Robustness evaluation of multipartite complex networks based on percolation theory

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

2020

Cai, Q., Alam, S., Pratama, M. & Liu, J. (2020). Robustness evaluation of multipartite complex networks based on percolation theory. IEEE Transactions On Systems, Man, and Cybernetics: Systems. <https://dx.doi.org/10.1109/TSMC.2019.2960156>

<https://hdl.handle.net/10356/147383>

<https://doi.org/10.1109/TSMC.2019.2960156>

© 2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at:
<https://doi.org/10.1109/TSMC.2019.2960156>

Downloaded on 26 Apr 2023 09:30:43 SGT

Robustness Evaluation of Multipartite Complex Networks Based on Percolation Theory

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

Abstract—To investigate the robustness of complex networks in face of disturbances can help prevent potential network disasters. Percolation on networks is a potent instrument for network robustness analysis. However, existing percolation theories are primarily developed for interdependent or multilayer networks. Little attention is paid to multipartite networks which are an indispensable part of complex networks. In this paper, we theoretically explore the robustness of multipartite networks under node failures. We put forward the generic percolation theory for gauging the robustness of multipartite networks with arbitrary degree distributions. Our developed theory is capable of quantifying the robustness of multipartite networks under either random or target node attacks. Our theory unravels the second order phase transition phenomenon for multipartite networks. In order to verify the correctness of the proposed theory, simulations on computer generated multipartite networks have been carried out. The experiments demonstrate that the simulation results coincide quite well with that yielded by the proposed theory.

Index Terms—Complex networks, multipartite networks, system control, percolation, network robustness

I. INTRODUCTION

COMPLEX systems such as transportation systems, power grid systems, etc., are ubiquitous and facilitate our daily lives unprecedentedly. Because a real-world complex system normally possesses many components and each of which can suffer from unpredictable external and/or internal disturbances [1], the focal system might be out of control as the failures of some system components can trigger cascading failures throughout the entire system [2, 3] and a system-level catastrophe is likely to occur. To ensure the stabilities of complex systems is therefore of pivotal significance towards reliable and better service providing [4, 5].

In order to better understand complex systems so as to take proactive measures to enhance their stabilities in face of perturbations, one of the most promising approaches is to model complex systems as complex networks and then apply network theories for problem-specific analysis [6]. In order to evaluate the capabilities of complex systems to withstand perturbations, the intriguing research agenda of network robustness came into being [7, 8]. Hitherto, tremendous endeavors have been made by researchers to gauge the robustness of complex networks in face of perturbations [9, 10].

Existing studies on network robustness can be roughly categorised into two branches, i.e., empirical studies [11–13] and theoretical studies [14–17]. Empirical studies mainly harness simulation methods to exploit the robustness of a network. More specifically, empirical studies generally evaluate the robustness of a given network by removing a fraction of components of the focal network based on certain network ranking strategies [18, 19] and then quantifying its robustness based on proper statistical metrics [20–22]. As a network is generally depicted by a graph consisting of nodes and edges, existing empirical studies thus could be archived into two classes, i.e., node-level robustness (robustness of networks to node failures) and edge-level robustness (robustness of networks to edge failures). With many networks are reported to display community structures (a community is universally recognized as a subgraph of a network that is densely inter-connected but sparsely intra-connected [23, 24]), a handful of empirical work has investigated the robustness of complex networks at the community level [25–27]. The paramount merits of empirical studies on network robustness are their simplicity and effectiveness. However, their principal demerit is that their implementations are time consuming when the studied network is large in size. Another drawback lies in their unexplainable nature, i.e., they cannot disclose the sciences beneath network dynamics. To circumvent those defects, theoretical studies eminently represented by percolation theories [28, 29] appeared. The last decade has witnessed the research enthusiasm on percolation theories for network robustness analysis [30].

Percolation on single layer networks, i.e., independent networks, has been well studied [7]. Nevertheless, complex networks in reality are commonly not independent but inter-dependent [31]. Consequently, failures on one network could elicit failures on its coupled networks, i.e., networks with which the focal network interacts, and eventually those failures would wreak havoc on the entire network. It is therefore pivotal to study the robustness of interdependent networks in face of perturbations [32, 33]. The seminal work in [28] for the first time investigated the robustness of interdependent or multilayer networks [34, 35]. It has been proved that multilayer networks are extremely vulnerable to disturbances. The pinnacle work in [28] has sparked the research flush on robustness analysis of multilayer networks. For instance, the outstanding work in [32] has developed the percolation theories for multilayer networks that are organized in diverse structures, while the distinguished work in [29] has derived the percolation theory for directed multilayer networks. Other splendid work can be found in [36, 37].

Q. Cai and S. Alam are with the School of Mechanical and Aerospace Engineering, Nanyang Technological University, Singapore, e-mail: sameer-alam@ntu.edu.sg.

M. Pratama is with the School of Computer Science and Engineering, Nanyang Technological University, Singapore, e-mail: mpratama@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.

Percolation on multilayer networks are well studied. However, little attention is paid to multipartite networks [7], which are an indispensable part of complex networks. Some real-world networks can be modeled as multipartite networks. For example, a mutualistic ecological network involving birds (act as seeds dispersers), plants, and butterflies (act as pollinators) can be modeled as a tripartite network in which each node set represents a certain category of species [26]. Some metabolic networks can be modeled as bipartite networks [38]. In the literature, several works have empirically exploited the robustness of multipartite networks [39, 40]. Nevertheless, to the best of our knowledge, there is no theoretical study (the work in [38, 41, 42] only investigates bipartite networks and those theories are not amenable to multipartite networks). With regard to this, this paper aims to theoretically investigate the robustness of multipartite networks. The contributions of this work are as follows:

- 1) We have elucidated the cardinal principles of existing network fragmentation models and the corresponding percolation theories for calculating the robustness of multilayer networks.
- 2) We have proved that the application of existing percolation theories to multipartite networks is infeasible due to the structural nuance between multipartite and multilayer networks.
- 3) We have established a non-cascading network fragmentation model for multipartite networks. Based on the established model we further devise the generic percolation theory for calculating the robustness of multipartite networks with arbitrary degree distributions under either random or target node attacks.
- 4) To validate the correctness of the proposed theory, we have carried out extensive simulations on artificial multipartite networks with Poisson degree distributions. The simulation results coincide quite well with the theoretical results.

The remainder of this paper is structured as follows. Section II presents related preliminaries with emphasis on the introductions to extant percolation theories. Section III details the reasons why extant percolation theories are not amenable to multipartite networks. Section IV delineates in detail our proposed generic percolation theory, including the introduced non-cascading network dynamic model and the corresponding mathematical derivations of the devised percolation theory for analyzing the robustness of multipartite network to random or target node attacks. Section V demonstrates the simulations on computer-generated multipartite networks with Poisson degree distributions and Section VI concludes the paper.

II. RELATED BACKGROUNDS

A. Basic Notations and Terminologies

A complex network is generally depicted by a graph that is composed of a set of nodes and edges [7]. A graph can be mathematically denoted by $G = \{V, E\}$, where V and E respectively represent the node set and edge set of G . Fig. 1(a) graphically exhibits a toy network G with seven nodes.

One of the frequently discussed terminologies concerning a complex network G is its adjacency matrix $\mathbf{A}_{N \times N}$, where $N = |V|$ is the number of nodes in G . The entry a_{ij} of matrix $\mathbf{A}$ reflects the relation between nodes i and j . For instance,

the value of a_{ij} can measure the connection intensity¹ between nodes i and j . Another frequently investigated terminologies concerning a network G is the degree of a node. The degree k_i of node i is defined as $k_i = \sum_j a_{ij}$. Along with the degree concept comes the concept of degree distribution. The degree distribution $P(k)$ of network G represents the probability distribution of degree k_i over the whole network.

Fig. 1. Graphical examples of (a) a single layer network, (b) a multilayer network with three subnetworks G_1 , G_2 and G_3 and (c) a multipartite network with three partite sets V_1 , V_2 and V_3 .

