^i = \frac{N - 1}{\sum_{j \neq i} d_{ij}}, \quad (6)$$

where $d_{ij}$ denotes the geodesic distance between nodes $i$ and $j$.

4.4.4. EigenVector Centrality. The EigenVector centrality of node $i$ is figured out by solving the following equation:

$$\overrightarrow{x} = cA\overrightarrow{x}, \quad (7)$$

where vector $\overrightarrow{x} = (C_{c1}^i, C_{c2}^i, \ldots, C_{cn}^i)$ and $c$ is a proportionality constant which is generally set to $c = 1/\lambda$ with $\lambda$ being the largest eigenvalue of $A$.

4.4.5. Coreness Centrality. The Coreness centrality of node $i$ is figured out by implementing the $k$-shell [88, 89] decomposition of $G$ and $C_{cor}^i = k$ for all the nodes in the $k$-shell.

4.4.6. Subgraph Centrality. The Subgraph centrality of node $i$ is calculated as follows:

$$C_{sub}^i = \sum_{\alpha=1}^{\infty} \frac{(A^\alpha)_{ii}}{\alpha!}, \quad (8)$$

where $(A^\alpha)_{ii}$ stands for the diagonal element of the $\alpha$th power of $A$.

4.4.7. PageRank Centrality. The PageRank centrality of node $i$ at step $t$ is calculated as follows:

$$C_{pr}^i(t) = \sum_{j=1}^{N} a_{ij} C_{pr}^j(t-1) + \frac{1}{N} (1 - \beta), \quad (9)$$

where $\beta$ is a random jumping probability and is set to $\beta = 0.85$ in this study. The above process will stop once a steady state is reached and all the $C_{pr}^i$ values are obtained.

4.4.8. LocalRank Centrality. The LocalRank centrality of node $i$ is calculated as follows:

$$C_{lr}^i = \sum_{j \in N(i)} \sum_{t \in N(j)} R(t), \quad (10)$$

where $N(i)$ denotes the neighbouring nodes of node $i$ and $R(t)$ represents the number of node $t$’s neighbours and their neighbours’ neighbours.

5. Simulations

5.1. Experimental Settings. For the sake of testing purpose, in the experiments we generate multipartite networks with controllable Poisson degree distributions. Let us define a probability vector $\bar{p} = (p_1, p_2, \ldots, p_{L-1})$. Then, we generate an $L$-partite network with $N = \sum n_i$ nodes by connecting each node $a \in V_i$ with each node $b \in V_{i+1}$ with the probability $p_i$ for all $i \in [1, L - 1]$.

It is easy to figure out that the degree distribution $P_{i+1} (k)$ of the nodes in $V_i$ that have connections with nodes in $V_{i+1}$ follows the Poisson distribution which can be formulated as

$$P_{i+1} (k) \approx e^{-(k_{i+1})} \frac{(k_{i+1})^k}{k!}, \quad (11)$$

with its mean degree $\langle k_{i+1} \rangle = n_{i+1} p_i$. Analogously, it is easy to get

$$P_{i+1} (k) \approx e^{-(k_{i+1})} \frac{(k_{i+1})^k}{k!}, \quad (12)$$

with the corresponding mean degree $\langle k_{i+1} \rangle = n_{i+1} p_i$.

In the simulations, without loss of generality, we generate a tripartite network $G_t$ with its parameter settings being given as follows: $(n_1, n_2, n_3) = (1.5, 1.5, 1) \times 10^6$, $\bar{p} = (6/ (n_1 + n_2), 4/ (n_1 + n_3))$. During the simulations, the settings of the parameters interval and $T$ as presented in Algorithm 1 are interval $= 0.04$ and $T = 100$. We also generate $G_t$ for 5 times. Therefore, all the results are averaged over 500 times.

