Breakup of directed multipartite networks

Cai, Qing; Pratama, Mahardhika; Alam, Sameer; Ma, Chunyao; Liu, Jiming

2019

Cai, Q., Pratama, M., Alam, S., Ma, C., & Liu, J. (2020). Breakup of directed multipartite networks. IEEE Transactins on Network Science and Engineering, 7(3), 947-960. doi:10.1109/TNSE.2019.2894142

https://hdl.handle.net/10356/144369

https://doi.org/10.1109/TNSE.2019.2894142

Breakup of Directed Multipartite Networks

Qing Cai, Mahardhika Pratama, Sameer Alam, Chunyao Ma, and Jiming Liu, *Fellow, IEEE*

Abstract—A complex network in reality often consists of profuse components each of which may suffer from unpredictable perturbations. Because the components of a network could be interdependent, therefore the failures of some components may trigger catastrophes to the whole network. It is thus pivotal to exploit the robustness of complex networks to perturbations. Existing studies on network robustness mainly deal with interdependent or multilayer networks, little work is done to investigate the robustness of multipartite networks which are an indispensable part of complex networks. Here we plumb the robustness of directed multipartite networks. To be specific, we exploit the robustness of bi-directed and unidirectional multipartite networks in face of random node failures. We respectively establish cascading and non-cascading models based on the largest connected component concept for depicting the dynamical processes on bi-directed and unidirectional multipartite networks subject to random node attacks. Based on our developed models, we respectively derive the corresponding percolation theories for mathematicaly computing the robustness of directed multipartite networks to random node failures. We theoretically unravel the first-order and second-order phase transition phenomena on the robustness of directed multipartite networks. The correctness of our developed theories coincide quite well with simulations on computer-generated multipartite networks.

Index Terms—Complex networks, directed multipartite networks, network robustness, percolation, largest connected component

1 Introduction

Complex systems are ubiquitous in our daily life [1]. The form of a complex system ranges from the macroscopic level like the power grid systems [2], to the microscopic level like the metabolic systems [3]. A complex system in real world is usually composed of countless components, which makes it difficult to be controlled [4]. With the advent of network science, the situation of system control has been significantly improved by modeling a complex system as a network composed of vertices and edges where the vertices represent the system components while edges denote the relationships between components [5, 6]. Network modeling has been proved to be an effective instrument not only for system control [7–10] but also for data science [11, 12].

Due to the fact that the components of a complex system may suffer from internal and/or external perturbations which may induce the breakdown of the whole system, an effective method for predicting system stability so as to avoid potential catastrophe is therefore imperative [13–16]. As a consequence, network robustness analysis has emerged and is gaining momentum [17–20].

1.1 Previous Work

Network robustness analysis aims to investigate how robust a network is in face of perturbations. To this end, tremendous efforts have been made along this line. Because the perturbations could occur to vertices and/or edges of a network, existing studies thus can be categorized into three groups, i.e., vertex level [17, 21–23] (Fig. 1(a)), edge level [19, 24–26] (Fig. 1(b)), and mixed level [27–31] (Fig. 1(c)), with their main ideas literally self-explained. From the perspective of perturbation manners, existing studies can be roughly classified as: network robustness to random failure [21] (every vertex is given the same probability to be attacked) and network robustness to target attacks [22, 32–34] (the probability for a vertex to be attacked depends on the importance of the focal vertex, see Fig. 1(d)). If the methods for analyzing network robustness are of concern, existing studies therefore could be archived into two groups: simulations based studies [17, 33, 35] (the curve in Fig. 1(e) is obtained by simulations) and theoretical analysis [19, 23, 36] (the curve in Fig. 1(e) is obtained by theoretical computing).

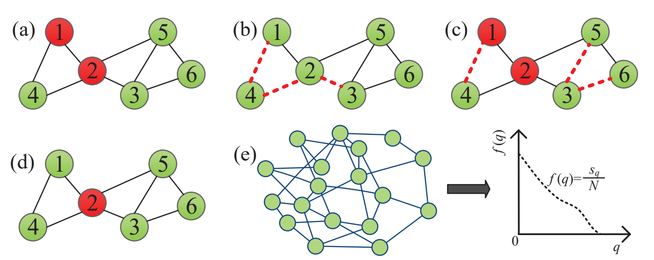


Fig. 1. Graphical examples of existing studies for network robustness analysis. (a) vertex level analysis. (b) edge level analysis. (c) mixed level analysis. (d) robustness to target attacks. (e) simulation based or theoretical analysis.

Due to the fact that a real-world network normally consists of many sub-networks which are interdependent, existing studies therefore can be divided into two branches, i.e., robustness of a single network [18] and robustness of interdependent networks [21, 23, 36, 37]. It has been discovered that a single network could be robust to perturbations

- Q. Cai and M. Pratama are with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. E-mail: mpratama@ntu.edu.sg.
- S. Alam and C. Ma are with the School of Mechanical and Aerospace Engineering, Nanyang Technological University, Singapore. E-mail: sameeralam@ntu.edu.sg.
- J. Liu is with the Department of Computer Science, Hong Kong Baptist University, Hong Kong . E-mail: jiming@comp.hkbu.edu.hk.

(the curve in Fig. 1(e) is smooth), while an interdependent network or a network of networks could be extremely vulnerable [38–40] (the curve in Fig. 1(e) exhibits an abrupt jump from a finite value to zero).

Note that the above classification for existing studies on network robustness can be continued, depending on the angle from which the problem is viewed. For instance, in reality it is necessary to repair or recover a damaged network, thus existing studies can be categorized as: network robustness under attacks and network robustness under recoveries [33, 41, 42]. While many studies make efforts to answer the question of how robust a network is in face of perturbations, another research direction explores answers towards questions like what are the optimal structures of a network that are robust to perturbations and what kind of measures can be taken to enhance the robustness of a network [25, 34, 40, 43–45].

1.2 Motivation and Contribution

Multipartite networks are an essential part of complex networks [46–48]. The notion of multipartite network is the counterpart of monopartite or unipartite network [1, 2]. Although the works in [17, 26, 27, 29] have explored the robustness of multipartite networks, they are all empirical studies. Putting it another way, they can only tell whether a focal multipartite network is robust or not but cannot tell to what extent a multipartite network can survive perturbations.

To eliminate the deficiency of empirical studies on the robustness of multipartite networks, theoretical analysis on the robustness of bipartite networks which are a special case of multipartite networks have been erected [49–51]. However, on the one hand, the dynamics of bipartite networks as studied in [49–51] require domain-specific knowledge. On the other hand, the corresponding theories are only devised for bipartite networks and therefore are not applicable to multipartite network scenarios.

Note that theoretical methods like those in [21, 23, 36, 37] for analyzing the robustness of interdependent networks are mature, they are monopartite networks oriented and cannot be applied to handle multipartite networks. Though the latest work in [37] puts forward a mathematical method for analyzing the robustness of interdependent directed networks (still monopartite networks oriented), the method is not straightforward because it is developed in a manner similar to the seminal work in [21] where the robustness analysis involves recursive calculations of many transcendental equations.

To circumvent the above mentioned shortcomings, in this paper we present a precise yet direct theoretical method for analyzing the robustness of directed multipartite networks. The main contributions of this paper are threefold:

1) Network models for depicting the dynamical processes of bi-directed and unidirectional multipartite networks subject to vertex perturbations are respectively established. The structural differences between multipartite and monopartite networks render direct technology transfers from monopartite networks infeasible. The dynamic model used in [21] requires one-to-one interdependency, while the interdependency of a multipartite network is in a one-to-many mode.

2) Mathematical methods for calculating the proportions of vertices that eventually survive the perturbations occurred to multipartite networks with arbitrary degree distributions are accordingly developed. Although the theories developed in [23, 37, 52] are capable of handling interdependent networks with one-to-many interdependency, the transcendental equations involved in the calculation process require the variable $P_i(k)$ which denotes the degree distribution of the vertices in the i-th network. Note that for an interdependent network, the vertices of the i-th network are interconnected, i.e., $P_i(k) \neq 0$, while for a multipartite network there is no connections between vertices in the same partite set, i.e., $P_i(k) = 0$. As a consequence, existing models and methods are not amenable to the robustness analysis of multipartite networks.

3) Our proposed theories unravel the first-order and second-order phase transition phenomena on the robustness of directed multipartite networks. Experimental simulations on random multipartite networks with Poisson degree distributions are carried out to validate the correctness of our proposed mathematical methods. The experiments coincide quite well with our theoretical results.

1.3 Paper Organization

The remainder of this paper is structured as follows. Section 2 presents the preliminaries including basic network notations, canonical network models for robustness analysis, and robustness evaluation metrics. Section 3 delineates in detail our proposed method for analyzing the robustness of multipartite network subject to random vertex loss. Section 4 validates the correctness of our proposed method through experiments on random multipartite networks with Poisson degree distributions. Section 5 concludes the paper.

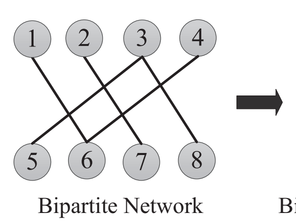
2 Preliminaries

2.1 Network Notation

Given a network denoted by $G = \{V, E\}$, where V and E respectively represent the sets of vertices and edges. We use e_{ij} to represent the edge between vertices i and j. If the vertex set V of a network G is composed of L different types of vertices, i.e., $V = \{v_1, v_2, ..., v_L\}$, G is said to be a multipartite (or L-partite) network if the following condition is satisfied:

$$\begin{cases} v_i \cap v_j = \emptyset, & \forall i, j \wedge i \neq j \\ \exists e_{ij}, & iff\ i = j-1 \vee i = j+1 \end{cases}, \tag{1}$$

where v_i is called a partite set which contains $n_i = |v_i|$ vertices. The total number of vertices of G is thus $N = \sum n_i$.



$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Fig. 2. Graphical illustration of a bipartite network and its bipartite matrix.

The left part of Fig. 2 exhibits an example of a multi-partite network. Because $L = 2$ for the network shown in Fig. 2, G is therefore commonly called a bipartite network or a two-mode network [1]. The right part of Fig. 2 shows the bipartite matrix $\mathbf{B}$ of network G. The entry b_{ij} of $\mathbf{B}$ denotes the interaction between vertices i and j. Note that $\mathbf{B}$ is generally asymmetric.

2.2 Network Robustness Analysis

Studies on network robustness aim to investigate the problem of to what extent a network can withstand perturbations occuring to vertices and/or edges. In the literature, two typical network models for depicting the dynamics of networks subject to perturbations are commonly utilized to analyze the robustness of networks. Fig. 3 takes the vertex robustness analysis as an example to delineate the two network models.