Now let us consider two special networks respectively shown in Fig. 1(b) and Fig. 1(c). The network shown in Fig. 1(b) consists of three networks G_1 , G_2 and G_3 (distinguished by different colors). Network G_1 correlates (has connections) with network G_2 and network G_2 correlates with network G_3 . In the literature, a network with this kind of structure is called a multilayer network² [31, 34, 49].

Now let us look at the network shown in Fig. 1(c) which has a quite similar structure to that of Fig. 1(b). It can be clearly seen from the figure that the only difference lies in the structures of networks G_1 , G_2 and G_3 . In Fig. 1(b) the nodes in each subnetwork have connections with one another. By contrast, in Fig. 1(c) the nodes in each ‘subnetwork’ are isolated. In the literature, a network possessing that kind of structure is termed as a multipartite network [7]. Each ‘subnetwork’ displayed in Fig. 1(c) is commonly called a partite set. Generally, the node set V of an L -partite network G can be denoted by $V = \{V_1, V_2, \dots, V_L\}$ with N_i be the number of nodes in the i -th partite set.

B. Quantitative Definition of Network Robustness

In the literature, the term “network robustness” generally refers to a network’s ability to withstand the failures of its components, i.e., nodes and edges. Without loss of generality, throughout this paper we only consider node failures as related definitions can be generalized to the case of edge failures.

Researchers so far have put forward a handful of quantitative definitions for network robustness [50]. One of the most utilized definitions is from [22]. Given a network G with N nodes, then its robustness R_n to node failures is defined

¹The connection intensity between nodes i and j also can be called the weight of edge e_{ij} . An adjacency matrix can be symmetric or asymmetric depending on how one models the connections between the nodes.

²In the literature, several synonyms of multilayer networks are interdependent networks [43, 44] and network of networks [32, 45]. In addition, please refer to refs. [37, 46–48] for extensive reading on multiplex networks.

as $R_n = \sum_{q=1}^N r_q$, where q is the number of the original failed nodes and r_q represents the portion of surviving nodes. Normally, the larger the value of R_n , the more robust the network is to node failures.

One can observe from the above definition that the calculation of R_n depends on r_q . Generally, r_q can be obtained through computer simulations or theoretical calculations. Computer simulations could be time consuming when the size of a network is large. Therefore, theoretical calculations will be more appealing for large scale networks. The most effective method as reported in the literature to calculate r_q is the percolation theory [8, 51] which will be introduced in what follows.

C. Percolation on Single Layer Networks

Percolation on networks aims to figure out the fraction of components that can survive component failures occurred to a network³. Specifically, when $1 - p$ fraction of nodes are removed from a given network G with degree distribution $P(k)$ (the removal of nodes is likely to fragment network G), the percolation theory is dedicated to calculating the fraction of nodes in the largest connected component (LCC), hereafter denoted by P^∞ (nodes in the LCC are regarded as the surviving nodes and P^∞ is therefore equivalent to r_q). Putting it another way, the purpose of percolation theory is to mathematically derive the following relation

$$P^\infty = F(p, P(k)), \quad (1)$$

where $F(\cdot)$ is a map function [16, 29]. Next, we are going to elaborate the percolation theory for a single layer network under a simple case where the fraction $1 - p$ of nodes are randomly removed.

Fig. 2. The key component for understanding the percolation theory for a single network under random node failures.

Fig. 2 demonstrates the key component that is pivotal to the understanding of percolation theory. As shown in Fig. 2 we randomly choose an edge from a network G and following the edge we reach a node a and let node b be the neighboring node of a . We further posit that apart from node a node b has k neighboring nodes.

Let us define u as the probability that node a is not connected to the LCC via node b . Now let us consider the event that node a is not connected to the LCC via node b . We can observe from Fig. 2 that if node b is removed, then the above mentioned event definitely happens and the probability

for it to happen is $1 - p$. We also could see from Fig. 2 that the above mentioned event still could happen even if node b is not removed as long as node b is not connected to the LCC via its neighboring nodes. It is easy to know that the event in this case happens with a probability $p \cdot u^k$. As a consequence, we can figure out the probability u as follows

$$u = 1 - p + \sum_{k=0}^{\infty} p u^k P^{ex}(k), \quad (2)$$

where $P^{ex}(k)$ is the probability for node b to have k excess (except node a) neighboring nodes.

Note that the probability for a randomly chosen node to have k neighbours is $P(k)$. Because node b is reached by node a , therefore $P^{ex}(k) \neq P(k)$. As node b totally has $k + 1$ neighboring nodes, thus $P^{ex}(k)$ practically equals the probability for a randomly chosen node to have $k + 1$ neighbours. As such, $P^{ex}(k)$ can be calculated as

$$P^{ex}(k) = \frac{N(k+1)P(k+1)}{N\langle k \rangle} = \frac{(k+1)P(k+1)}{\langle k \rangle}, \quad (3)$$

where $\langle k \rangle = \sum P(k)k$ is the mean degree of network G .

The probability for a node with degree k to exist in the LCC is $P(k)(1 - u^k)$. After randomly removing $1 - p$ fraction of nodes from a given network G , the fraction of nodes that eventually exist in the LCC is therefore calculated as

$$P^\infty = p \sum_{k=0}^{\infty} P(k)(1 - u^k). \quad (4)$$

In the literature, the tool of generating function is widely used for scientific computing. The generating function for a probability distribution function $P(k)$ can be written as

$$G(x) = \sum_{k=0}^{\infty} P(k)x^k. \quad (5)$$

Analogously, the generating function for $P^{ex}(k)$ can be formulated as

$$H(x) = \sum_{k=0}^{\infty} P^{ex}(k)x^k = \frac{G'(x)}{G'(1)}. \quad (6)$$

Equipped with the generating functions, Eqs. 2 and 4 thus can be simplified as

$$u = 1 - p + pH(u), \quad (7)$$

$$P^\infty = p(1 - G(u)). \quad (8)$$

For a given network with known degree distribution, when randomly removing $1 - p$ fraction of nodes from the network, the percolation theory delineated in the above two equations could mathematically calculate the fraction of nodes that can survive the node failures.

³If node failure is of concern, then the corresponding theory is called site percolation. If edge failure is considered, then the corresponding theory is called bond percolation [16].

D. Percolation on O2O Coupled Multilayer Networks

As emphasized earlier that complex networks in reality are structured in a multilayer style. Component failures in one network are very likely to trigger cascading failures in other networks and system disasters could occur. It is therefore essentially pertinent to investigate the robustness of multilayer networks. Percolation theory introduced in subsection II-C for single layer networks definitely does not apply to multilayer networks.

With regard to this, the seminal work in [28] investigated the robustness of two-layer networks. The authors put forward the network dynamic model illustrated in Fig. 3 to depict the dynamic process on two-layer networks with one-to-one (O2O) correlations.

Fig. 3. Network fragmentation model for analyzing the robustness of multilayer networks with one-to-one correlations. Initially node 5 from network A is removed. Due to the O2O correlations, node 5 in network B is also eliminated in Stage 1 and network A breaks into three clusters, denoted by a_{11} , a_{12} and a_{13} . In Stage 2, nodes 4 and 6 both in networks A and B together with the links attached to them are removed, and network B breaks into four clusters, namely b_{21} , b_{22} , b_{23} and b_{24} . In Stage 3, node 3 in network A is removed and network A breaks into four clusters. Because in Stage 3 no further link elimination and network breaking occur, therefore the cluster consist of a_{34} and b_{24} , also the LCC, survives.