5.2. Robustness Based on Network Model M1. For a tripartite network $G_t$, we, respectively, investigate its robustness under three different cases, i.e., the case that the node removal happens to the first partite set $V_1$, the case that the node removal happens to the second partite set $V_2$, and the case that the node removal happens to every partite set. We first calculate the centralities of the nodes in $G_t$ given a specific centrality metric. For each case scenario, we then sort the corresponding nodes in a descend order. Afterward, for a given value of $p_c$, we remove the former $1 - p$ fraction of nodes from the corresponding node set. We then let the cascading failures propagate with respect to model M1. When $G_t$ reaches a stable state where no node and edge removals are possible, we can calculate the values of $P_{sc}$ and $P_{cs}$. The simulation results are exhibited in Figure 7.

Note that an important indicator for network robustness analysis is the critical point $p_c$ of $p$ at which the value of $P_{sc}$ starts to change from a small value close to zero to a relatively large value. The smaller the value of $p_c$ is, the more robust the network is. We can clearly see from Figures 7(a)–7(c) that $p_c = 0$, which indicates that the studied multipartite networks are extremely robust to targeted attacks if the node attacks only occur to $V_1$. Figures 7(d)–7(f) show that the values of $p_c$ are approximately in the range $p_c \in [0.4, 0.7]$. While Figures 7(g)–7(i) indicate that the values of $p_c$ are approximately in the range $p_c \in [0.9, 0.7]$. The results recorded in Figure 7 suggest that the robustness of multipartite networks based on the network model M1 presents a continuous phase transition phenomenon, which indicates that multipartite networks are
robust when model M1 is considered. As for the eight investigated node centrality metrics, we can see from Figures 7(a)–7(f) that the robustness curves are close to each other when the attacks only happen to one partite set, which indicates that their impacts on the networks’ robustness are not significant. When the attacks happen to every partite set of a multipartite network, we can see from Figures 7(g)–7(i) that a multipartite network is relatively more fragile with respect to the Degree and PageRank centralities. By observing Figure 7, we also notice that the EigenVector centrality has the least impact on the robustness of multipartite networks to target node attacks.

Figure 7: Model M1-based robustness of tripartite network $G_1$ subject to target node attacks. The fractions $P^\infty_i$, i.e., fractions of nodes in $V_i \subseteq G_1$ that also belong to the LCC, are drawn with respect to different values of $p$. (a–c) the case where the node attacks occur to $V_1$. (d–f) the case where the node attacks occur to $V_2$. (g–i) the case where the node attacks occur to the whole network.
5.3. Robustness Based on Network Model M2. Analogous to what are done in the above subsection, we here study the robustness of tripartite network $G_1$ subject to target node attacks with respect to the network model M2. Figure 8 presents the simulation results.

It can be observed from the robustness curves drawn in Figure 8 that there exist drastic jumps of the values of $P_i^\infty$, i.e., at the critical points of $p_c$, the values of $P_i^\infty$ suddenly change from some small values close to zero to some large values. The results shown in Figures 8(a)–8(c) indicate that even small scale attacks could break down the studied multipartite networks. The values of $p_c$ as recorded in Figure 8 are relatively larger than those recorded in Figure 7. Different to what are shown in Figure 7, the values of $p_c$ do not vary too much with regard to the three node attack strategies. The results shown in Figure 8 display discontinuous phase transition, which indicates that multipartite networks are extremely vulnerable in the face of target attacks when the network model M2 is considered.

As for the eight investigated node centrality metrics, the experiments demonstrated in Figures 8(g)–8(i) indicate that if the node attacks occur to every partite set, their impacts on the robustness of multipartite networks are tinnier as the curves are very close to each other, which is different from the phenomenon observed in Figure 7. Meanwhile, we notice from Figure 8 that the Coreness centrality has the least impact on the robustness of multipartite networks to target node attacks when model M2 is considered. Moreover, a multipartite network is relatively more vulnerable with respect to the Degree and LocalRank centralities.

5.4. Discussion on Network Robustness. The above experiments on L-partite networks are carried out in the case of $L = 3$. One may argue the generalization of the robustness phenomena observed from the above experiments. With regard to this, here we carry out experiments for the case of $L > 3$. As indicated by the above experiments that the effects of the eight centrality metrics on the network robustness are not so significant, here we therefore choose the Degree centrality for testing purpose.