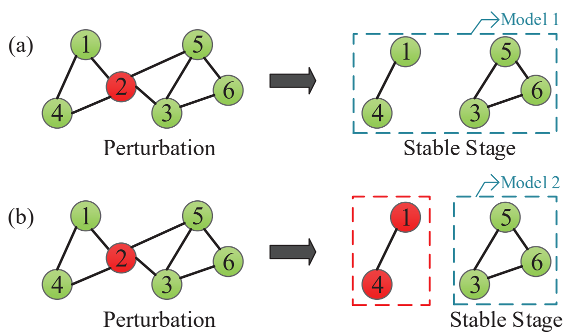


Fig. 3. Schematic illustrations of network models for depicting the dynamics of networks subject to perturbations. Network model 1 is based on the calculation of remaining vertices while network model 2 is based on the calculation of the largest connected component.

In Fig. 3(a), vertex 2 is removed from the network and the removal breaks the network into two clusters, i.e., $c_1 = \{1, 4\}$ and $c_2 = \{3, 5, 6\}$. The network model based on the calculation of remaining vertices is interested in vertices in clusters c_1 and c_2. As shown in Fig. 3(b), the network model based on the calculation of the largest connected component (LCC) only concerns cluster c_2 since it contains the largest number of vertices, and as a result cluster c_1 will be disfunctional and removed.

2.3 Robustness Evaluation Metric

Fig. 3 exhibits two commonly used network models for network robustness analysis. In the literature, three metrics are accordingly proposed and widely adopted to quantitatively measure the robustness of a network. Other kinds of measures can be found in [53].

1) *Node Robustness Index*: Let s_q be the number of remaining vertices after removing a fraction q of vertices from a network G. The node robustness index R_n is defined as $R_n = \frac{1}{N}\sum_{q=0}^{1} s_q$. The node robustness index is first used in [22]. The larger the value of R_n, the more robust the network is. Two successors can be found in [25, 54] where ref. [25] put forward a link robustness index R_l in a similar manner to R_n and ref. [54] developed a community robustness index R_c which is a combination of R_n and R_l.
2) *Area Based Robustness Index*: For a focal network G, if the value of q is known, then we can easily obtain s_q. We thus can draw q and s_q in a 2-D space for all $q \in [0, 1]$ and a curve will be yielded. The area based robustness index is then calculated as the area covered by the X-Y axis and the yielded curve. The larger the value of the area, the more robust the network is. The area based index is commonly used in the field of ecology, e.g., refs. [17] and [29] respectively make use of this index to measure the robustness of ecological networks to the loss of species and species community.
3) *LCC Based Index*: Given that a fraction $1 - p$ of vertices are removed from G. The LCC based index quantifies the robustness of a network as the proportion P^{∞} of vertices contained in the LCC. The robustness of a network in this context can be formulated as $P^{\infty} = \frac{N_{\text{LCC}}}{N}$, where N_{LCC} denotes the number of vertices in the LCC after removing a fraction $1 - p$ of vertices from G. This kind of robustness evaluation index is widely used in the fields of network science and physics [36, 37].

3 Methodology

For an L-partite network, we randomly remove a fraction $1 - p_i$ of vertices from v_i for all $i \in [1, L]$. Our purpose is to mathematically figure out the proportions of vertices P_i^{∞} in v_i that are contained in the LCC after perturbations. To do so, we first list all related notations in Table 1.

TABLE 1
Notations concerning the mathematical analysis of the robustness of an *L*-partite network *G*.

Variable	Definition
p_i	a fraction $1 - p_i$ of vertices in v_i are randomly removed
P_i^{∞}	fraction of vertices in v_i that are contained in the LCC
z_{ij}	probability that a vertex in v_i is not connected to the LCC via a vertex in v_j
$P_i(k)$	degree distribution of vertices in v_i
$q_i(k)$	excess degree distribution of $P_i(k)$
$P_{ij}(k)$	degree distribution of vertices in v_i which are connected to vertices in v_j
k	vertex degree
$\langle k_i \rangle$	$\langle k_i \rangle = \sum_{k=0}^{\infty} kP_i(k)$, mean degree of vertices in v_i
$\langle k_{ij} \rangle$	$\langle k_{ij} \rangle = \sum_{k=0}^{\infty} kP_{ij}(k)$, mean degree of vertices in v_i which are connected to vertices in v_j

For an L-partite network, the vertex perturbation occured to one partite may affect vertices in other partite sets and eventually cascading failures are likely to occur. In the following, we present our establish dynamic models and theoretical methods for analyzing the robustness of bidirected and unidirectional L-partite networks subject to random vertex losses.

To enhance the elegance of the theoretical calculations, we make use of the mathematical tool of generating functions [21]. Given a probability distribution function $P_{ij}(k)$, its generating function can be defined as

$$G_{ij}(x) = \sum_{k=0}^{\infty} x^k P_{ij}(k). \tag{2}$$

Based on Eq. 2 we define another function which reads

$$\begin{aligned} H_{ij}(x) &= \frac{G_{ij}^{'}(x)}{G_{ij}^{'}(1)} = \frac{\sum_{k=0}^{\infty} k x^{k-1} P_{ij}(k)}{\sum_{k=0}^{\infty} k x^{k-1} P_{ij}(k)|_{x=1}} \\ &= \frac{\sum_{k=0}^{\infty} (k+1) x^{k} P_{ij}(k+1)}{\langle k_{ij} \rangle} \end{aligned} . \quad (3)$$

3.1 Dynamic Model for Unidirectional Multipartite Networks

Models exhibited in Fig. 3 are for single networks, while networks in reality are often interdependent and could be vulnerable to perturbations. Fig. 4 takes a toy interdependent network as an example to introduce the widely adopted network model for analyzing the robustness of interdependent networks.

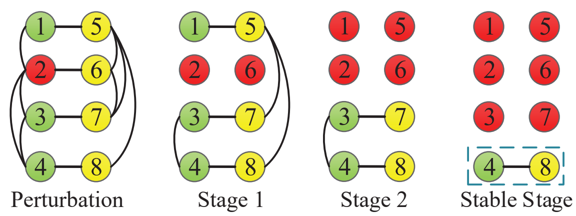


Fig. 4. A schematic illustration of the widely used network model for depicting the dynamics of an interdependent network subject to vertex perturbations.

In Fig. 4, the toy interdependent network consists of two networks (distinguished by different colors) which are one-to-one corrected. Originally, vertex 2 from one network is removed. In stage 1, the edges attached to vertex 2 are removed. The same process occurs to vertex 6 since vertices 2 and 6 are interdependent. The removal of vertex 2 fragments the network in the left side into two parts and it is assumed that only the vertices in the LCC will be of interest. As a result, in stage 2 vertices 1 and 5 are removed. The removal of vertex 5 leads to the fragmentation of the network in the right side. This process is continued until no further vertex remove is possible. In the final stage, only vertices 4 and 8 are remained functioning.

As aforementioned, there is no connection between vertices in the same partite set of a multipartite network. Thus the model demonstrated in Fig. 4 is not applicable to multipartite networks.

We establish the dynamic model shown in Fig. 5 to depict the dynamic process of a unidirectional multipartite network subject to vertex perturbations.

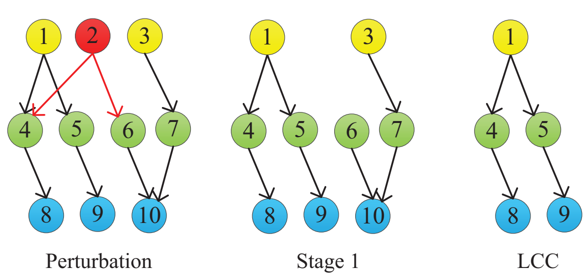


Fig. 5. The network model for depicting the robustness of a unidirectional multipartite network subject to vertex loss.

As shown in Fig. 5, vertex 2 is removed from a unidirectional tripartite network. This removal breaks the network into two parts. Because the network is unidirectional, no cascading failures will occur. Therefore, in the final stage we only consider the vertices in the LCC which is shown in the right panel of Fig. 5.

Note that, since we are considering a unidirectional multipartite network, we should focus on the LCC of the whole network when analyzing its robustness. For example, let us consider the network shown in Fig. 5 as a complex control system where vertices 1, 2, and 3 represent the controllers. In order to ensure the success of the control mission, it is generally required that there exists a LCC which contains as many components as possible.

3.2 Dynamic Model for Bi-directed Multipartite Networks

We establish the dynamic model shown in Fig. 6 to depict the dynamic process of a bi-directed multipartite network subject to vertex perturbations.

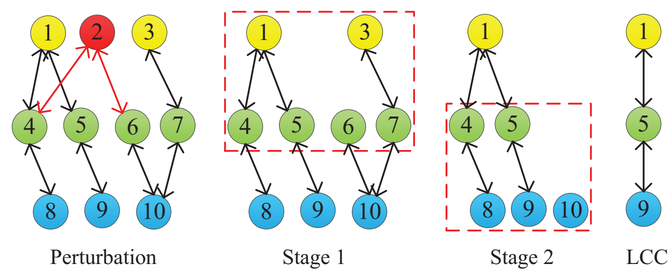


Fig. 6. The network model for depicting the robustness of a bi-directed multipartite network subject to vertex loss.

As shown in Fig. 6, vertex 2 is removed from a bi-directed tripartite network. The removal also fragments the network into two parts. However, we cannot simply compute the robustness of this network in the same manner as shown in Fig. 5 since the focal network is bi-directed and its dynamics are different from that of a unidirectional multipartite network.

After removing vertex 2, the bipartite network (surrounded by red circle in stage 1) breaks into three parts and only vertices 1, 4, and 5 will still be functional. As a consequence, in stage 1 vertices 3, 6, and 7 will be disfunctional. The removal of vertices 3, 6, and 7 further divides the second bipartite network (surrounded by red circle in stage 2) into three groups and only vertices in the LCC of the second bipartite network (because there are two LCCs, we randomly choose the one that contains vertices 5 and 9) will survive. In the final stage, only vertices 1, 5, and 9 are remained in the final LCC.

3.3 Theoretical Method for Bipartite Networks

Existing theoretical methods for analyzing the robustness of interdependent networks are largely based on the network model displayed in Fig. 4. As discussed above, those theories are not amenable to multipartite networks and therefore new theories are desired.

Because the simplest form of a multipartite network is the bipartite network, here we first investigate the robustness of bipartite networks to random vertex perturbations.