Based on the proposed dynamic model the authors further developed the corresponding percolation theory for measuring the robustness of two-layer networks. Assume that networks A and B have equal size and let $P_A(k)$ and $P_B(k)$ respectively be their degree distributions. Initially we randomly remove $1 - p$ fraction of nodes from network A. We then let the cascading failures propagate on the network in the way shown in Fig. 3. In the final stable stage, the fraction of nodes in the LCC of the focal network is calculated as

$$P^\infty = xg_B(x) = yg_A(y), \quad (9)$$

where $g_A(y) = 1 - G_A(1 - y(1 - f_A))$ and $g_B(x) = 1 - G_B(1 - x(1 - f_B))$ with $G_A(\cdot)$ and $G_B(\cdot)$ respectively being the generating functions of $P_A(k)$ and $P_B(k)$.

The four unknowns x , y , f_A and f_B are calculated as (please refer to [28])

$$\begin{cases} x = p(1 - G_A(1 - y(1 - f_A))) \\ y = p(1 - G_B(1 - x(1 - f_B))) \end{cases}, \quad (10)$$

$$\begin{cases} f_A = H_A(1 - y(1 - f_A)) \\ f_B = H_B(1 - x(1 - f_B)) \end{cases}, \quad (11)$$

with $H_A(\cdot)$ and $H_B(\cdot)$ respectively being the generating functions of the excess degree distribution $P_A^{ex}(k)$ and $P_B^{ex}(k)$.

Based on the above theory the authors have found a simple form of the critical value p_c (once a fraction $1 - p_c$ of nodes are removed from network A, the whole network will collapse) which reads

$$p_c = \frac{2.4554}{\langle k \rangle}, \quad (12)$$

under the condition that $P_A(k) = P_B(k) = e^{-\langle k \rangle} \frac{\langle k \rangle^k}{k!}$, i.e., networks A and B follow the same Poisson distribution.

It has been discovered that the robustness of two-layer networks with O2O correlations display first-order phase transition phenomenon, which indicates that two-layer networks with O2O correlations are extremely fragile to node failures.

III. RESEARCH PROBLEM AND MOTIVATIONS

A. Definition of Research Problem

This paper aims to develop the percolation theory for measuring the robustness of multipartite networks to either random or target node attacks. A specific description of the research problem is provided below.

Consider an L -partite network G . We define $P_{ij}(k)$ as the degree distribution of the nodes in V_i that have edges with nodes in V_j , neglecting the edges that the nodes in V_i have with nodes in other partite set, if any. Assume that $1 - p_i$ fraction of nodes from V_i for $\forall i \in [1, L]$ with $p_i \in [0, 1]$ are removed from G based on a given node attack model which specifies the probability for each node to be removed. Afterward, based on a prescribed network fragmentation model, G fragments into different parts and the LCC is considered. Then the research problem is to figure out the mathematical relationship between P_i^∞ , $P_{ij}(k)$ and p_i with P_i^∞ being the fraction of nodes in V_i that are remained in the LCC.

For a given L -partite network G , we adopt the node attack model investigated in [51, 52]. To be specific, we remove node i with degree k_i from partite set V_j with N_j nodes based on the following probability

$$w_\alpha = \frac{k_i^\alpha}{\sum_{i=1}^{N_j} k_i^\alpha}, \quad (13)$$

where α is a constant. Eq. 13 calculates the probability for a node to be removed. If $\alpha = 0$, then $w_\alpha = \frac{1}{N_j}$. In this case, every node is removed with the same probability which corresponds to the random node removal situation. If $\alpha > 0$, then nodes with larger degrees have higher removal probabilities. On the contrary, nodes with larger degrees have lower removal probabilities if $\alpha < 0$.

Note that percolation on complex networks relies on the network fragmentation models. Different models will lead to different ways of characterizing the LCC of a focal network which will eventually affect the calculation of P_i^∞ . We illustrate the proposed fragmentation model in Section IV.

B. Research Motivations

1) Limit of Theory for Single Layer Networks

Percolation theory for single layer networks is not applicable to multipartite networks. It can be seen from subsection II-C that the percolation theory formulated in Eqs. 7 and 8 involves variable u which is a function of $P(k)$. Nevertheless, the definition presented in the above subsection indicates that an L -partite network involves $2 \times (L - 1)$ degree distribution functions of $P_{ij}(k)$. Besides, node failures may only occur to only one partite set of an L -partite network. Putting it another way, the node failures in one partite set may not change the degree distributions of nodes in other partite sets. As a consequence, the percolation theory for single layer networks is only applicable to multipartite networks under the following conditions: 1) $N_i = N_j$ for all $i \in [1, L]$; 2) the $2 \times (L - 1)$ degree distribution functions of $P_{ij}(k)$ are the same; 3) node failures occur to V_i for all $i \in [1, L]$.

2) Limit of Theory for O2O Coupled Multilayer Networks

The percolation theory illustrated in subsection II-D for O2O coupled two-layer networks also is not applicable to multipartite networks. Even though its successive work in [32] perfects the percolation theory for L -layer networks, the corresponding theories still do not work for multipartite networks. The reason is that all those theories are based on the hypothesis that the studied multilayer network is with O2O correlations, while a multipartite network is organized in a way of one-to-many (O2M) correlations, i.e., a node in partite set V_i could have connections with more than one nodes in partite set V_{i-1} and/or partite set V_{i+1} .

3) Limit of Theory for O2M Coupled Multilayer Networks

To circumvent the limit of percolation theories for O2O coupled multilayer networks, scientists have explored the percolation theories for analyzing the robustness of multilayer networks with O2M correlations [15, 53, 54].

Fig. 4 displays the dynamic model utilized in [54] for analyzing the robustness of two-layer networks with O2M correlations. Let $P_A^{out}(k)$ (and $P_B^{out}(k)$) be the degree distribution of the nodes in A (and B) that have correlations with nodes in B (and A). Assume that a fraction $1 - p_A$ and a fraction $1 - p_B$ of nodes are randomly removed from A and B, respectively. Based on the model shown in Fig. 4 the authors then have devised the following system of equations (go to ref. [54] for details)

$$\begin{cases} f_A = H_A(1 - u_A(1 - f_A)) \\ f_B = H_B(1 - u_B(1 - f_B)) \\ u_A = p_A(1 - G_A^{out}(1 - P_B^\infty)) \\ u_B = p_B(1 - G_B^{out}(1 - P_A^\infty)) \end{cases}, \quad (14)$$

$$\begin{cases} P_A^\infty = u_A(1 - G_A(1 - u_A(1 - f_A))) \\ P_B^\infty = u_B(1 - G_B(1 - u_B(1 - f_B))) \end{cases}, \quad (15)$$

where f_A , f_B , u_A and u_B are four unknowns. G_A^{out} and G_B^{out} are respectively the generating functions of $P_A^{out}(k)$ and $P_B^{out}(k)$.

One may argue based on Fig. 1 that a multipartite network is a simplified multilayer network with O2M correlations. However, it is easy to prove that the above percolation theory

Fig. 4. Network fragmentation model for analyzing the robustness of interdependent networks with one-to-many correlations. Arrows represent the support links connecting a support node in one network to the dependent node in the other network. Initially, the attacks are on node 1 in A and node 6 in B. For network A in Stage 1, node 7 fails because of it has no support links, and nodes 2 and 6 are eliminated because they do not belong to the LCC of A. For network B in Stage 1, nodes 1, 2 and 7 fail because of no support, and node 3 is removed since it is not in the LCC of B. The above processes continue until a stable state is reached.

still does not fit for multipartite networks. For one thing, it is laborious to extend the above theory to the case of L -layer networks. For another thing, the above theory involves functions $P_A(k)$ and $P_B(k)$ while $P_A(k) = P_B(k) \equiv 0$ for a bipartite network.

IV. METHODOLOGY

A. Network Fragmentation Model

Section III has elaborated the infeasibility of applications of the network models delineated in Figs. 3 and 4 to multipartite networks. In this paper we put forward a non-cascading model for evaluating the robustness of multipartite networks under attacks.

Fig. 5 depicts our proposed non-cascading model. As a multipartite network could be fragmented into different clusters when it is under attacks, our proposed model posits that only nodes in the LCC of the focal multipartite network are of concern. When calculating the robustness of the focal network, our model calculates the fraction of nodes in the LCC.