Figure 9 demonstrates the robustness experiments on four multipartite networks whose sizes are controlled by the parameter $L$. It can be seen from Figure 9 that the impacts of $L$ on the robustness of multipartite networks with respect to network models M1 and M2 are not significant since the robustness curves are close to each other. In the literature, it has been reported that the robustness of multilayer networks decreases sharply with the increase of $L$ [14]. However, by contrast, Figure 9 indicates that the robustness of multipartite networks with respect to network models M1 and M2 does not change sharply with respect to $L$. Surprisingly, the robustness curves recorded in Figure 9 indicate that the robustness of multipartite networks increases with the increase of $L$.

One may observe from Figure 9(b) that the robustness curves show some bumps for $p \in [0.3, 0.5]$. The bumps are caused by the relatively small number of experimental trials which is set to be 500. For a given multipartite network with $L$ node sets, in the experiments we set $n_i = n_j = 4 \times 10^4$ for all $i, j \in [1, L]$. For $L = 4$, we can see from Figure 9(b) that the robustness curve does not show any bump. With the increase of $L$, the generated L-partite networks are becoming larger, while the number of experimental trials is fixed to be 500. The larger the size of an L-partite network, the larger the size of the corresponding bump, and this is what has been reflected in Figure 9(b). The bumps will disappear with the increase of the number of experimental trials.

In the above experiments, we have fixed $p_i$ and $p_j$, i.e., the degree of nodes in each partite set is fixed. Here, we investigate the impacts of degree on the robustness of multipartite networks. For simplicity and without loss of generality, we in the experiments study the case of $L = 3$. Figure 10 exhibits the impact of degree on the robustness of a tripartite network. Figure 10 apparently demonstrates the continuous and discontinuous phase transition phenomena on the robustness of multipartite networks. The robustness curves drawn in Figure 10 indicate that the larger the degree of a multipartite network is, the more robust the network is in face of target attacks.

5.5. Discussion on Percolation Theories. Note that this paper adopts the empirical method to investigate the robustness of multipartite networks. The motivation has been clarified in Section 3. Based on the assertion that a multipartite network is practically a simple case of a multilayer network, one therefore may argue that existing percolation theories for analyzing the robustness of multilayer networks could be applied to multipartite networks. Here, we will prove that this idea is not working.

One could see from Figure 5 that the network model M1 practically regards a multipartite network as a whole. Therefore, if the node attacks occur to every partite set of a multipartite network, then percolation theory for single-layer networks [3] might be possible for analyzing the robustness of multipartite networks. As the majority of existing percolation theories for analyzing the robustness of networks deal with random node attack scenarios, in the following we only pay attention to network robustness under random node attacks.

Given a single-layer network $G$, let $P(k)$ be its degree distribution. When we randomly remove $1 - p$ fraction of nodes from $G$, the remaining fraction of nodes in the LCC can be mathematically calculated as follows:

$$P^c_i = p(1 - G_0(u)),$$

where $G_0(u) = \sum_{k=0}^{\infty} P(k) u^k$ is the generating function of $P(k)$. The variable $u$ is calculated as follows:

$$u = 1 - p + pG_1(u),$$
where $G_1(u) = G_0'(u)/G_0(1)$ is the excess generating function of $P(k)$ with $G_0'(u)$ being the first-order derivative of $G_0(u)$. For an $L$-partite network $G_L$ generated in the way shown in this paper, we can easily work out the degree distribution $P_i(k)$ for the nodes in $V_i$ as follows:
\( P_i(k) = \left( \frac{n_a}{q} \right) p_a^q (1 - p_a)^{n_a - q} \left( \frac{n_b}{k - q} \right) p_b^{k - q} (1 - p_b)^{n_b - k + q} \approx \frac{\langle k_i \rangle^k}{k!} e^{-\langle k_i \rangle}, \)  

(15)

where \( \langle k_i \rangle = \langle k_{i,a} \rangle + \langle k_{i,b} \rangle \) and \( a = i - 1 \) and \( b = i + 1 \).