In order to figure out P_1^{∞} and P_2^{∞} for a bipartite network, we first define z_{12} as the probability that a vertex $i \in v_1$ is not connected to the LCC via a vertex $j \in v_2$. Anologously, we can define another probability z_{21}. Suppose the degree of vertex i is k, i.e., it has k neighbors in v_2. As a consequence, the average probability $P_r(i \notin \mathrm{LCC})$ that vertex i does not belong to the LCC is

$$P_r(i \notin \mathrm{LCC}) = \sum_{k=0}^{\infty} P_{12}(k) z_{12}^k = G_{12}(z_{12}). \tag{4}$$

Therefore, the average probability $P_r(i \in \mathrm{LCC})$ that vertex i belongs to the LCC is $P_r(i \in \mathrm{LCC}) = 1 - P_r(i \notin \mathrm{LCC})$. Since we randomly remove a fraction $1-p_1$ and a fraction $1-p_2$ of vertices from the bipartite network, the proportion of vertices in v_1 that belong to the LCC, i.e., P_1^{∞}, thus can be written as

$$P_1^{\infty} = p_1 P_r(i \in \mathrm{LCC}) = p_1 \left(1 - G_{12}(z_{12})\right). \tag{5}$$

Analogously, we can derive the expression of P_2^{∞} which reads

$$P_2^{\infty} = p_2 \left(1 - G_{21}(z_{21})\right). \tag{6}$$

The key to Eqs. 5 and 6 is to figure out the expressions of variables z_{12} and z_{21}. Note that the event that a vertex $i \in v_1$ is not connected to the LCC via a vertex $j \in v_2$ happens under two independent cases: 1) the vertex in v_2 is removed, which happens with a probability $1-p_2$; 2) the vertex in v_2 is not removed (this happens with a probability p_2) and it is not connected to the LCC via its k extra neighbors in v_1 (this happens with a probability z_{21}^k).

Note that the probability $q_{21}(k)$ for vertex j to have k extra neighbors in v_1 is not $P_{21}(k+1)$. Because for a bipartite network there are totally $n_2 P_{21}(k+1)$ vertices in v_2 each of which has degree $k+1$, thus $q_{21}(k)$ can be calculated as follows

$$q_{21}(k) = \frac{n_2 P_{21}(k+1)(k+1)}{n_2 \langle k_2 \rangle} = \frac{(k+1)P_{21}(k+1)}{\langle k_2 \rangle}. \tag{7}$$

Based on Eq. 7, we can get the expression of z_{12} as

$$\begin{aligned} z_{12} &= \sum_{k=0}^{\infty} \left(1 - p_2 + p_2 z_{21}^k\right) q_{21}(k) \\ &= 1 - p_2 + p_2 H_{21}(z_{21}) \end{aligned}. \tag{8}$$

Analogously, we can get the expression of z_{21} as

$$z_{21} = 1 - p_1 + p_1 H_{12}(z_{12}). \tag{9}$$

By substituting the expression of z_{21} into that of z_{12} we can get the following self-consistent equation

$$z_{12} = 1 - p_2 + p_2 H_{21}\left(1 - p_1 + p_1 H_{12}(z_{12})\right). \tag{10}$$

A possible non-trivial solution z_{12} may appear if the two curves $f_1 = z_{12}$ and $f_2 = 1 - p_2 + p_2 H_{21}\left(1 - p_1 + p_1 H_{12}(z_{12})\right)$ meet with each other tangentially at $z_{12} = 1$. Putting it another way, a critical value p_c occurs when

$$\left.\frac{\mathrm{d}f_1}{\mathrm{d}z_{12}}\right|_{z_{12}=1} = \left.\frac{\mathrm{d}f_2}{\mathrm{d}z_{12}}\right|_{z_{12}=1}. \tag{11}$$

From Eq. 11 we further derive the following relations

$$p_c = p_1 p_2 = \frac{\langle k_1 \rangle \langle k_2 \rangle}{\left(\langle k_1^2 \rangle - \langle k_1 \rangle\right)\left(\langle k_2^2 \rangle - \langle k_2 \rangle\right)}. \tag{12}$$

3.4 Theoretical Method for Unidirectional Multipartite Networks

For generality and simplicity, hereafter we take a tripartite network as an example to delineate our mathematical derivations for the robustness analysis of multipartite networks. Analogous to the analysis of bipartite networks, we therefore have four variables z_{12}, z_{21}, z_{23}, and z_{32}.

We can notice from Fig. 5 that the LCC may not encompass vertices in v_1 or v_3. Consequently, it is easy to get the expressions of P_1^{∞} and P_3^{∞} as

$$\left\{ \begin{aligned} P_1^{\infty} &= p_1 \left(1 - \sum_{k=0}^{\infty} P_{12}(k) z_{12}^k\right) = p_1 \left(1 - G_{12}(z_{12})\right) \\ P_3^{\infty} &= p_3 \left(1 - \sum_{k=0}^{\infty} P_{32}(k) z_{32}^k\right) = p_3 \left(1 - G_{32}(z_{32})\right) \end{aligned} \right. . \tag{13}$$

For a vertex $j \in v_2$, if it does not belong to the LCC, then it should not be connected to the LCC via its neighbors in v_1 and v_3. Thus, the average probability $P_r(j \notin \mathrm{LCC})$ that vertex j does not belong to the LCC is

$$\begin{aligned} P_r(j \notin \mathrm{LCC}) &= \sum_{k=0}^{\infty} P_{21}(k) z_{21}^k \cdot \sum_{k=0}^{\infty} P_{23}(k) z_{23}^k \\ &= G_{21}(z_{21}) G_{23}(z_{23}) \end{aligned}. \tag{14}$$

As a consequence, we can get the expression of P_2^{∞} as

$$\begin{aligned} P_2^{\infty} &= p_2 \left(1 - P_r(j \notin \mathrm{LCC})\right) \\ &= p_2 \left(1 - G_{21}(z_{21}) G_{23}(z_{23})\right) \end{aligned}. \tag{15}$$

In the next step we are going to derive the relations between the four variables z_{12}, z_{21}, z_{23}, and z_{32}.

Since the event that a vertex in v_2 is not connected to the LCC via a vertex in v_1 happens under two cases which are very similar to that of a bipartite network, we therefore can formulate z_{21} and z_{23} as

$$\left\{ \begin{aligned} z_{21} &= 1 - p_1 + p_1 H_{12}(z_{12}) \\ z_{23} &= 1 - p_3 + p_3 H_{32}(z_{32}) \end{aligned} \right. . \tag{16}$$

Now let us consider the event that a vertex $i \in v_1$ is not connected to the LCC via a vertex $j \in v_2$, i.e., the probability z_{12}. This event happens under two cases: 1) j is removed; 2) j is not removed. Case 1 happens with a probability $1-p_2$. Now the key is to work out the probability for case 2.

Because a vertex $j \in v_2$ could have neighbors in v_1 and v_3, if j does not belong to the LCC, then it must not be connected to the LCC via its neighbors in v_1 and v_3. Note that the event for j to have k neighbors in v_1 and the event for j to have k neighbors in v_3 are independent. Therefore, the probability $P_r(j \notin \mathrm{LCC})$ in this situation becomes

$$\begin{aligned} P_r(j \notin \mathrm{LCC}) &= \sum_{k=0}^{\infty} q_{21}(k) z_{21}^k \cdot \sum_{k=0}^{\infty} q_{23}(k) z_{23}^k \\ &= H_{21}(z_{21}) H_{23}(z_{23}) \end{aligned}. \tag{17}$$

As a result, the probability for case 2 to happen is $p_2 H_{21}(z_{21}) H_{23}(z_{23})$. With all these, the expression for z_{12} becomes

$$z_{12} = 1 - p_2 + p_2 H_{21}(z_{21}) H_{23}(z_{23}). \tag{18}$$

Note that the event that a vertex $l \in v_3$ is not connected to the LCC via a vertex $j \in v_2$ happens in the same way as that of vertex i does, we can easily derive the expression of z_{32}, which has the same form as Eq. 18.

3.5 Theoretical Method for Bi-directed Multipartite Networks

By comparing Figs. 5 and 6 we can notice that the main difference between the two network models lies in the calculation of the LCC. For a bi-directed tripartite network, the derivation process of P_1^∞ and P_3^∞ is the same as that of a unidirectional tripartite network. It is easy to prove that P_1^∞ and P_3^∞ have the same form as Eq. 13, while z_{21} and z_{23} have the same form as Eq. 16. The most difficult part lies in the calculations of P_2^∞, z_{12}, and z_{32}.

In order to figure out P_2^∞, z_{12}, and z_{32}, we first figure out the probability that a vertex j in v_2 belongs to the LCC. As mentioned above, vertex j may have neighbors in v_1 and v_3. If $j \in \mathrm{LCC}$, then at least one neighbor vertex i in v_1 should connect j to the LCC, and this event happens with a probability $1 - z_{21}^k$. Because the LCC contains vertices from v_1, v_2, and v_3, thus there should exist at least one neighbor vertex l in v_3 which also connects j to the LCC, and this event happens with a probability $1 - z_{23}^k$. As a consequence, the probability that a vertex j in v_2 belongs to the LCC is $(1 - z_{21}^k)(1 - z_{23}^k)$.

Bear in mind that probabilities for j to have k neighbors in v_1 and k neighbor in v_3 are respectively $P_{21}(k)$ and $P_{23}(k)$. Note that the probabilities are not $q_{21}(k)$ and $q_{23}(k)$ since vertex j is randomly picked but not arrived from vertex i. Therefore, we can formulate P_2^∞ as

$$\begin{aligned} P_2^\infty &= p_2 \sum_{k=0}^{\infty} P_{21}(k)(1 - z_{21}^k) \sum_{k=0}^{\infty} P_{23}(k)(1 - z_{23}^k) \\ &= p_2 \left(1 - \sum_{k=0}^{\infty} P_{21}(k) z_{21}^k\right)\left(1 - \sum_{k=0}^{\infty} P_{23}(k) z_{23}^k\right) \\ &= p_2 \left(1 - G_{21}(z_{21})\right)\left(1 - G_{23}(z_{23})\right) \end{aligned}. \tag{19}$$

Analogously, we can figure out z_{12} and z_{32} as

$$\begin{cases} z_{12} &= 1 - p_2 \left(1 - \sum_{k=0}^{\infty} q_{21}(k) z_{21}^k\right)\left(1 - \sum_{k=0}^{\infty} q_{23}(k) z_{23}^k\right) \\ &= 1 - p_2 \left(1 - H_{21}(z_{21})\right)\left(1 - H_{23}(z_{23})\right) \\ z_{32} &= z_{12} \end{cases}. \tag{20}$$

In summary, the robustness analysis for a bi-directed tripartite network with arbitrary degree distributions can be written as

$$\begin{cases} z_{12} &= z_{32} = 1 - p_2 \left(1 - H_{21}(z_{21})\right)\left(1 - H_{23}(z_{23})\right) \\ z_{21} &= 1 - p_1 + p_1 H_{12}(z_{12}) \\ z_{23} &= 1 - p_3 + p_3 H_{32}(z_{32}) \end{cases}, \tag{21}$$

$$\begin{cases} P_1^\infty &= p_1 \left(1 - G_{12}(z_{12})\right) \\ P_2^\infty &= p_2 \left(1 - G_{21}(z_{21})\right)\left(1 - G_{23}(z_{23})\right) \\ P_3^\infty &= p_3 \left(1 - G_{32}(z_{32})\right) \end{cases}. \tag{22}$$

4 Results

4.1 Random Networks

In order to validate the correctness of our proposed method for analyzing the robustness of directed multipartite networks subject to random vertex perturbations, here we generate random multipartite networks.