B. Network Equivalent Model for Target Attacks

In order to derive the percolation theory for multipartite networks subject to node attacks with the adopted model shown in Eq. 13, we introduce the following network equivalent model displayed in Fig. 6.

Fig. 6 cites a bipartite network G with two node sets V_1 and V_2 as an example to elucidate the principle of the equivalent model. As shown in Fig. 6, the symbols $P_1(k)$ and $P_2(k)$ respectively denote the degree distributions of nodes in V_1 and V_2 . When intentionally removing $1 - p$ fraction of nodes from V_1 , the degree distributions of the remaining nodes in V_1 and V_2 all change (denoted by $P_1^r(k)$ and $P_2^r(k)$ in Fig. 6). The

Fig. 5. Our proposed non-cascading model for depicting the dynamic process on multipartite networks under node attacks. Initially, node 2 is under attack. In Stage 1, node 2 is removed from the focal network. In Stage 2 the removal of node 2 fragments the focal network into two parts. In Stage 3 we remove nodes that do not belong to the LCC and only nodes in the LCC are remained.

Fig. 6. Our introduced network equivalent model for transforming network target attacks to the case of random attacks.

equivalent model aims to find an equivalent bipartite network $\tilde{G}$ with the same number of nodes such that after randomly removing $1 - p$ fraction of nodes from V_1 of $\tilde{G}$ the degree distributions of the remaining nodes in V_1 and V_2 are equal to that of G . Specifically, we have the equivalent condition as follows

$$P_i^r(k) = \widetilde{P_i^r(k)} \iff P_i(k) = \widetilde{P_i(k)}. \quad (16)$$

Because it is generally more convenient to utilize the tool of generating functions instead of the probability distribution functions as the former is computationally appealing, thus we could reformulate Eq. 16 into the following form

$$G_i^r(k) = \widetilde{G_i^r(k)} \iff G_i(k) = \widetilde{G_i(k)}. \quad (17)$$

Note that target node attacks on a multipartite network only changes its degree distribution but does not affect the dynamic model exhibited in Fig. 5. By harnessing the equivalent network model we can transfer the target attack situation to a random attack case thereby mitigating the laborious development of the corresponding percolation theory.

C. Degree Distributions of Remaining Nodes

For a given L -partite network, we remove $1 - p_i$ fraction of nodes from V_i for all $i \in [1, L]$ based on Eq. 13. We define

$P_{ij}^r(k)$ as the degree distribution of the remaining nodes in V_i that have connections with nodes in V_j . In what follows we elucidate in detail the calculation of $P_{ij}^r(k)$.

1) *Case 1 of Bipartite Networks:* For simplicity, we first investigate the simple case of bipartite networks. Let $f_1(p_1)$ be the number of nodes with degree k in V_1 after removing $1 - p_1$ fraction of nodes from V_1 based on Eq. 13 (we do not remove nodes from V_2 in case 1). Because $P_{12}(k)$ changes to be $P_{12}^r(k)$, therefore we have

$$f_1(p_1) = P_{12}^r(k) \cdot N_1 \cdot p_1. \quad (18)$$

Now let us consider the situation that one more node is removed from V_1 . In this case, $f_1(p_1)$ changes to be $f_1(p_1 - \frac{1}{N_1})$ and it can be calculated as

$$f_1(p_1 - \frac{1}{N_1}) = f_1(p_1) - \frac{P_{12}^r(k)k^\alpha}{\sum_{k=0}^{N_1} P_{12}^r(k)k^\alpha}. \quad (19)$$

Recall the definition of derivative⁴, if $N_1 \rightarrow \infty$, then the above equation could be reformulated in the way of derivative of $f_1(p_1)$ with respect to the variable p_1 in the following form

$$\frac{df_1(p_1)}{dp_1} = N_1 \frac{P_{12}^r(k)k^\alpha}{\sum_{k=0}^{N_1} P_{12}^r(k)k^\alpha}. \quad (20)$$

By calculating the derivative of Eq. 18 we have

$$\frac{df_1(p_1)}{dp_1} = \frac{dP_{12}^r(k)}{dp_1} \cdot N_1 \cdot p_1 + P_{12}^r(k) \cdot N_1. \quad (21)$$

Substituting Eq. 20 into Eq. 21 we have

$$p_1 \frac{dP_{12}^r(k)}{dp_1} + P_{12}^r(k) = \frac{P_{12}^r(k)k^\alpha}{\sum_{k=0}^{N_1} P_{12}^r(k)k^\alpha}. \quad (22)$$

Eq. 22 is a first order nonlinear differential equation of $P_{12}^r(k)$. In order to solve Eq. 22, we define

$$\varphi_{12}(x) = \sum_{k=0}^{\infty} P_{12}(k)x^{k^\alpha}, \quad (23)$$

$$t_{12} = \varphi_{12}^{-1}(p_1) = \left[\sum_{k=0}^{\infty} P_{12}(k)p_1^{k^\alpha} \right]^{-1}, \quad (24)$$

⁴The derivative of $f(x)$ with respect to x is the function $f'(x)$ and is defined as $f'(x) = \lim_{h \rightarrow 0} \frac{f(x+h) - f(x)}{h}$.

where $\varphi_{12}^{-1}(p_1)$ represents the inverse function of $\varphi_{12}(p_1)$, i.e., we have $p_1 = \varphi_{12}(t_{12})$.

With the above definitions we find the solution to Eq. 22 as

$$P_{12}^r(k) = \frac{P_{12}(k)t_{12}^{k\alpha}}{\varphi_{12}(t_{12})} = \frac{1}{p_1} P_{12}(k)t_{12}^{k\alpha}. \quad (25)$$

Eq. 25 mathematically computes the degree distribution of the remaining nodes in V_1 . Next we illustrate in detail the calculation of $P_{21}^r(k)$. One important thing should be pointed out that when removing $1-p_1$ fraction of nodes from V_1 based on Eq. 13, whether we keep the edges attached to the removed nodes or not will not change the degree distribution $P_{12}^r(k)$ as $P_{12}^r(k)$ is immediately determined upon the removal of nodes from V_1 . Removing the edges attached to the removed nodes only changes the degree distribution $P_{21}(k)$.

Note that no nodes are removed from V_2 . Before the node attacks happen, totally there are $|E|$ edges in G and $|E|$ could be calculated as

$$|E| = N_1 \langle k_{12} \rangle = N_1 \sum_{k=0}^{\infty} k P_{12}(k). \quad (26)$$

After the node attacks, the number of edges remained in G becomes $|E^r|$ which is calculated as

$$|E^r| = N_1 \langle k_{12}^r \rangle = p_1 N_1 \sum_{k=0}^{\infty} k P_{12}^r(k). \quad (27)$$

Therefore, the proportion $\widetilde{p}_{12}$ of the remaining edges is

$$\widetilde{p}_{12} = \frac{|E^r|}{|E|} = \frac{\sum_{k=0}^{\infty} k P_{12}(k) t_{12}^{k\alpha}}{\sum_{k=0}^{\infty} k P_{12}(k)}. \quad (28)$$

As the edges of G are randomly connected to nodes in V_2 , removing the edges attached to the removed nodes in V_1 is equal to randomly remove $1 - \widetilde{p}_{12}$ fraction of edges attached to nodes in V_2 . Therefore, the degree distribution $P_{21}^r(k)$ can be calculated as follows

$$P_{21}^r(k) = P_{21}(k) \sum_{m=0}^k \binom{k}{m} \widetilde{p}_{12}^m (1 - \widetilde{p}_{12})^{k-m}. \quad (29)$$