Based on the above equation, we can further figure out the degree distribution \( P(k) \) of \( G_1 \) as follows:

\[
P(k) \approx \sum_{i=1}^{L} \frac{n_i}{N} P_i(k). \tag{16}
\]

In compliance with the percolation theory formulated in equations (13) and (14), we can have the following simplified formula for multipartite networks:
Figure 11: Validation of the correctness of the application of existing percolation theory for single-layer networks to multipartite networks. (a) Simulations on multipartite networks where each multipartite network has equal number of nodes for each partite set. (b) Simulations on bipartite networks where the number of nodes for each partite set of the focal network is controlled by parameter $\alpha$.

Note that the theoretical results shown in Figure 11(a) are obtained based on two conditions, i.e., $n_i = n_j$ and node failures occur to every partite set of the focal network. To further check the correctness of equations (17) and (18), we investigate the condition where $n_i \neq n_j$. Specifically, for network $G_1$, we introduce parameter $\alpha$ to control the number of nodes for its two node sets, i.e., we set $\alpha = n_j/(n_i + n_j)$. We fix $N = 4 \times 10^4$ for $G_1$, and we test the correctness of equations (17) and (18) for $\alpha = \{1/8, 2/8, 4/8\}$. The corresponding experiments are presented in Figure 11(b). We can clearly see from Figure 11(b) that the theoretical results obtained by equations (17) and (18) do not comply with the simulation results if $n_i \neq n_j$. We conclude that the existing percolation theory for single-layer networks only applies to multipartite networks where the focal multipartite network has equal number of nodes for each partite set and the node failures occur to every partite set.

As for the network model M2, the robustness analysis of multipartite networks based on model M2 shares something in common with the work presented in [55]. Let us consider a multipartite network $G_1$ with $L = 3$ and $n_i = n_j$. If we take the bipartite network consisting of partite sets $V_3$ and $V_2$ as a whole, then network $G_1$ therefore could be regarded as a special multilayer network that is similar to the network model investigated in [55]. One thus might argue that the percolation theory developed in [55] could be applicable to multipartite networks.

Given a two-layer network (consisting of networks A and B) as discussed in [55], when randomly removing $1 - p_A$ and $1 - p_B$ fractions of nodes, respectively, from A and B, the corresponding percolation theory is formulated as follows:

$$P^\infty = P\left(1 - \sum_{i=1}^{L} \frac{n_i}{N} G_i(u)\right) = P\left(1 - \sum_{i=1}^{L} \frac{n_i}{N} e^{\langle k_i \rangle (u-1)}\right),$$

(17)

$$u = 1 - p + pG_1(u) = 1 - p + p \sum_{i=1}^{L} G_i(u) G_0(1)$$

(18)

where we have made use of the following expression to simplify the above derivations:

$$G_i(u) = \sum_{k=0}^{\infty} P_i(k)u^k = \sum_{k=0}^{\infty} \langle k_i \rangle^k e^{-\langle k_i \rangle} u^k$$

(19)

In what follows, we will check the correctness of equations (17) and (18) through experiments on multipartite networks. To do so, we generate four multipartite networks $G_1$, $G_2$, $G_3$, and $G_4$. For the four networks, we fix $p_i = p_j = d/2n_j$, $n_i = n_j = 4 \times 10^4$, and $d = 6$. We, respectively, set $L = 2$, $L = 3$, $L = 4$, and $L = 5$ for $G_1$, $G_2$, $G_3$, and $G_4$.

Figure 11(a) exhibits the simulation results on the robustness of networks $G_1$, $G_2$, $G_3$, and $G_4$ as well as the theoretical results obtained by solving equations (17) and (18). It can be seen from Figure 11(a) that the simulation results coincide well with the theoretical results.
we then could figure out the solutions to $P_{A}^{\infty}$ and $P_{B}^{\infty}$ by numerically solving the following equations:

$$
\begin{align*}
P_{A}^{\infty} &= p \left( 1 - e^{-(d_2/2)P_{B}^{\infty}} \right), \\
P_{B}^{\infty} &= (1 - e^{-(d_2/2)P_{A}^{\infty}})(1 - e^{-(d_2/2)P_{B}^{\infty}}).
\end{align*}
$$

(22)

Figure 12 exhibits the simulation results on the robustness of networks $G_1$ as well as the theoretical results obtained by solving equation (21). We get $P_{A}^{\infty}$ through expression $P^{\infty} = (P_{A}^{\infty} + 2P_{B}^{\infty})/3$. It can be clearly seen from Figure 12 that the theory does not apply to multipartite networks.