Let us define a probability vector $\boldsymbol{R} = (r_1, r_2, ..., r_{L-1})$. Given an empty L-partite network, we connect two arbitrary vertices with one comes from v_i and the other one comes from v_{i+1} with a probability r_i. Then the degree distribution $P_{ij}(k)$ becomes

$$\begin{aligned} P_{ij}(k) &= \binom{n_j}{k} r_j^k (1 - r_j)^{n_j - k} \\ &\approx \mathrm{e}^{-\langle k_{ij} \rangle} \frac{\langle k_{ij} \rangle^k}{k!} \end{aligned}, \tag{23}$$

where $j = i - 1$ and $\langle k_{ij} \rangle = n_j r_j$. Analogously, we can get the degree distribution $P_{il}(k)$ which read

$$\begin{aligned} P_{il}(k) &= \binom{n_l}{k} r_i^k (1 - r_i)^{n_l - k} \\ &\approx \mathrm{e}^{-\langle k_{il} \rangle} \frac{\langle k_{il} \rangle^k}{k!} \end{aligned}, \tag{24}$$

where $l = i + 1$ and $\langle k_{il} \rangle = n_l r_i$.

Eqs. 23 and 24 indicate that the generated network follows the Poisson degree distributions. The main reason for only generating networks with Poisson distributions is that a Poisson distribution $P_{ij}(k)$ has good mathematical properties. To be specific, for a Poisson distribution $P_{ij}(k) = \mathrm{e}^{-\lambda} \frac{\lambda^k}{k!}$, we have the following equations:

$$\begin{aligned} G_{ij}(x) &= \sum_{k=0}^{\infty} x^k P_{ij}(k) = \sum_{k=0}^{\infty} x^k \mathrm{e}^{-\lambda} \frac{\lambda^k}{k!} \\ &= \mathrm{e}^{\lambda(x-1)} \end{aligned}, \tag{25}$$

$$H_{ij}(x) = \frac{G'_{ij}(x)}{G'_{ij}(1)} = \mathrm{e}^{\lambda(x-1)} = G_{ij}(x), \tag{26}$$

$$\begin{aligned} \langle k_{ij}^2 \rangle &= \sum_{k=0}^{\infty} k^2 P_{ij}(k) = \sum_{k=0}^{\infty} k^2 \mathrm{e}^{-\lambda} \frac{\lambda^k}{k!} \\ &= \lambda \mathrm{e}^{-\lambda} \left(\sum_{k=0}^{\infty} (k-1) \frac{\lambda^{k-1}}{(k-1)!} + \sum_{k=0}^{\infty} \frac{\lambda^{k-1}}{(k-1)!}\right) \\ &= \lambda \mathrm{e}^{-\lambda} \left(\lambda \mathrm{e}^{\lambda} + \mathrm{e}^{\lambda}\right) \\ &= \langle k_{ij} \rangle^2 + \langle k_{ij} \rangle \end{aligned}, \tag{27}$$

where $\langle k_{ij}^2 \rangle$ is the second moment of $P_{ij}(k)$.

Note that the generated multipartite networks for testing purpose are undirected. This is because that the directions of the edges have already been taken into account when developing the network models and mathematical methods for the robustness analysis. While calculating the robustness of a directed multipartite network, we only need to know the degree distributions for vertices in each partite set.

4.2 Robustness of bipartite networks

For a bipartite network with Poisson degree distributions, we can simplify the robustness analysis functions into the following forms

$$\begin{cases} z_{12} &= 1 - p_2 + p_2 \mathrm{e}^{\langle k_2 \rangle (z_{21}-1)} \\ z_{21} &= 1 - p_1 + p_1 \mathrm{e}^{\langle k_1 \rangle (z_{12}-1)} \end{cases}, \tag{28}$$

$$\begin{cases} P_1^{\infty} &= p_1 \left(1 - \mathrm{e}^{\langle k_1 \rangle (z_{12}-1)}\right) \\ P_2^{\infty} &= p_2 \left(1 - \mathrm{e}^{\langle k_2 \rangle (z_{21}-1)}\right) \end{cases}. \tag{29}$$

We can notice that as long as parameters n_1, n_2, and r are given, then we can directly solve Eqs. 28 and and 29 so as to investigate the robustness of the focal bipartite network.

Now let us consider bipartite networks with the following configurations: $N = n_1 + n_2 = 8 \times 10^4$, $n_1 = \alpha N$, and $r = C/N$, where $\alpha \in (0, 1)$ and C is a constant. We test the robustness of two sets of bipartite networks:

1) $\alpha = \frac{1}{8}$ and $C = \{4, 5, 6, 7\}$;
2) $\alpha = \frac{2}{8}$ and $C = \{4, 5, 6, 7\}$.

For simplicity we set $p_1 = p_2 = p$, i.e., for each network we randomly remove a fraction $1-p$ of vertices from the whole network.

Fig. 7 displays the robustness results on bipartite networks with Poisson degree distributions. The size for each network is controlled by α and the degree is controlled by C. The simulation results are averaged over 1000 independent trials while numerical results are obtained by solving Eqs. 28 and 29 by substituting the corresponding values of $\langle k_1 \rangle$ and $\langle k_2 \rangle$. We can clearly see from Fig. 7 that our theoretical results coincide quite well with the simulation results.

For a bipartite network with Poisson degree distributions, the critical value as given in Eq. 12 now becomes

$$\begin{aligned} p_c^2 &= \frac{\langle k_1 \rangle \langle k_2 \rangle}{\left(\langle k_1^2 \rangle - \langle k_1 \rangle\right)\left(\langle k_2^2 \rangle - \langle k_2 \rangle\right)} \\ &= \frac{1}{\langle k_1 \rangle \langle k_2 \rangle} = \frac{1}{\alpha(1-\alpha)C^2} \\ \Rightarrow p_c &= \frac{1}{C\sqrt{\alpha(1-\alpha)}} \end{aligned}. \tag{30}$$

Based on Eq. 30 we have

1) when $\alpha = \frac{1}{8}$ and $C = \{4, 5, 6, 7\}$, the critical values are $p_c = \{0.7559, 0.6047, 0.5040, 0.4320\}$;
2) when $\alpha = \frac{2}{8}$ and $C = \{4, 5, 6, 7\}$, the critical values are $p_c = \{0.5773, 0.4619, 0.3850, 0.3299\}$,

which are in accordance with the simulation results shown in Fig. 7.

Fig. 8 exhibits the simulations on the robustness of two bipartite networks in a more general way. We respectively remove a fraction $1 - p_1$ and a fraction $1 - p_2$ of vertices from v_1 and v_2 of each bipartite network. P_1^{∞} and P_2^{∞} are respectively shown with respect to different settings of p_1 and p_2. We can clearly see from Fig. 8 that the robustness curves are smooth and the turning points of p_1 and p_2 are small in values, which indicates that bipartite networks are extremely robustness to random vertex perturbations.

4.3 Robustness of Unidirectional multipartite networks

For a unidirectional tripartite network with Poisson degree distributions, we can simplify Eqs. 16, 18, 13 and 15 into the following forms

$$\begin{cases} z_{21} &= 1 - p_1 + p_1 \mathrm{e}^{\langle k_{12} \rangle (z_{12}-1)} \\ z_{23} &= 1 - p_3 + p_3 \mathrm{e}^{\langle k_{32} \rangle (z_{32}-1)} \\ z_{12} &= 1 - p_2 + p_2 \mathrm{e}^{\langle k_{23} \rangle (z_{23}-1)} \mathrm{e}^{\langle k_{21} \rangle (z_{21}-1)} \\ z_{32} &= z_{12} \end{cases}, \tag{31}$$

$$\begin{cases} P_1^{\infty} &= p_1 \left(1 - \mathrm{e}^{\langle k_{12} \rangle (z_{12}-1)}\right) \\ P_2^{\infty} &= p_2 \left(1 - \mathrm{e}^{\langle k_{23} \rangle (z_{23}-1)} \mathrm{e}^{\langle k_{21} \rangle (z_{21}-1)}\right) \\ P_3^{\infty} &= p_3 \left(1 - \mathrm{e}^{\langle k_{32} \rangle (z_{32}-1)}\right) \end{cases}. \tag{32}$$

For simplicity we set $p_1 = p_2 = p_3 = p$. In the experiments we generate three tripartite networks with their parameter configurations respectively given as

1) $(n_1, n_2, n_3) = (3, 1, 2) \times 10^4$, $\boldsymbol{R} = (\frac{C_1}{n_1+n_2}, \frac{C_2}{n_3+n_2})$, $C_1 = 8$, $C_2 = 6$;
2) $(n_1, n_2, n_3) = (1, 4, 1) \times 10^4$, $\boldsymbol{R} = (\frac{C_1}{n_1+n_2}, \frac{C_2}{n_3+n_2})$, $C_1 = 12$, $C_2 = 14$;
3) $(n_1, n_2, n_3) = (2, 2, 2) \times 10^4$, $\boldsymbol{R} = (\frac{C_1}{n_1+n_2}, \frac{C_2}{n_3+n_2})$, $C_1 = 4$, $C_2 = 3$.

Fig. 9 displays the robustness of three tripartite networks with each network subject to random vertices remove from every partite set. The theoretical results P^{∞} as shown in the last subfigure of Fig. 9 are simply obtained by solving $P^{\infty} = \sum P_i^{\infty}$. Fig. 9 clearly validates the correctness of our proposed method.