2) *Case 2 of Bipartite Networks:* Case 1 only deals with the situation where node attacks occur to V_1 . Here we investigate the case that the node attacks happen to both partite sets of a bipartite network. After respectively removing $1-p_1$ fraction and $1-p_2$ fraction of nodes from V_1 and V_2 together with the edges attached to those removed nodes, in accordance with the theory exhausted above we can respectively recalculate the degree distributions of the remaining nodes in V_1 and V_2 as follows

$$P_{12}^r(k) = \frac{1}{p_1} P_{12}(k) \sum_{m=0}^k \binom{k}{m} \widetilde{p}_{21}^m (1 - \widetilde{p}_{21})^{k-m} t_{12}^{k\alpha}, \quad (30)$$

$$P_{21}^r(k) = \frac{1}{p_2} P_{21}(k) \sum_{m=0}^k \binom{k}{m} \widetilde{p}_{12}^m (1 - \widetilde{p}_{12})^{k-m} t_{21}^{k\alpha}, \quad (31)$$

where the calculations of variables t_{12} and $\widetilde{p}_{12}$ are respectively given in Eqs. 24 and 28, while the variables $\widetilde{p}_{21}$ and t_{21} are respectively calculated as

$$\widetilde{p}_{21} = \frac{\sum_{k=0}^{\infty} k P_{21}(k) t_{21}^{k\alpha}}{\sum_{k=0}^{\infty} k P_{21}(k)}, \quad (32)$$

$$t_{21} = \varphi_{21}^{-1}(p_2) = \left[\sum_{k=0}^{\infty} P_{21}(k) p_2^{k\alpha} \right]^{-1}. \quad (33)$$

3) *Simple Case of Multipartite Networks:* The above deductions only analyze the special case of bipartite networks. Here we investigate multipartite networks. We first consider the simple situation where target node attacks only happen to one partite set of an L -partite network. Specifically, we only remove nodes from V_i for $\forall i \in [2, L-1]$ as it is easy to figure out the cases of $i=1$ and $i=L$ based on Eqs. 25 and 29.

Note that removing nodes from V_i of an L -partite network only changes degree distributions $P_{i-1,i}(k)$, $P_{i,i-1}(k)$, $P_{i,i+1}(k)$ and $P_{i+1,i}(k)$. One thing that should be kept in mind is that a node in partite set V_i could have neighbours in both partite sets V_{i-1} and V_{i+1} . Consequently, the node removing probability given in Eq. 13 should be calculated based on the degrees of the nodes in V_i .

After intentionally removing $1-p_i$ fraction of nodes from V_i but keeping the edges attached to the removed nodes, we can work out $P_i^r(k)$ by the same token exhausted in subsection IV-C1 as follows

$$P_i^r(k) = \frac{P_i(k)t_i^{k\alpha}}{\varphi_i(t_i)} = \frac{1}{p_i} P_i(k)t_i^{k\alpha}, \quad (34)$$

where function $\varphi_i(z)$ and t_i are respectively calculated as

$$\varphi_i(z) = \sum_{k=0}^{\infty} P_i(k) z^{k\alpha}, \quad (35)$$

$$t_i = \varphi_i^{-1}(p_i) = \left[\sum_{k=0}^{\infty} P_i(k) p_i^{k\alpha} \right]^{-1}. \quad (36)$$

Let $|E_i|$ be the number of edges that connect nodes in V_{i-1} , V_i and V_{i+1} . After the node attacks $|E_i|$ becomes $|E_i^r|$. Therefore, the proportion of $|E_i^r|$ to $|E_i|$ becomes

$$\widetilde{p}_i = \frac{|E_i^r|}{|E_i|} = \frac{\sum_{k=0}^{\infty} k P_i(k) t_i^{k\alpha}}{\sum_{k=0}^{\infty} k P_i(k)}, \quad (37)$$

which indicates a proportion of $1 - \widetilde{p}_i$ edges attached to the removed nodes will be deleted.

Note that removing the edges attached to the removed nodes is equal to randomly removing the same proportion of edges attached to nodes in V_{i-1} and V_{i+1} . Consequently, we can respectively figure out the degree distributions of nodes in V_{i-1} and V_{i+1} as

$$P_{i-1,i}^r(k) = P_{i-1,i}(k) \sum_{m=0}^k \binom{k}{m} \widetilde{p}_i^m (1 - \widetilde{p}_i)^{k-m}, \quad (38)$$

$$P_{i+1,i}^r(k) = P_{i+1,i}(k) \sum_{m=0}^k \binom{k}{m} \tilde{p}_i^m (1 - \tilde{p}_i)^{k-m}. \quad (39)$$

The key component for the simple case of multipartite networks lies in the calculation of $P_{i,i-1}^r(k)$ and $P_{i,i+1}^r(k)$. It is easy to work out $P_{i,i-1}^r(k)$ and $P_{i,i+1}^r(k)$ in many wrong ways like substituting $P_i(k) = P_{i,i-1}(k) + P_{i,i+1}(k)$ or $P_i(k) = P_{i,i-1}(k) \cdot P_{i,i+1}(k)$ into Eq. 34. The right way to work out them is to follow the idea elucidated in subsection IV-C1. In such a way, we have to work out the corresponding node removal proportions $1 - p_{i,i-1}$ and $1 - p_{i,i+1}$ respectively for the bipartite network $G_{i,i-1}$ consisting of nodes in V_{i-1} and V_i and the bipartite network $G_{i,i+1}$ consisting of nodes in V_{i+1} and V_i .

Note that the node removal probability given in Eq. 13 should be calculated based on the degree of the nodes in V_i . Because the event for nodes in V_i of $G_{i,i-1}$ to have degree distribution $P_{i,i-1}(k)$ and the event for nodes in V_i of $G_{i,i+1}$ to have degree distribution $P_{i,i+1}(k)$ are independent, therefore when removing $1 - p_i$ fraction of nodes from V_i , the equivalent proportions $p_{i,i-1}$ and $p_{i,i+1}$ should be proportional to the corresponding mean degrees. More specifically, we can calculate $p_{i,i-1}$ and $p_{i,i+1}$ in the following way

$$p_{i,i-1} = p_i^{\langle k_{i,i-1} \rangle / \langle k_i \rangle}, \quad (40)$$

$$p_{i,i+1} = p_i^{\langle k_{i,i+1} \rangle / \langle k_i \rangle}. \quad (41)$$

By the same token illustrated in subsection IV-C1 we can therefore figure out $P_{i,i-1}^r(k)$ and $P_{i,i+1}^r(k)$ as follows

$$P_{i,i-1}^r(k) = \frac{1}{p_{i,i-1}} P_{i,i-1}(k) t_i^{k^\alpha}, \quad (42)$$

$$P_{i,i+1}^r(k) = \frac{1}{p_{i,i+1}} P_{i,i+1}(k) t_i^{k^\alpha}. \quad (43)$$

It should be pointed out that in the above equations the variable t_i is calculated by Eq. 36 but not by the similar way as presented in Eq. 24.