### 6. Conclusions

Complementary to existing studies on the robustness of multilayer networks, in this work we investigate the robustness of multipartite networks under target node attacks. To do so, two network models, i.e., M1 and M2, have been developed for describing the dynamic process of a multipartite network subject to node failures. Afterward, for a multipartite network, we rank its nodes with respect to eight node centrality metrics. Then, we remove $1 - p$ fraction of the sorted nodes and, respectively, calculate the fraction of nodes in the LCC based on models M1 and M2. Experiments on multipartite networks with Poisson degree distributions reveal that the robustness of multipartite networks with respect to models M1 and M2, respectively, displays continuous and discontinuous phase transitions. Experiments also discover that higher degrees and larger number of node sets of multipartite networks could improve their robustness to target node failures.

Percolation theories are well studied for analyzing the robustness of multilayer networks. Because a multipartite network could be regarded as a simple case of an interdependent network with one-to-many correlations, therefore theories developed in [21, 81] might be applicable to multipartite networks. However, in this paper, we have proved that those theories are not feasible for multipartite networks. How to develop theories for analyzing the robustness of multipartite networks is still challenging. We are positive that this work could provide clues for future theories for robustness analysis of multipartite networks.

A myriad of real-world networks are reported to be scale-free [90–94]. However, in the experiments, only multipartite networks with mixed Poisson degree distributions are tested. The reason is that sampling multipartite networks with power-law degree distributions still remains a challenging issue [95–97]. Let us cite a bipartite network as an example. Let $k_i$ and $d_i$, respectively, be the degree of a node in $V_1$ and $V_2$. Therefore, when sampling a bipartite network with power-law distributions, one needs to consider the constraint $\sum k_i = \sum d_i$. One more thing is that one needs to consider the graphicality condition [98] when sampling multipartite networks with power-law degree distributions. How to sample multipartite networks with arbitrary degree distributions is also challenging and deserves further in-depth dedications [99–101].