By combining Eqs. 11 and 31 we can get

$$\begin{aligned} & 1 = p_2 \frac{\mathrm{d}}{\mathrm{d}z_{12}} \left(\mathrm{e}^{\langle k_{23} \rangle (z_{23}-1)} \mathrm{e}^{\langle k_{21} \rangle (z_{21}-1)}\right)\Big|_{z_{12}=1} \\ \Rightarrow\ & 1 = p_2 \left(p_3 \langle k_{23} \rangle \langle k_{32} \rangle + p_1 \langle k_{21} \rangle \langle k_{12} \rangle\right) \end{aligned}. \tag{33}$$

Since we set $p_1 = p_2 = p_3 = p$ in our experiments, from the above equation we can figure out the critical value of p_c which reads

$$p_c = \sqrt{\frac{1}{\langle k_{23} \rangle \langle k_{32} \rangle + \langle k_{21} \rangle \langle k_{12} \rangle}}. \tag{34}$$

For the three tested tripartite networks, we have

1) $\langle k_{12} \rangle = 2$, $\langle k_{21} \rangle = 6$, $\langle k_{23} \rangle = 4$, $\langle k_{32} \rangle = 2$;
2) $\langle k_{12} \rangle = 9.6$, $\langle k_{21} \rangle = 2.4$, $\langle k_{23} \rangle = 2.8$, $\langle k_{32} \rangle = 11.2$;
3) $\langle k_{12} \rangle = 2$, $\langle k_{21} \rangle = 2$, $\langle k_{23} \rangle = 1.5$, $\langle k_{32} \rangle = 1.5$.

By substituting the mean degrees into Eq. 34 we respectively get the critical values for the three networks which are $p_c = 0.224$, $p_c = 0.136$, and $p_c = 0.400$. We can observe from Fig. 9 that our theoretical results are the same as the simulations.

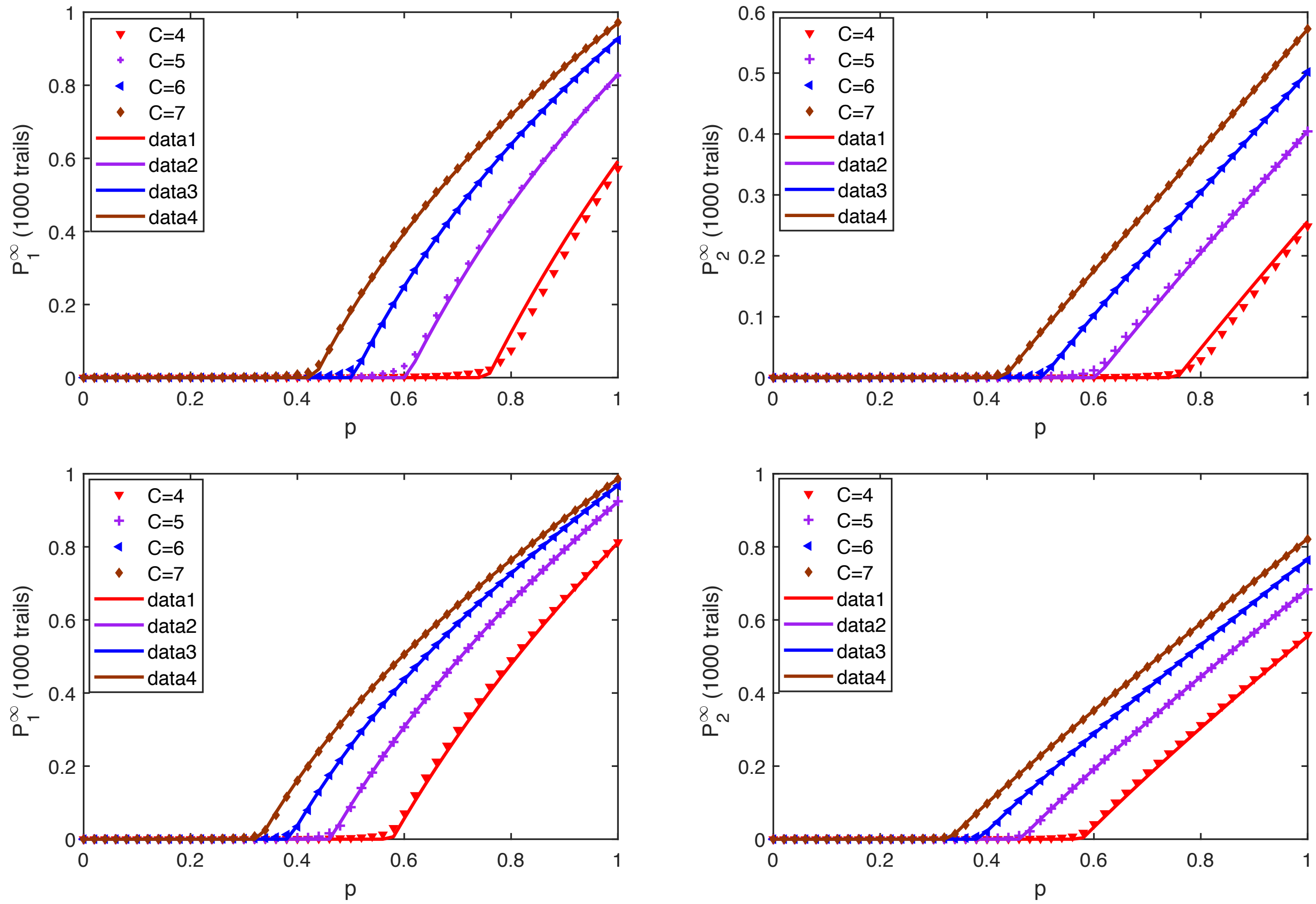


Fig. 7. Theoretical (denoted by lines) and simulation (denoted by symbols) results on the robustness of bipartite networks with Poisson degree distributions. A fraction $1-p$ of vertices are randomly removed from each network. We set $\alpha = 1/8$ and $\alpha = 2/8$ respectively for networks in the first row and the second row.

4.4 Robustness of Bi-directed multipartite networks

For a bi-directed tripartite network with Poisson degree distributions, we can simplify Eqs. 19 and 20 into the following forms

$$\begin{cases} z_{21} &= 1 - p_1 + p_1 \mathrm{e}^{\langle k_{12}\rangle (z_{12}-1)} \\ z_{23} &= 1 - p_3 + p_3 \mathrm{e}^{\langle k_{32}\rangle (z_{32}-1)} \\ z_{12} &= 1 - \left(p_2 - p_2 \mathrm{e}^{\langle k_{21}\rangle (z_{21}-1)}\right)\left(1 - \mathrm{e}^{\langle k_{23}\rangle (z_{23}-1)}\right) \\ z_{32} &= z_{12} \end{cases} . \tag{35}$$

$$\begin{cases} P_1^\infty &= p_1 \left(1 - \mathrm{e}^{\langle k_{12}\rangle (z_{12}-1)}\right) \\ P_2^\infty &= p_2 \left(1 - \mathrm{e}^{\langle k_{21}\rangle (z_{21}-1)}\right)\left(1 - \mathrm{e}^{\langle k_{23}\rangle (z_{23}-1)}\right) \\ P_3^\infty &= p_3 \left(1 - \mathrm{e}^{\langle k_{32}\rangle (z_{32}-1)}\right) \end{cases} . \tag{36}$$

In our experiments, we set $p_1 = p_2 = p_3 = p$. We still carry out experiments and theoretical analysis on the previously generated three tripartite networks. For the third network, we slightly change the constant C_2 to be $C_2 = 7$.

Fig. 10 displays the robustness of bi-directed tripartite networks with Poisson degree distributions. Each network is subject to random removal of a fraction $1-p$ of vertices from the whole network. Fig. 10 once again proves the correctness of our proposed method for analyzing the robustness of directed multipartite networks.

It can be seen from Fig. 10 that there exist abrupt jumps for the robustness curves, i.e., at the critical point p_c, P_i^∞ suddenly falls from a finite value to zero. This phenomenon indicates that bi-directed multipartite networks are less robust then unidirectional multipartite networks to random vertex perturbations.

Note that the critical value p_c cannot be obtained by solving Eq. 11. The reason can be discovered from Fig. 11 in which we draw the two curves $f_1(z_{12}) = z_{12}$ and $f_2(z_{12})$. The expression of $f_2(z_{12})$ is the right term of the expression of z_{12} in Eq. 36 where z_{21} and z_{23} are functions of z_{12}.

It can be seen from Fig. 11 that there always exists a trivial solution of $z_{12} = 1$ to the function $f_2(z_{12}) = z_{12}$. When p increases from 0 to 1, there exist a critical value of p which makes function $f_2(z_{12}) = z_{12}$ have the first non-trivial solution. Note that $f_2(z_{12}) = z_{12}$ is a transcendental function, we use numerical analysis to figure out critical value of p.

5 Concluding Remarks

To explore the robustness of complex networks to perturbations is of pivotal significance toward system control. While existing studies are primarily developed for monopartite networks, in this paper we proposed a theoretical method to investigate the robustness of multipartite networks to