4) *General Case of Multipartite Networks*: Now we investigate the general case of L -partite networks where node attacks occur to V_i for all $i \in [1, L]$. With out loss of generality, we consider partite set V_{i-1} , V_i and V_{i+1} . After intentionally removing nodes from the three partite sets, we could derive the degree distributions of the remaining nodes in the three partite sets sectionally. We first compute $P_{ij}^r(k)$ based on Eqs. 42 and 43 when removing the nodes but keeping all the edges attached to them. Afterward, we further compute $P_{ij}^r(k)$ based on Eqs. 38 and 39 when removing all the edges attached to the removed nodes. In summary, we have the following explicit forms of $P_{ij}^r(k)$

$$P_{i-1,i}^r(k) = \frac{1}{p_{i-1,i}} P_{i-1,i}(k) \sum_{m=0}^k \binom{k}{m} \tilde{p}_i^m (1 - \tilde{p}_i)^{k-m} t_i^{k^\alpha}, \quad (44)$$

$$P_{i,i-1}^r(k) = \frac{1}{p_{i,i-1}} P_{i,i-1}(k) \sum_{m=0}^k \binom{k}{m} \widetilde{p_{i-1}}^m (1 - \widetilde{p_{i-1}})^{k-m} t_i^{k^\alpha}, \quad (45)$$

$$P_{i,i+1}^r(k) = \frac{1}{p_{i,i+1}} P_{i,i+1}(k) \sum_{m=0}^k \binom{k}{m} \widetilde{p_{i+1}}^m (1 - \widetilde{p_{i+1}})^{k-m} t_i^{k^\alpha}, \quad (46)$$

$$P_{i+1,i}^r(k) = \frac{1}{p_{i+1,i}} P_{i+1,i}(k) \sum_{m=0}^k \binom{k}{m} \tilde{p}_i^m (1 - \tilde{p}_i)^{k-m} t_{i+1}^{k^\alpha}. \quad (47)$$

D. Equivalent Multipartite Network

To this end, we have mathematically figured out the degree distribution $P_{ij}^r(k)$ of the remaining nodes in an L -partite network G after intentionally removing $1 - p_i$ fraction of nodes from V_i for all $i \in [1, L]$. As aforementioned, the equivalent model aims to find an equivalent network $\tilde{G}$ such that after randomly removing $1 - \widetilde{p_i}$ fraction of nodes from V_i of $\tilde{G}$, the degree distribution $\widetilde{P_{ij}^r}(k)$ of the remaining nodes in $\tilde{G}$ is equal to that of $P_{ij}^r(k)$. Next we show how to figure out $\widetilde{P_{ij}^r}(k)$.

For an L -partite network $\tilde{G}$ we randomly remove $1 - p_i$ fraction of nodes from V_i for all $i \in [1, L]$. Let us consider the bipartite network consisting nodes in V_i and V_{i+1} . Note that randomly removing $1 - p_i$ fraction of nodes from V_i does not change $\widetilde{P_{i,i+1}}(k)$ but changes $\widetilde{P_{i+1,i}}(k)$. Analogously, randomly removing $1 - p_{i+1}$ fraction of nodes from V_{i+1} only changes $\widetilde{P_{i,i+1}}(k)$ but will not change $\widetilde{P_{i+1,i}}(k)$. The degree distribution of the remaining nodes in V_i can be calculated as

$$\widetilde{P_{i,i+1}^r}(k) = \widetilde{P_{i,i+1}}(k) \sum_{m=0}^k \binom{k}{m} p_{i+1}^m (1 - p_{i+1})^{k-m}. \quad (48)$$

Analogous, we have

$$\widetilde{P_{i+1,i}^r}(k) = \widetilde{P_{i+1,i}}(k) \sum_{m=0}^k \binom{k}{m} p_i^m (1 - p_i)^{k-m}. \quad (49)$$

In compliance with the above derivations, we then could find out the equivalent network $\tilde{G}$ by combining and solving Eqs. 17, 48 and 49. To keep consistency with the network scenarios investigated in subsection IV-C, next we will present the detailed equivalent model for each network case.

1) *Equivalent Model for Case 1 of Bipartite Networks*: When the target node attacks only occur to V_1 of a bipartite network, we could get the following equivalent model

$$G_{12}^r(z) = \frac{1}{p_1} \sum_{k=0}^{\infty} P_{12}(k) t_1^{k^\alpha} z^k = \widetilde{G_{12}}(z), \quad (50)$$

$$\begin{aligned}
G_{21}^r(z) &= \sum_{k=0}^{\infty} P_{21}^r(k) z^k = G_{21} (1 - \widetilde{p}_{12} + \widetilde{p}_{12} z) \\
&= \widetilde{G}_{21} (1 - p_1 + p_1 z) \\
\Rightarrow \widetilde{G}_{21}(z) &= G_{21} \left(1 - \frac{\widetilde{p}_{12}}{p_1} + \frac{\widetilde{p}_{12}}{p_1} z \right)
\end{aligned} \quad (51)$$

2) Equivalent Model for Case 2 of Bipartite Networks:

When the target node attacks simultaneously occur to V_1 and V_2 of a bipartite network, we could get the following equivalent model

$$\begin{aligned}
G_{12}^r(z) &= \sum_{k=0}^{\infty} \frac{1}{p_1} P_{12}(k) \sum_{m=0}^k \binom{k}{m} \widetilde{p}_{21}^m (1 - \widetilde{p}_{21})^{k-m} t_{12}^{k^\alpha} z^k \\
&= \widetilde{G}_{12} (1 - p_2 + p_2 z)
\end{aligned} \quad (52)$$

$$\begin{aligned}
G_{21}^r(z) &= \sum_{k=0}^{\infty} \frac{1}{p_2} P_{21}(k) \sum_{m=0}^k \binom{k}{m} \widetilde{p}_{12}^m (1 - \widetilde{p}_{12})^{k-m} t_{21}^{k^\alpha} z^k \\
&= \widetilde{G}_{21} (1 - p_1 + p_1 z)
\end{aligned} \quad (53)$$

3) Equivalent Model for Simple Case of Multipartite Networks:

Without loss of generality, in the next we only consider tripartite networks, as we can see from subsection IV-C that intentional node attacks to V_i for $\forall i \in [2, L-1]$ only affects the degree distributions of nodes in V_i and of nodes that have connections with V_i .

When the node attacks occur to V_2 of a tripartite network, then we could arrive at the following equivalent model

$$\begin{aligned}
G_{12}^r(z) &= \sum_{k=0}^{\infty} P_{12}(k) \sum_{m=0}^k \binom{k}{m} \widetilde{p}_2^m (1 - \widetilde{p}_2)^{k-m} z^k \\
&= \widetilde{G}_{12} (1 - p_2 + p_2 z) \\
\Rightarrow \widetilde{G}_{12}(z) &= G_{12} \left(1 - \frac{\widetilde{p}_2}{p_2} + \frac{\widetilde{p}_2}{p_2} z \right)
\end{aligned} \quad (54)$$

$$G_{21}^r(z) = p_2^{-(k_{21})/\langle k_2 \rangle} \sum_{k=0}^{\infty} P_{21}(k) t_2^{k^\alpha} z^k = \widetilde{G}_{21}(z), \quad (55)$$

$$G_{23}^r(z) = p_2^{-(k_{23})/\langle k_2 \rangle} \sum_{k=0}^{\infty} P_{23}(k) t_2^{k^\alpha} z^k = \widetilde{G}_{23}(z), \quad (56)$$

$$\begin{aligned}
G_{32}^r(z) &= \sum_{k=0}^{\infty} P_{32}(k) \sum_{m=0}^k \binom{k}{m} \widetilde{p}_2^m (1 - \widetilde{p}_2)^{k-m} z^k \\
&= \widetilde{G}_{32} (1 - p_2 + p_2 z) \\
\Rightarrow \widetilde{G}_{32}(z) &= G_{32} \left(1 - \frac{\widetilde{p}_2}{p_2} + \frac{\widetilde{p}_2}{p_2} z \right)
\end{aligned} \quad (57)$$

4) *Equivalent Model for General Case of Multipartite Networks:* When node attacks occur to every partite set of a tripartite network, we could elicit the following equivalent model

$$\begin{aligned}
G_{12}^r(z) &= \frac{1}{p_1} \sum_{k=0}^{\infty} \sum_{m=0}^k P_{12}(k) \binom{k}{m} \widetilde{p}_2^m (1 - \widetilde{p}_2)^{k-m} t_1^{k^\alpha} z^k \\
&= \widetilde{G}_{12} (1 - p_2 + p_2 z)
\end{aligned} \quad (58)$$

$$\begin{aligned}
G_{21}^r(z) &= \frac{1}{p_{21}} \sum_{k=0}^{\infty} \sum_{m=0}^k P_{21}(k) \binom{k}{m} \widetilde{p}_1^m (1 - \widetilde{p}_1)^{k-m} t_2^{k^\alpha} z^k \\
&= \widetilde{G}_{21} (1 - p_1 + p_1 z)
\end{aligned} \quad (59)$$

$$\begin{aligned}
G_{23}^r(z) &= \frac{1}{p_{23}} \sum_{k=0}^{\infty} \sum_{m=0}^k P_{23}(k) \binom{k}{m} \widetilde{p}_3^m (1 - \widetilde{p}_3)^{k-m} t_2^{k^\alpha} z^k \\
&= \widetilde{G}_{23} (1 - p_3 + p_3 z)
\end{aligned} \quad (60)$$

$$\begin{aligned}
G_{32}^r(z) &= \frac{1}{p_3} \sum_{k=0}^{\infty} \sum_{m=0}^k P_{32}(k) \binom{k}{m} \widetilde{p}_2^m (1 - \widetilde{p}_2)^{k-m} t_3^{k^\alpha} z^k \\
&= \widetilde{G}_{32} (1 - p_2 + p_2 z)
\end{aligned} \quad (61)$$