The robustness phenomena observed on multipartite networks indicate that multipartite networks are more...
robust to perturbations than multilayer networks do. Note that this conclusion is drawn based on the established models M1 and M2 which are based on the largest connected component theory. During the robustness analysis, the models assume that nodes outside the largest connected component will be dysfunctional and removed. For some real-world complex networks, nodes outside the largest connected components will still be functioning, and models M1 and M2 therefore may not be applicable to such real-world multipartite networks. However, the findings of this work still provide a new thinking towards the robust structure design of complex systems.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] Y. Yang, T. Nishikawa, and A. E. Motter, “Small vulnerable sets determine large network cascades in power grids,” Science, vol. 358, no. 6365, p. 3184, 2017.
[2] X.-H. Li, P. L. Chavali, and M. M. Babu, “Capturing dynamic protein interactions,” Science, vol. 359, no. 6380, pp. 1105-1106, 2018.
[3] M. E. J. Newman, Networks: An Introduction, Oxford University Press, Oxford, UK, 2010.
[4] Y.-Y. Liu, J.-J. Slotine, and A.-L. Barabási, “Controllability of complex networks,” Nature, vol. 473, no. 7346, pp. 167–173, 2011.
[5] J. Gao, Y.-Y. Liu, R. M. D’soouza, and A.-L. Barabási, “Target control of complex networks,” Nature Communications, vol. 5, no. 5415, 2014.
[6] A. Vinayagam, T. E. Gibson, H.-J. Lee et al., “Controllability analysis of the directed human protein interaction network identifies disease genes and drug targets,” Proceedings of the National Academy of Sciences, vol. 113, no. 18, pp. 4976–4981, 2016.
[7] J. G. T. Zañudo, G. Yang, and R. Albert, “Structure-based control of complex networks with nonlinear dynamics,” Proceedings of the National Academy of Sciences, vol. 114, no. 28, pp. 7234–7239, 2017.
[8] S. L. Brunton, J. L. Proctor, and J. N. Kutz, “Discovering governing equations from data by sparse identification of nonlinear dynamical systems,” Proceedings of the National Academy of Sciences, vol. 113, no. 15, pp. 3932–3937, 2016.
[9] N. Pržulj and N. Malod-Dognin, “Network analytics in the age of big data,” Science, vol. 353, no. 6295, pp. 123–124, 2016.
[10] M. E. J. Newman, “Network structure from rich but noisy data,” Nature Physics, vol. 14, no. 6, pp. 542–545, 2018.
[11] Z. Li and L. Chen, “Robustness of multiparticle networks in face of random node failure,” Chaos, Solitons & Fractals, vol. 121, pp. 149–159, 2019.
[12] H. A. Malik, F. Abid, M. R. Wahiddin, and Z. Bhatti, “Robustness of dengue complex network under targeted versus random attack,” Complexity, vol. 2017, Article ID 2515928, 12 pages, 2017.
[13] L. Fraccascia, I. Giannoccaro, and V. Albino, “Resilience of complex systems: state of the art and directions for future research,” Complexity, vol. 2018, Article ID 3421529, 44 pages, 2018.
[14] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, “Networks formed from interdependent networks,” Nature Physics, vol. 8, no. 1, pp. 40–48, 2012.
[15] A. Bashan, Y. Berezin, S. V. Buldyrev, and S. Havlin, “The extreme vulnerability of interdependent spatially embedded networks,” Nature Physics, vol. 9, no. 10, pp. 667–672, 2013.
[16] Q. Cai, S. Alam, and J. Liu, “On the robustness of complex systems with multipartitivity structures under node attacks,” IEEE Transactions on Control of Network Systems, vol. 7, 2019.
[17] M. E. J. Newman, A.-L. Barabási, and D. J. Watts, The Structure and Dynamics of Networks, Princeton University Press, Princeton, NJ, USA, 2011.
[18] A. Vespignani, “The fragility of interdependency,” Nature, vol. 464, no. 7291, pp. 984-985, 2010.
[19] X. Liu, H. E. Stanley, and J. Gao, “Breakdown of interdependent directed networks,” Proceedings of the National Academy of Sciences, vol. 113, no. 5, pp. 1138–1143, 2016.
[20] I. Giannoccaro, V. Albino, and A. Nair, “Advances on the resilience of complex networks,” Complexity, vol. 2018, Article ID 8756418, 3 pages, 2018.
[21] X.-L. Ren, N. Gleinig, D. Tolić, and N. Antulov-Fantulin, “Underestimated cost of targeted attacks on complex networks,” Complexity, vol. 2018, Article ID 9826243, 15 pages, 2018.
[22] J. A. Dunne, R. J. Williams, and N. D. Martinez, “Network structure and biodiversity loss in food webs: robustness increases with connectance,” Ecology Letters, vol. 5, no. 4, pp. 558–567, 2002.
[23] J. M. Montoya, S. L. Pimm, and R. V. Solé, “Ecological networks and their fragility,” Nature, vol. 442, no. 7100, pp. 259–264, 2006.
[24] X. Yuan, Y. Hu, H. E. Stanley, and S. Havlin, “Eradicating catastrophic collapse in interdependent networks via reinforced nodes,” Proceedings of the National Academy of Sciences, vol. 114, no. 13, pp. 3311–3315, 2017.
[25] C. Liu, J. Liu, and Z. Jiang, “A multiobjective evolutionary algorithm based on similarity for community detection from signed social networks,” IEEE Transactions on Cybernetics, vol. 44, no. 12, pp. 2274–2287, 2014.
[26] M. Zhou and J. Liu, “A two-phase multiobjective evolutionary algorithm for enhancing the robustness of scale-free networks against multiple malicious attacks,” IEEE Transactions on Cybernetics, vol. 47, no. 2, pp. 539–552, 2017.
[27] D. Li, B. Fu, Y. Wang et al., “Percolation transition in dynamical traffic network with evolving critical bottlenecks,” Proceedings of the National Academy of Sciences, vol. 112, no. 3, pp. 669–672, 2015.
[28] H. Zhang, E. Fata, and S. Sundaram, “A notion of robustness in complex networks,” IEEE Transactions on Control of Network Systems, vol. 2, no. 3, pp. 310–320, 2015.
[29] M. Di Muro, C. La Rocca, H. Stanley, S. Havlin, and L. Braunstein, “Recovery of interdependent networks,” Scientific Reports, vol. 6, no. 22834, 2016.
[30] J. Kim and K.-H. Cho, “Robustness analysis of network modularity,” IEEE Transactions on Control of Network Systems, vol. 3, no. 4, pp. 348–357, 2016.
[31] D. Zelazo and M. Burger, "On the robustness of uncertain consensus networks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 2, pp. 170–178, 2017.