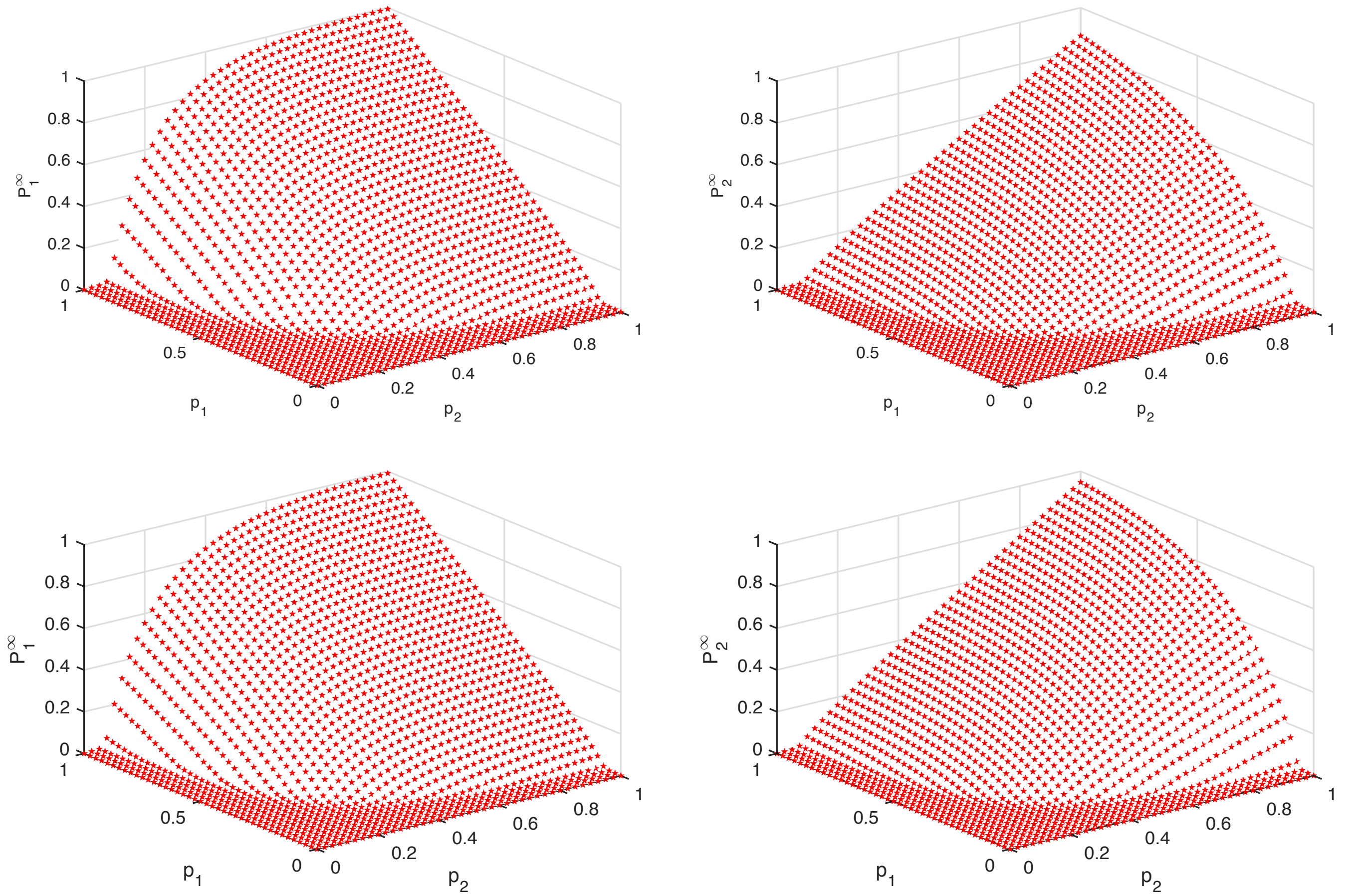


Fig. 8. Simulation results on the robustness of two bipartite network with Poisson degree distributions. We respectively set $\alpha = 1/8$, $C = 8$ and $\alpha = 3/8$, $C = 8$ for the two bipartite networks. A fraction $1 - p_1$ and a fraction $1 - p_2$ of vertices are randomly removed from v_1 and v_2, respectively.

random vertex perturbations. The correctness of our proposed methods have been verified through experiments on multipartite networks with Poisson degree distributions. Although we only mathematically investigated the robustness of bipartite and tripartite networks, it is easy to extend our proposed method to L-partite networks with $L > 3$.

Existing studies on network robustness indicate that a single network could be robust to random perturbations (exhibit second order phase transition) while an interdependent network could be vulnerable to random perturbations (exhibit first order phase transition). To some extent, a multipartite network could be regarded as a special case of an interdependent network. However, in this study we discovered that the robustness of bi-directed multipartite networks show first order phase transition while unidirectional multipartite networks display second order phase transition.

Note that it has long been reported that many real-world networks exhibit fat-tail degree distributions [1, 55], i.e., power law distributions. These networks are generally called scale-free (SF) networks. However, in the experiments multipartite networks with power law distributions are not tested. For one thing, our proposed methods can theoretically analyze the robustness of multipartite networks with arbitrary degree distributions. For another thing, SF networks in real-world are rare according to the lastest research [56]. Meanwhile, although many efforts have been done to generate single networks with arbitrary degree distributions [2, 57–66], generating multipartite networks with power law degree distributions is non-trivial and still demands tremendous efforts. Below are some useful discussions for generating multipartite SF networks.

For generality, let us consider generating a bipartite SF network $\mathbf{BP}_{m\times n}$ with m and n respectively denote the number of vertices in v_1 and v_2. The degree distributions of the vertices in v_1 and v_2 can be respectively formulated as

$$\begin{array}{l} P_1(d) = C_1 \cdot d^{-\lambda_1} \\ P_2(k) = C_2 \cdot k^{-\lambda_2} \end{array}, \tag{37}$$

where C_1 and C_2 are two constants and λ_1 and λ_2 are the exponents of the power law distributions.

In order to generate a bipartite SF network, one needs to do the inverse transform sampling, i.e., to sample the degree sequences $\boldsymbol{D} = (d_1, d_2, ..., d_m)$ and $\boldsymbol{K} = (k_1, k_2, ..., k_n)$ respectively from $P_1(d)$ and $P_2(k)$, where $d_i \in [\mathrm{d}_{min}, n]$ and $k_i \in [\mathrm{k}_{min}, m]$. Once $\boldsymbol{D}$ and $\boldsymbol{K}$ are obtained, then one can utilize the Configuration Model or its improved variants to graphically realize $\boldsymbol{D}$ and $\boldsymbol{K}$ and the bipartite network is thus generated.

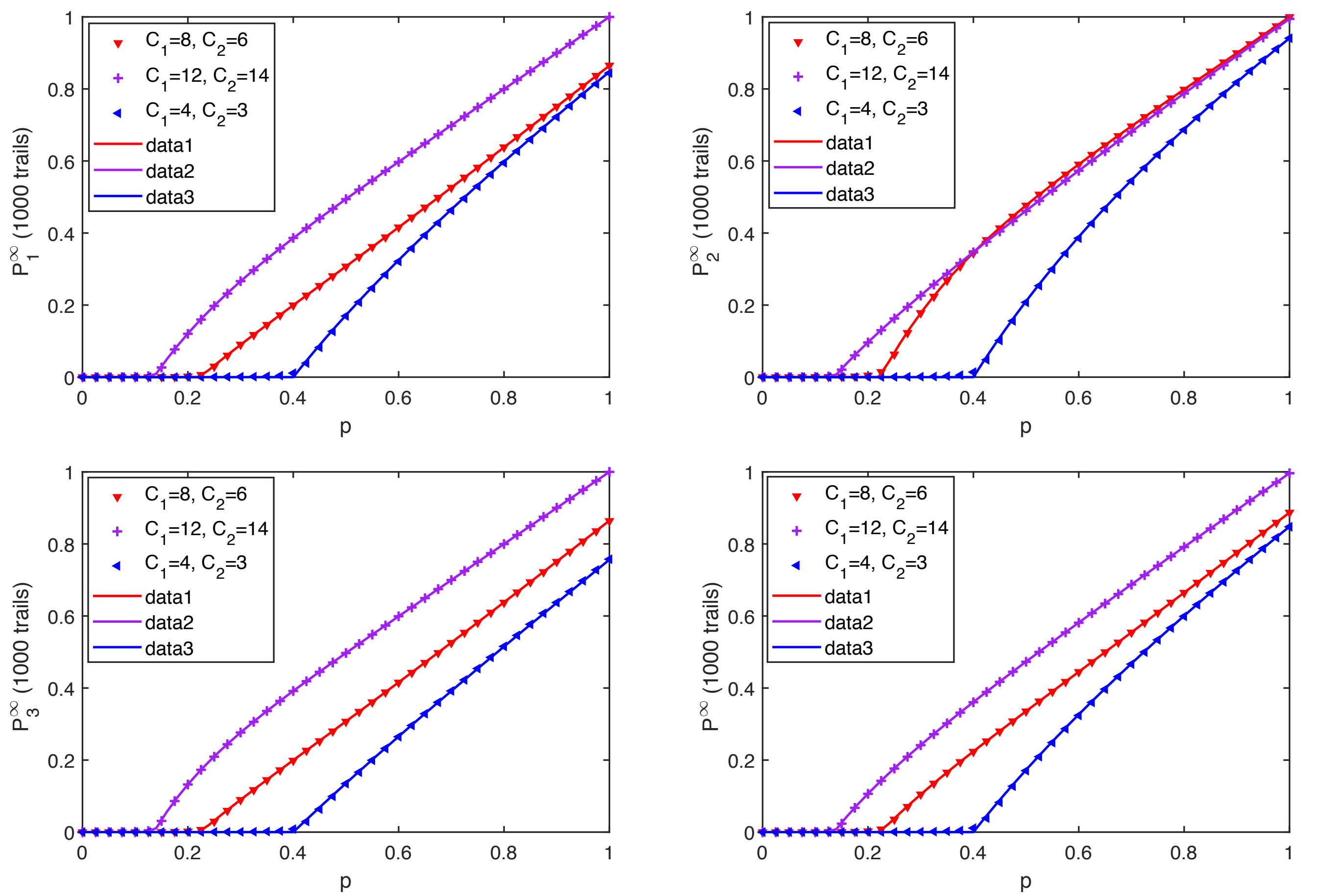


Fig. 9. Theoretical (denoted by lines) and simulation (denoted by symbols) results on the robustness of unidirectional tripartite networks with Poisson degree distributions. A fraction $1-p$ of vertices are randomly removed from each network.

Note that for a bipartite network, $\boldsymbol{D}$ and $\boldsymbol{K}$ should satisfy the following condition

$$\sum_{i=1}^{m} d_i \equiv \sum_{i=1}^{n} k_i \equiv |E|. \tag{38}$$

Eq. 38 has an equivalent form which reads

$$m \cdot \langle k_1 \rangle = n \cdot \langle k_2 \rangle . \tag{39}$$

Recall the definition for the first moment $\langle k \rangle$, along with Eq. 39 we can further derive

$$\begin{aligned} & m \cdot \sum_{d=\mathrm{d}_{min}}^{\infty} d \cdot P_1(d) = n \cdot \sum_{k=\mathrm{k}_{min}}^{\infty} k \cdot P_2(k) \\ \Rightarrow \quad & m \cdot C_1 \cdot \int_{\mathrm{d}_{min}}^{\infty} d^{-\lambda_1+1} \mathrm{d}d = n \cdot C_2 \cdot \int_{\mathrm{k}_{min}}^{\infty} k^{-\lambda_2+1} \mathrm{d}k \end{aligned} . \tag{40}$$

Assume that $\lambda_1 - 1 \geq 1$ and $\lambda_2 - 1 \geq 1$, the above equation thus can be simplified as

$$\frac{mC_1}{\lambda_1 - 2} \mathrm{d}_{min}^{2-\lambda_1} = \frac{nC_2}{\lambda_2 - 2} \mathrm{k}_{min}^{2-\lambda_2}. \tag{41}$$

Note that we always have $\sum P_1(d) = \sum P_2(k) = 1$. To be specific, in the limit of $m,\ n \to \infty$, we have

$$\begin{aligned} \sum P_1(d) &= C_1 \sum_{d=\mathrm{d}_{min}}^{n} d^{-\lambda_1} \simeq C_1 \int_{d=\mathrm{d}_{min}}^{\infty} d^{-\lambda_1} \mathrm{d}d \\ &= \frac{C_1}{\lambda_1 - 1} \mathrm{d}_{min}^{-(\lambda_1 - 1)} \end{aligned} , \tag{42}$$

$$\begin{aligned} \sum P_1(d) &= C_2 \sum_{k=\mathrm{k}_{min}}^{m} k^{-\lambda_2} \simeq C_2 \int_{k=\mathrm{k}_{min}}^{\infty} k^{-\lambda_2} \mathrm{d}k \\ &= \frac{C_2}{\lambda_2 - 1} \mathrm{k}_{min}^{-(\lambda_2 - 1)} \end{aligned} . \tag{43}$$