E. Robustness of Multipartite Networks Under Random Attacks

The above derivations have elucidated how to convert the problem of robustness analysis of multipartite networks under target node attacks to the problem of robustness analysis of multipartite networks under random node attacks, as the later one is easier to be solved. In the next we will present our developed percolation theory for analyzing the robustness of multipartite networks under random node attacks.

For a given L -partite network G , we randomly remove $1 - p_i$ fraction of nodes from V_i for all $i \in [1, L]$. In order to figure out P_i^∞ , we first define a set of variables in the form of u_{ij} which represents the probability that a node in V_i is not connected to the LCC via one of its neighbours in V_j where $j = i + 1$ or $j = i - 1$. As a consequence, we have a set of variables $\{u_{12}, u_{21}, u_{23}, \dots, u_{L,L-1}\}$. As long as the degree distributions $P_{ij}(k)$ are known, we can easily work out P_1^∞ and P_L^∞ as

$$P_1^\infty = p_1 \left(1 - \sum_{k=0}^{\infty} P_{12}(k) u_{12}^k \right) = p_1 (1 - G_{12}(u_{12})) \quad (62)$$

$$\begin{aligned}
P_L^\infty &= p_L \left(1 - \sum_{k=0}^{\infty} P_{L,L-1}(k) u_{L,L-1}^k \right) \\
&= p_L (1 - G_{L,L-1}(u_{L,L-1}))
\end{aligned} \quad (63)$$

Now we look at P_i^∞ for all $i \in [2, L-1]$. Let us consider the probability for a node A in V_i not to belong to the LCC. Note

that node A could have neighbouring nodes in V_{i-1} and/or V_{i+1} . If A does not belong to the LCC, then it must not be connected to the LCC neither via neighbouring nodes in V_{i-1} nor via neighbouring nodes in V_{i+1} . Bear in mind that the event that A has k neighbouring nodes in V_{i-1} and the event that A has k neighbouring nodes in V_{i+1} are independent. Therefore, the probability for a node A in V_i not to belong to the LCC can be calculated as $P_{i,i-1}(k)u_{i,i-1}^k \cdot P_{i,i+1}(k)u_{i,i+1}^k$. Let k run over the whole network, then we can reach the following expression

$$\begin{aligned} P_i^\infty &= p_i \left(1 - \sum_{k=0}^{\infty} P_{i,i-1}(k)u_{i,i-1}^k \cdot \sum_{k=0}^{\infty} P_{i,i+1}(k)u_{i,i+1}^k \right) \\ &= p_i \left(1 - G_{i,i-1}(u_{i,i-1})G_{i,i+1}(u_{i,i+1}) \right) \end{aligned} \quad (64)$$

Because the expressions of P_i^∞ involve the variables $u_{i,i-1}$ and $u_{i,i+1}$, thus in what follows we will delineate in detail the calculations of $u_{i,i-1}$ and $u_{i,i+1}$. Recall that $u_{i,i+1}$ denotes the probability that a node A in V_i is not connected to the LCC via a node B in V_{i+1} . It is obvious that if node B is removed, then A definitely does not belong to the LCC. This event happens with a probability $1 - p_{i+1}$. If B is not removed and B is not connected to the LCC via its neighboring nodes, then A also does not belong to the LCC. Because node B could have neighbouring nodes in V_i and/or V_{i+2} , therefore the probability for B not to be connected to the LCC via its neighboring nodes in V_i and/or V_{i+2} is $P_{i+1,i}^{ex}(k)u_{i+1,i}^k \cdot P_{i+1,i+2}^{ex}(k)u_{i+1,i+2}^k$. As a result, we can formulate $u_{i,i+1}$ as

$$u_{i,i+1} = 1 - p_{i+1} + p_{i+1}H_{i+1,i}(u_{i+1,i}) \cdot H_{i+1,i+2}(u_{i+1,i+2}). \quad (65)$$

Note that the expression of $u_{i,i-1}$ possesses the similar form to that of $u_{i,i+1}$. Specially we have

$$u_{21} = 1 - p_1 + p_1 \cdot H_{12}(u_{12}), \quad (66)$$

$$u_{L-1,L} = 1 - p_L + p_L \cdot H_{L,L-1}(u_{L,L-1}). \quad (67)$$

To this end, we have mathematically derived the percolation theory for analyzing the robustness of multipartite networks under random node attacks. The robustness of multipartite networks under target node attacks can be mathematically calculated by combining the theories presented in subsections IV-C, IV-D and IV-E.

V. SIMULATION

A. Generating Multipartite Networks

Our proposed percolation theory could calculate the fraction of nodes in the LCC of a multipartite network subject to either random or target node attacks. The proposed theory can handle multipartite networks with arbitrary degree distributions. In order to verify the correctness of the proposed theory, here we test the proposed theory on computer-generated multipartite networks with Poisson degree distributions.

Fig. 7. An illustration on how to generate an L -partite network with Poisson degree distributions.

Fig. 7 elucidates the method for generating an L -partite network with Poisson degree distributions. As shown in Fig. 7, we generate an L -partite network by randomly adding edges between node sets V_i and V_{i+1} with a probability $r_i = \frac{C_i}{N_i + N_{i+1}}$ in which C_i is a predefined constant. The degree distributions $P_{i,i+1}(k)$ and $P_{i+1,i}(k)$ are then calculated as

$$P_{i,i+1}(k) = \binom{N_{i+1}}{k} r_i^k (1-r_i)^{N_{i+1}-k} \approx e^{-N_{i+1}r_i} \frac{(N_{i+1}r_i)^k}{k!}, \quad (68)$$

$$P_{i+1,i}(k) = \binom{N_i}{k} r_i^k (1-r_i)^{N_i-k} \approx e^{-N_i r_i} \frac{(N_i r_i)^k}{k!}, \quad (69)$$

which indicates that $P_{i,i+1}(k)$ and $P_{i+1,i}(k)$ follow Poisson degree distributions. It is easy to work out the mean degrees of $P_{i,i+1}(k)$ and $P_{i+1,i}(k)$ as

$$\langle k_{i,i+1} \rangle = \sum_{k=0}^{\infty} k P_{i,i+1}(k) = \frac{N_{i+1} C_i}{N_i + N_{i+1}}, \quad (70)$$

$$\langle k_{i+1,i} \rangle = \sum_{k=0}^{\infty} k P_{i+1,i}(k) = \frac{N_i C_i}{N_i + N_{i+1}}. \quad (71)$$

B. Node Removal Strategy

During the simulations, for a given L -partite network we need to remove $1 - p_i$ fraction of nodes from V_i for $\forall i \in [1, L]$ based on Eq. 13. The utilized node removal strategy to determine the $1 - p_i$ fraction of nodes from V_i such that each removed node approximately has the removal probability as calculated by Eq. 13 is elucidated below.