[32] X. Huang, S. Shao, H. Wang, S. V. Buldyrev, H. Eugene Stanley, and S. Havlin, "The robustness of interdependent clustered networks," *EPL (Europhysics Letters)*, vol. 101, no. 1, p. 18002, 2013.

[33] M. Gong, L. Ma, Q. Cai, and L. Jiao, "Enhancing robustness of coupled networks under targeted recoveries," *Scientific Reports*, vol. 5, p. 8439, 2015.

[34] Y. Berezin, A. Bashan, M. M. Danziger, D. Li, and S. Havlin, "Localised attacks on spatially embedded networks with dependencies," *Scientific Reports*, vol. 5, p. 8934, 2015.

[35] Y. Shang, "Localised recovery of complex networks against failure," *Scientific Reports*, vol. 6, no. 30521, 2016.

[36] L. M. Shekhtman, M. M. Danziger, and S. Havlin, "Recent advances on failure and recovery in networks of networks," *Chaos, Solitons & Fractals*, vol. 90, pp. 28–36, 2016.

[37] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, "Network robustness and fragility: percolation on random graphs," *Physical Review Letters*, vol. 85, no. 25, pp. 5468–5471, 2000.

[38] D. Achlioptas, R. M. D’Souza, and J. Spencer, "Explosive percolation in random networks," *Science*, vol. 323, no. 5920, pp. 1453–1455, 2009.

[39] R. A. da Costa, S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, "Explosive percolation transition is actually continuous," *Physical Review Letters*, vol. 105, no. 25, p. 255701, 2010.

[40] G. Bianconi, "Dangerous liaisons?", *Nature Physics*, vol. 10, no. 10, pp. 712–714, 2014.

[41] S. Boccaletti, G. Bianconi, R. Criado et al., "The structure and dynamics of multilayer networks," *Physics Reports*, vol. 544, no. 1, pp. 1–122, 2014.

[42] M. Kivelä, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter, "Multilayer networks," *Journal of Complex Networks*, vol. 2, no. 3, pp. 203–271, 2014.

[43] M. De Domenico, A. Solé-Ribalta, E. Omelède, S. Gómez, and A. Arenas, "Ranking in interconnected multilayer networks reveals versatile nodes," *Nature Communications*, vol. 6, p. 6868, 2015.

[44] M. De Domenico, V. Nicosia, A. Arenas, and V. Latora, "Structural reducibility of multilayer networks," *Nature Communications*, vol. 6, p. 6864, 2015.

[45] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[46] F. Radicchi and C. Castellano, "Breaking of the site-bond percolation universality in networks," *Nature Communications*, vol. 6, no. 10196, 2015.

[47] Y. Hu, B. Ksherim, R. Cohen, and S. Havlin, "Percolation in interdependent and interconnected networks: abrupt change from second-to first-order transitions," *Physical Review E*, vol. 84, no. 6, p. 066116, 2011.

[48] S. Xiao, G. Xiao, T. H. Cheng, S. Ma, X. Fu, and H. Soh, "Robustness of scale-free networks under rewiring operations," *EPL (Europhysics Letters)*, vol. 89, no. 3, p. 38002, 2010.