From the above equation we can easily figure out the constants as

$$\begin{aligned} C_1 &= (\lambda_1 - 1) \mathrm{d}_{min}^{\lambda_1 - 1} \\ C_2 &= (\lambda_2 - 1) \mathrm{k}_{min}^{\lambda_2 - 1} \end{aligned} . \tag{44}$$

Putting the above equation back into Eq. 41 we get the relationships between the exponents λ_1 and λ_2 as follows

$$m \cdot \frac{\lambda_1 - 1}{\lambda_1 - 2} \cdot \mathrm{d}_{min} = n \cdot \frac{\lambda_2 - 1}{\lambda_2 - 2} \cdot \mathrm{k}_{min}. \tag{45}$$

Therefore, when generating a bipartite SF network, the following deterrents should be taken into account:

1) Exponents λ_1 and λ_2 should obey the constraint shown in Eq. 45. Note that it is easy to generating a

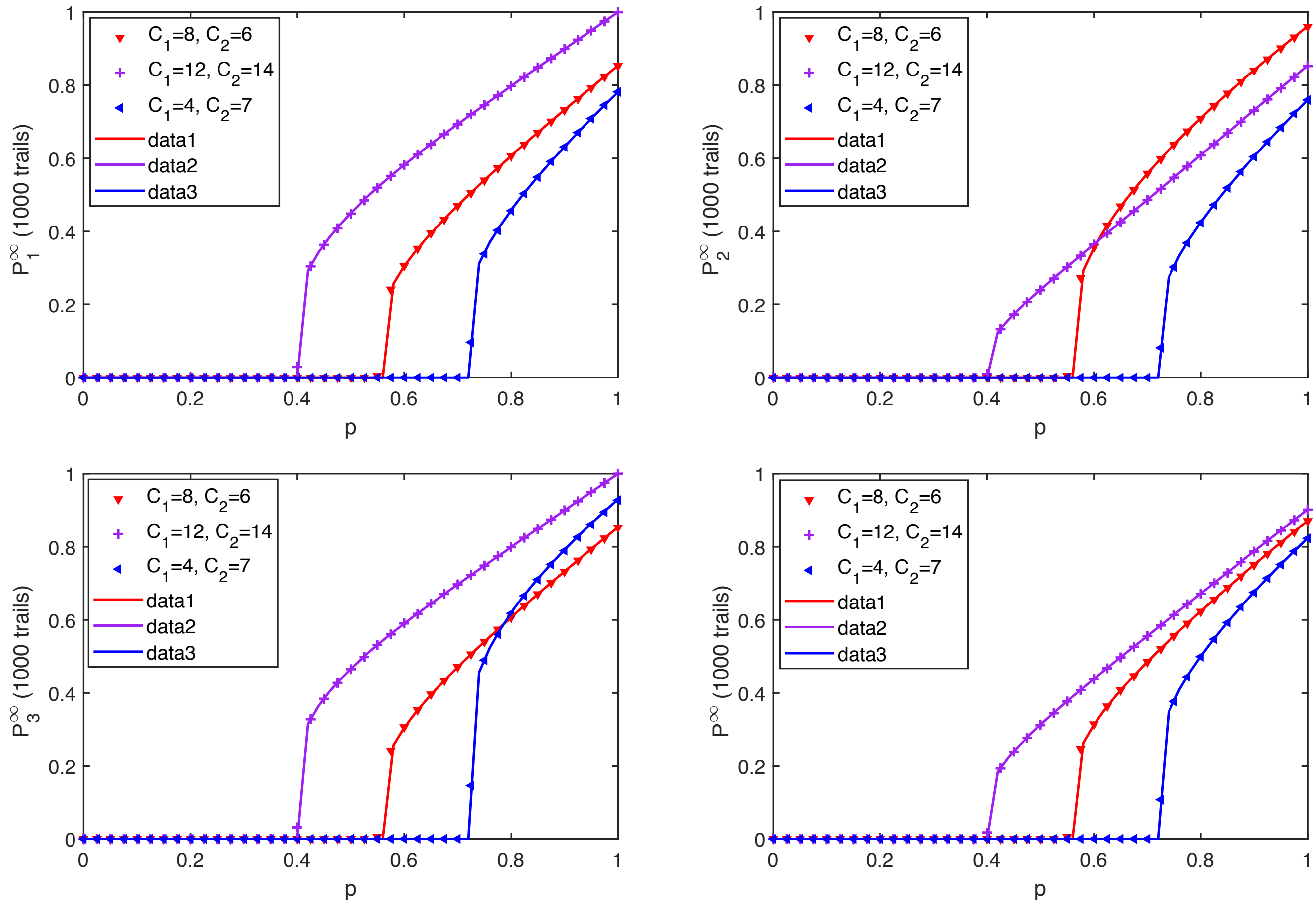


Fig. 10. Theoretical (denoted by lines) and simulation (denoted by symbols) results on the robustness of bi-directed tripartite networks with Poisson degree distributions. A fraction $1-p$ of vertices are randomly removed from each network.

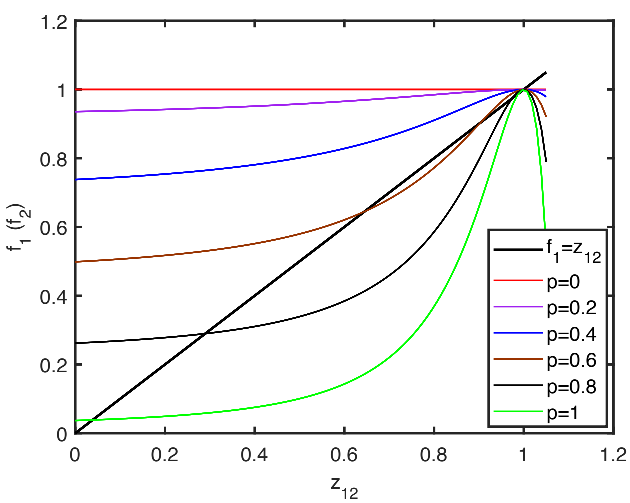


Fig. 11. Function plot of $f_1(z_{12})$ and $f_2(z_{12})$. The parameter settings are $z_{12}=[0,1]$, $p=\{0,0.2,0.4,0.6,0.8,1\}$, $\langle k_{12}\rangle=2$, $\langle k_{21}\rangle=6$, $\langle k_{23}\rangle=4$, $\langle k_{32}\rangle=2$;

SF-SF interdependent network, since exponents λ_1 and λ_2 of a SF-SF interdependent network can be set to arbitrary values.

2) Degree sequences $\boldsymbol{D}$ and $\boldsymbol{K}$ should satisfy the condition shown in Eq. 38. On the one hand, it is hard to sample two degree sequences $\boldsymbol{D}$ and $\boldsymbol{K}$ which exactly follow the distributions $P_1(k)\sim\lambda_1^k$ and $P_2(k)\sim\lambda_2^k$. On the other hand, even if $\boldsymbol{D}$ and $\boldsymbol{K}$ strictly follow $P_1(k)$ and $P_2(k)$, there is no guarantee that the condition shown in Eq. 38 will be satisfied. As a consequence, modifications like increasing or decreasing the values of some $d_i\in\boldsymbol{D}$ and $k_j\in\boldsymbol{K}$ have to be made, while which d_i and k_j should be chosen and modified is yet an open question.
3) Graphicality condition checking. Even though $\boldsymbol{D}$ and $\boldsymbol{K}$ simultaneously satisfy Eqs. 45 and 38, one still has to check the graphicality condition as shown in [63, 65] to see whether $\boldsymbol{D}$ and $\boldsymbol{K}$ can be graphically realized or not.
4) Unbiased graph sampling. Note that the number of networks that can graphically realize sequences $\boldsymbol{D}$ and $\boldsymbol{K}$ could grow exponentially as N increases [62, 64]. How to efficiently sample a small amount of networks which are less correlated with each other is an open issue.

References

[1] M. E. J. Newman, *Networks: An Introduction*. Oxford University Press, 2010.

[2] M. E. J. Newman, A.-L. Barabási, and D. J. Watts, *The structure and dynamics of networks*. Princeton University Press, 2011.

[3] P. Chen, R. Liu, Y. Li, and L. Chen, "Detecting critical state before phase transition of complex biological systems by hidden markov model," *Bioinformatics*, vol. 32, no. 14, pp. 2143–2150, 2016.

[4] 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.

[5] K. Drakopoulos, A. Ozdaglar, and J. Tsitsiklis, "An efficient curing policy for epidemics on graphs," *IEEE Transactions on Network Science and Engineering*, vol. 1, no. 2, pp. 67–75, 2014.

[6] K. Scaman, A. Kalogeratos, and N. Vayatis, "Suppressing epidemics in networks using priority planning," *IEEE Transactions on Network Science and Engineering*, vol. 3, no. 4, pp. 271–285, 2016.

[7] Y.-Y. Liu, J.-J. Slotine, and A.-L. Barabási, "Controllability of complex networks," *Nature*, vol. 473, no. 7346, pp. 167–173, 2011.

[8] J. Gao, Y.-Y. Liu, R. M. D'souza, and A.-L. Barabási, "Target control of complex networks," *Nature Communications*, vol. 5, no. 5415, 2014.

[9] S. Dhamal, K. Prabuchandran, and Y. Narahari, "Information diffusion in social networks in two phases," *IEEE Transactions on Network Science and Engineering*, vol. 3, no. 4, pp. 197–210, 2016.

[10] Y. Zhuang and O. Yagan, "Information propagation in clustered multilayer networks," *IEEE Transactions Network Science and Engineering*, vol. 3, no. 4, pp. 211–224, 2016.

[11] N. Pržulj and N. Malod-Dognin, "Network analytics in the age of big data," *Science*, vol. 353, no. 6295, pp. 123–124, 2016.

[12] C. C. Aggarwal, *Social Network Data Analytics*. Springer, 2011.

[13] K. Savla, G. Como, and M. A. Dahleh, "Robust network routing under cascading failures," *IEEE Transactions on Network Science and Engineering*, vol. 1, no. 1, pp. 53–66, 2014.

[14] J. Gao, B. Barzel, and A.-L. Barabási, "Universal resilience patterns in complex networks," *Nature*, vol. 530, no. 7590, pp. 307–312, 2016.

[15] G. Como and F. Fagnani, "Robustness of large-scale stochastic matrices to localized perturbations," *IEEE Transactions on Network Science and Engineering*, vol. 2, no. 2, pp. 53–64, 2015.