[49] A. Zeng and W. Liu, "Enhancing network robustness against malicious attacks," *Physical Review E*, vol. 85, no. 6, p. 066130, 2012.

[50] C. M. Schneider, N. Yazdani, N. A. Araújo, S. Havlin, and H. J. Herrmann, "Towards designing robust coupled networks," *Scientific Reports*, vol. 3, p. 2013, 2016.

[51] X. Tang, J. Liu, and M. Zhou, "Enhancing network robustness against targeted and random attacks using a memetic algorithm," *EPL (Europhysics Letters)*, vol. 111, no. 3, p. 38005, 2015.

[52] W. Liu, M. Gong, S. Wang, and L. Ma, "A two-level learning strategy based memetic algorithm for enhancing community robustness of networks," *Information Sciences*, vol. 422, pp. 290–304, 2018.

[53] W. Yuming, C. Si, P. Chengsheng, and C. Bo, "Measure of invulnerability for command and control network based on mission link," *Information Sciences*, vol. 426, pp. 148–159, 2018.

[54] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proceedings of the National Academy of Sciences*, vol. 108, no. 10, pp. 3838–3841, 2011.

[55] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Cascade of failures in coupled network systems with multiple support-dependence relations," *Physical Review E*, vol. 83, no. 3, Article ID 036116, 2011.

[56] M. J. O. Pocock, D. M. Evans, and J. Memmott, "The robustness and restoration of a network of ecological networks," *Science*, vol. 335, no. 6071, pp. 973–977, 2012.

[57] S. Shao, X. Huang, H. E. Stanley, and S. Havlin, "Percolation of localized attack on complex networks," *New Journal of Physics*, vol. 17, no. 2, p. 023049, 2015.

[58] L.-W. Kong, M. Li, R.-R. Liu, and B.-H. Wang, "Percolation on networks with weak and heterogeneous dependency," *Physical Review E*, vol. 95, no. 3, Article ID 032301, 2017.

[59] R.-R. Liu, D. A. Eisenberg, T. P. Seager, and Y.-C. Lai, "The weak interdependence of infrastructure systems produces mixed percolation transitions in multilayer networks," *Scientific Reports*, vol. 8, no. 1, p. 2111, 2018.

[60] C. N. Kaiser-Bunbury, S. Muff, J. Memmott, C. B. Müller, and A. Callisch, "The robustness of pollination networks to the loss of species and interactions: a quantitative approach incorporating pollinator behaviour," *Ecology Letters*, vol. 13, no. 4, pp. 442–452, 2010.

[61] P. P. A. Staniczenko, O. T. Lewis, N. S. Jones, and F. Reed-Tsochas, "Structural dynamics and robustness of food webs," *Ecology Letters*, vol. 13, no. 7, pp. 891–899, 2010.

[62] A. Valiente-Banuet, M. A. Aizen, J. M. Alcántara et al., "Beyond species loss: the extinction of ecological interactions in a changing world," *Functional Ecology*, vol. 29, no. 3, pp. 299–307, 2015.

[63] D. M. Evans, J. O. Pocock, and J. Memmott, "The robustness of a network of ecological networks to habitat loss," *Ecology Letters*, vol. 16, no. 7, pp. 844–852, 2013.

[64] T. A. Revilla, F. Encinas-Viso, and M. Loreau, "Robustness of mutualistic networks under phenological change and habitat destruction," *Oikos*, vol. 124, no. 1, pp. 22–32, 2015.

[65] Q. Cai and J. Liu, "The robustness of ecosystems to the species loss of community," *Scientific Reports*, vol. 6, Article ID 035904, 2016.

[66] Z. Wang, D. Zhou, and Y. Hu, "Group percolation in interdependent networks," *Physical Review E*, vol. 97, no. 3, Article ID 032306, 2018.

[67] P. T. J. Johnson, J. C. De Roode, and A. Fenton, "Why infectious disease research needs community ecology," *Science*, vol. 349, no. 6252, Article ID 1259504, 2015.