[16] R. J. La, "Cascading failures in interdependent systems: Impact of degree variability and dependence," *IEEE Transactions on Network Science and Engineering*, vol. 5, no. 2, pp. 127–140, 2018.

[17] M. J. 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.

[18] 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, p. 5468, 2000.

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

[20] S. Wang and J. Liu, "A multi-objective evolutionary algorithm for promoting the emergence of cooperation and controllable robustness on directed networks," *IEEE Transactions on Network Science and Engineering*, vol. 5, no. 2, pp. 92–100, 2018.

[21] 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.

[22] 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.

[23] 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, p. 036116, 2011.

[24] P. 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.

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

[26] A. Valiente-Banuet, M. A. Aizen, J. M. Alcántara, J. Arroyo, A. Cocucci, M. Galetti, M. B. García, D. García, J. M. Gómez, P. Jordano *et al.*, "Beyond species loss: the extinction of ecological interactions in a changing world," *Functional Ecology*, vol. 29, no. 3, pp. 299–307, 2015.

[27] D. M. Evans, M. J. 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.

[28] 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.

[29] Q. Cai and J. Liu, "The robustness of ecosystems to the species loss of community," *Scientific Reports*, vol. 6, no. 35904, 2016.

[30] X. Yuan, Y. Dai, H. E. Stanley, and S. Havlin, "k-core percolation on complex networks: Comparing random, localized, and targeted attacks," *Physical Review E*, vol. 93, no. 6, p. 062302, 2016.

[31] Z. Wang, D. Zhou, and Y. Hu, "Group percolation in interdependent networks," *arXiv preprint arXiv:1801.00665*, 2018.

[32] G. Dong, J. Gao, R. Du, L. Tian, H. E. Stanley, and S. Havlin, "Robustness of network of networks under targeted attack," *Physical Review E*, vol. 87, no. 5, p. 052804, 2013.

[33] M. Gong, L. Ma, Q. Cai, and L. Jiao, "Enhancing robustness of coupled networks under targeted recoveries," *Scientific Reports*, vol. 5, no. 8439, 2015.

[34] 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.

[35] S. Wang and J. Liu, “Constructing robust cooperative networks using a multiobjective evolutionary algorithm,” *Scientific Reports*, vol. 7, no. 41600, 2017.

[36] 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.

[37] 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.

[38] A. Vespignani, “Complex networks: The fragility of interdependency,” *Nature*, vol. 464, no. 7291, pp. 984–985, 2010.

[39] 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.

[40] 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.

[41] Y. Shang, “Localized recovery of complex networks against failure,” *Scientific Reports*, vol. 6, no. 30521, 2016.

[42] 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.

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

[44] C. M. Schneider, N. Yazdani, N. A. Araújo, S. Havlin, and H. J. Herrmann, “Towards designing robust coupled networks,” *Scientific Reports*, vol. 3, no. 1969, 2013.

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

[46] C. A. Hidalgo and R. Hausmann, “The building blocks of economic complexity,” *Proceedings of the National Academy of Sciences*, vol. 106, no. 26, pp. 10 570–10 575, 2009.

[47] T. P. Peixoto, “Parsimonious module inference in large networks,” *Physical Review Letters*, vol. 110, no. 14, p. 148701, 2013.

[48] D. M. Pelt and J. A. Sethian, “A mixed-scale dense convolutional neural network for image analysis,” *Proceedings of the National Academy of Sciences*, vol. 115, no. 2, pp. 254–259, 2017.

[49] A. G. Smart, L. A. Amaral, and J. M. Ottino, “Cascading failure and robustness in metabolic networks,” *Proceedings of the National Academy of Sciences*, vol. 105, no. 36, pp. 13 223–13 228, 2008.

[50] H. Hooyberghs, B. Van Schaeybroeck, and J. O. Indekeu, “Percolation on bipartite scale-free networks,” *Physica A: Statistical Mechanics and its Applications*, vol. 389, no. 15, pp. 2920–2929, 2010.

[51] X. Huang, I. Vodenska, S. Havlin, and H. E. Stanley, “Cascading failures in bi-partite graphs: model for systemic risk propagation,” *Scientific Reports*, vol. 3, p. 1219, 2013.

[52] G. Dong, R. Du, L. Tian, and R. Liu, “Robustness of network of networks with interdependent and interconnected links,” *Physica A: Statistical Mechanics and its Applications*, vol. 424, pp. 11–18, 2015.

[53] W. Ellens and R. E. Kooij, “Graph measures and network robustness,” *arXiv preprint arXiv:1311.5064*, 2013.

[54] L. Ma, M. Gong, Q. Cai, and L. Jiao, “Enhancing community integrity of networks against multilevel targeted attacks,” *Physical Review E*, vol. 88, no. 2, p. 022810, 2013.

[55] A.-L. Barabási and R. Albert, “Emergence of scaling in random networks,” *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[56] A. D. Broido and A. Clauset, “Scale-free networks are rare,” *arXiv preprint arXiv:1801.03400*, 2018.

[57] A. Barrat, M. Barthelemy, and A. Vespignani, *Dynamical processes on complex networks*. Cambridge University Press, 2008.

[58] M. Catanzaro, M. Boguñá, and R. Pastor-Satorras, “Generation of uncorrelated random scale-free networks,” *Physical Review E*, vol. 71, no. 2, p. 027103, 2005.

[59] M. Bayati, J. H. Kim, and A. Saberi, “A sequential algorithm for generating random graphs,” in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*. Springer, 2007, pp. 326–340.

[60] C. Cooper, M. Dyer, and C. Greenhill, “Sampling regular graphs and a peer-to-peer network,” *Combinatorics, Probability and Computing*, vol. 16, no. 4, pp. 557–593, 2007.

[61] R. Cohen and S. Havlin, *Complex networks: structure, robustness and function*. Cambridge University Press, 2010.

[62] C. I. Del Genio, H. Kim, Z. Toroczkai, and K. E. Bassler, “Efficient and exact sampling of simple graphs with given arbitrary degree sequence,” *PloS one*, vol. 5, no. 4, p. e10012, 2010.

[63] H. Kim, C. I. Del Genio, K. E. Bassler, and Z. Toroczkai, “Constructing and sampling directed graphs with given degree sequences,” *New Journal of Physics*, vol. 14, no. 2, p. 023012, 2012.

[64] O. Williams and C. I. Del Genio, “Degree correlations in directed scale-free networks,” *PloS one*, vol. 9, no. 10, p. e110121, 2014.

[65] K. E. Bassler, C. I. Del Genio, P. L. Erdős, I. Miklós, and Z. Toroczkai, “Exact sampling of graphs with prescribed degree correlations,” *New Journal of Physics*, vol. 17, no. 8, p. 083052, 2015.

[66] B. K. Fosdick, D. B. Larremore, J. Nishimura, and J. Ugander, “Configuring random graph models with fixed degree sequences,” *arXiv preprint arXiv:1608.00607*, 2016.

placeholder

Qing Cai received the B.S. degree in electronic information engineering from Wuhan Textile University, Wuhan, China, in 2010. He received the Ph.D. degree in Pattern Recognition and Intelligent Systems at the School of Electronic Engineering, Xidian University, Xi'an, China, in 2015. His current research interests are in the area of computational intelligence, complex network analytics, recommender systems and population ecology.

placeholder

Mahardhika Pratama received his PhD degree from the University of New South Wales, Australia in 2014. He completed his PhD in 2.5 years with a special approval of the UNSW higher degree committee due to his outstanding PhD research achievement. He is currently assistant professor at School of Computer Science and Engineering, Nanyang Technological University. Before joining NTU. He worked as a lecturer at the Department of Computer Science and IT, La Trobe University from 2015 till 2017. Prior to joining La Trobe University, he was with the Centre of Quantum Computation and Intelligent System, University of Technology, Sydney as a postdoctoral research fellow of Australian Research Council Discovery Project. Dr. Pratama received various competitive research awards in the past 5 years, namely the Institution of Engineers, Singapore (IES) Prestigious Engineering Achievement Award in 2011, the UNSW high impact publication award in 2013 and 2014. He recently has been appointed as Indonesias government world-class professor. Dr. Pratama has produced over 64 high-quality papers in journals and conferences and edited one book, and has been invited to deliver keynote speeches in international conferences. Dr. Pratama has led five special sessions and two special issues in prestigious conferences and journals. He currently serves as an editor in-chief of International Journal of Business Intelligence and Data Mining and a consultant at Lifebytes, Australia. Dr. Pratama is a member of IEEE, IEEE Computational Intelligent Society (CIS) and IEEE System, Man and Cybernetic Society (SMCS), and Indonesian Soft Computing Society (ISC-INA). His research interests involve machine learning, computational intelligent, evolutionary computation, fuzzy logic, neural network and evolving adaptive systems.

placeholder

Sameer Alam received the master's degree in computer science from Birla Institute of Technology, Mesra, India, in 1999 and the Ph.D. degree in computer science from University of New South Wales (UNSW), Canberra, Australia, in 2008. He is a Senior Lecturer in aviation with UNSW, Australia Defense Force Academy. He has authored over 40 peer-reviewed research articles and two books. His research interests include simulation, modeling, risk assessment, and the optimization of advanced air traffic management concepts. Dr. Alam is the Founding Member of the IEEE Computational Intelligence Society Chapter in Canberra. He is a Chief Investigator of ICAO-MIDRMA Collision Risk Project and served as a Co-Chief Investigator for several projects of Air Service Australia and EUROCONTROL. He is a recipient of the Australian National University Science Medal in 2011, the Tall Poppy Science Award in 2011, and the Fresh Science Award in 2009. He received four Best Paper Awards in premier air traffic conferences, including the IEEE DASC in 2010, the ATM Research and Devel- opment in 2011, the ATM Research and Development in 2015, and the ICRAT in 2014.

placeholder

Chunyao Ma received her B.S. degree in aircraft design from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2017. After that she had been working as a research associate with the School of Mechanical & Aerospace Engineering, Nanyang Technological University (NTU), Singapore. Currently she is a Ph.D. student at ATM Research Institute of NTU, Singapore. Her current research interests are in the area of Complex Network Analytics, Artificial Intelligence and Aviation Science.

placeholder

Jiming Liu is currently the Chair Professor of Computer Science and the Associate Vice-President (Research) at Hong Kong Baptist University. He received his M.Eng. and Ph.D. degrees from McGill University. His research interests include Data Analytics, Data Mining and Machine Learning, Complex Network Analytics, Data-Driven Complex Systems Modeling, and Health Informatics. He is a Fellow of the IEEE. Prof. Liu has served as the Editor-in-Chief of Web Intelligence Journal (IOS), and the Associate Editor of Big Data and Information Analytics (AIMS), IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Cybernetics, Neuroscience and Biomedical Engineering (Bentham), and Computational Intelligence (Wiley), among others.