For the nodes in V_i , we first calculate the probability vector $W = (w_1, w_2, \dots, w_{N_i})$ with w_i being the removal probability for node i that is calculated using Eq. 13. We then calculate an integer vector $L = (l_1, l_2, \dots, l_{N_i})$ with $l_i = \text{round}(N_i w_i)$ being the number of times that node i should be removed so as to ensure that its removal probability approximates w_i . Based on L we further generate a node sequence $S = \{i \times \text{ones}(1, l_i) \mid \forall i = [1, N_i], l_i \neq 0\}$ in which $\text{ones}(1, l_i)$ represents an all-ones vector that has l_i entries. For example, if $L = (2, 1, 0, 3)$, then $S = \{1, 1, 2, 4, 4, 4\}$. We then randomly select $(1 - p_i)N_i$ unique elements from S and the final selections are the $1 - p_i$ fraction of nodes which needs be removed from V_i .

Note that when $l_i = 0$ for some $i \in [1, N_i]$, the number of the unique elements in S , hereafter denoted by n_s , will be

smaller than N_i (in the above example, $n_s = 3$). Consequently, the situation that $n_s < (1 - p_i)N_i$ could happen. In this case, we randomly choose the nodes whose degrees lead to $l_i = 0$ to compensate the shortage of nodes (in the above example, node 3 would be considered).

C. Network Robustness in the Case of $\alpha = 0$

We first explore the robustness of multipartite networks in face of target node attacks under the case $\alpha = 0$, i.e., we investigate the robustness of multipartite networks under random node attacks. Specifically, for a given L -partite network we randomly remove $1 - p_i$ fraction of nodes from V_i . We then theoretically and experimentally calculate P_i^∞ .

Without loss of generality, throughout the paper we here investigate L -partite networks with $L = 3$, i.e., tripartite networks. For a Poisson degree distribution $P(k) = e^{-\langle k \rangle} \frac{\langle k \rangle^k}{k!}$ we can easily prove that $G(x) = \sum P(k)x^k = e^{\langle k \rangle(x-1)} = H(x)$. Based on our developed percolation theory, the robustness of a tripartite network with Poisson degree distributions is then mathematically calculated as

$$\begin{cases} u_{21} = 1 - p_1 + p_1 e^{\langle k_{12} \rangle (u_{12} - 1)} \\ u_{23} = 1 - p_3 + p_3 e^{\langle k_{32} \rangle (u_{32} - 1)} \\ u_{12} = 1 - p_2 + p_2 e^{\langle k_{23} \rangle (u_{23} - 1)} e^{\langle k_{21} \rangle (u_{21} - 1)} \\ u_{32} = 1 - p_2 + p_2 e^{\langle k_{21} \rangle (u_{21} - 1)} e^{\langle k_{23} \rangle (u_{23} - 1)} \end{cases}, \quad (72)$$

$$\begin{cases} P_1^\infty = p_1 (1 - e^{\langle k_{12} \rangle (u_{12} - 1)}) \\ P_2^\infty = p_2 (1 - e^{\langle k_{23} \rangle (u_{23} - 1)} e^{\langle k_{21} \rangle (u_{21} - 1)}) \\ P_3^\infty = p_3 (1 - e^{\langle k_{32} \rangle (u_{32} - 1)}) \end{cases}. \quad (73)$$

In the experiments, when generating tripartite networks we set the parameter configurations to be $N_1 = N_2 = N_3 = 4 \times 10^4$ and $r_1 = r_2 = C/N$, where $C = \{6, 9, 12, 15\}$. For each generated network we investigate its robustness under random node attacks in two ways: 1) $p_1 = p$, $p_2 = p_3 = 1$, i.e., we remove nodes from V_1 ; 2) $p_2 = p$, $p_1 = p_3 = 1$, i.e., we remove nodes from V_2 . In the experiments, we set $p \in [0, 1]$ with an interval of 0.025.

The theoretical and experimental results on the robustness of tripartite networks under random node attacks are displayed in Fig. 8. We can clearly see from Fig. 8 that our proposed percolation theory coincides quite well with the simulations. The robustness curves exhibited in Fig. 8 indicate that multipartite networks are robust to random node attacks as the curves are smooth.

D. Network Robustness in the Case of $\alpha = 1$

We now explore the robustness of multipartite networks in face of target node attacks in the case of $\alpha = 1$, as equations presented in Section IV could have simple forms when $\alpha = 1$. Specifically, if $1 - p_i$ fraction of nodes are intentionally removed from V_i of a multipartite network with Poisson degree distributions, the expressions of variables t_{ij} and $\bar{p}_{ij}$ could respectively have the simple forms as $t_{ij} = \ln p_{ij} / \langle k_{ij} \rangle + 1$ and $\bar{p}_{ij} = t_{ij} p_i$.

1) Bipartite Network Case

Fig. 8. Robustness of tripartite networks with Poisson degree distributions under random attacks. The first and second columns respectively represent the situation where node attacks occur to V_1 and that to V_2 . Lines denote theoretical results while symbols represent simulation results which are averaged over 100 trials.

When intentionally removing $1 - p_1$ fraction of nodes from V_1 of a bipartite network with Poisson degree distributions, the percolation theory for analyzing its robustness could be simplified as follows

$$\begin{cases} u_{21} = 1 - p_1 + e^{\langle k_{12} \rangle (t_{12} u_{12} - 1)} \\ u_{12} = e^{t_{12} \langle k_{21} \rangle (u_{21} - 1)} \end{cases}, \quad (74)$$

$$\begin{cases} P_1^\infty = p_1 - e^{\langle k_{12} \rangle (t_{12} u_{12} - 1)} \\ P_2^\infty = 1 - e^{t_{12} \langle k_{21} \rangle (u_{21} - 1)} \end{cases}. \quad (75)$$

When intentionally removing $1 - p_i$ fraction of nodes from V_i for all $i \in [1, 2]$ of a bipartite network with Poisson degree distributions, the percolation theory for analyzing its robustness could be simplified as follows

$$\begin{cases} u_{21} = 1 - p_1 + p_1 e^{\langle k_{12} \rangle t_{12} t_{21} (u_{12} - 1)} \\ u_{12} = 1 - p_2 + p_2 e^{\langle k_{21} \rangle t_{12} t_{21} (u_{21} - 1)} \end{cases}, \quad (76)$$

$$\begin{cases} P_1^\infty = p_1 (1 - e^{\langle k_{12} \rangle t_{12} t_{21} (u_{12} - 1)}) \\ P_2^\infty = p_2 (1 - e^{\langle k_{21} \rangle t_{12} t_{21} (u_{21} - 1)}) \end{cases}, \quad (77)$$

where $t_{12} = \ln p_1 / \langle k_{12} \rangle + 1$ and $t_{21} = \ln p_2 / \langle k_{21} \rangle + 1$.

Fig. 9 demonstrates the robustness of bipartite networks under target attacks. The robustness results yielded by our proposed percolation theory comply with that of simulations. Bipartite networks are a special case of multipartite networks. In the next we exploit the robustness of multipartite networks under target node attacks.

Fig. 9. Robustness of bipartite networks with Poisson degree distributions under target attacks. The first and second rows respectively represent the situation where node attacks occur to V_1 and that to V_1 and V_2 . Lines denote theoretical results while symbols represent simulation results which are averaged over 100 trials.

2) Tripartite Network Case

When intentionally removing $1 - p_2$ fraction of nodes from V_2 of a tripartite network with Poisson degree distributions, the percolation theory for analyzing its robustness could be simplified as follows

$$\begin{cases} u_{21} = e^{\langle k_{12} \rangle t_2 (u_{12} - 1)} \\ u_{23} = e^{\langle k_{32} \rangle t_2 (u_{12} - 1)} \\ u_{12} = 1 - p_2 + p_2 e^{\langle k_{23} \rangle t_2 (u_{23} - 1)} e^{\langle k_{21} \rangle t_2 (u_{21} - 1)} \end{cases}, \quad (78)$$

$$\begin{cases} P_1^\infty = 1 - e^{\langle k_{12} \rangle t_2 (u_{12} - 1)} \\ P_2^\infty = p_2 (1 - e^{\langle k_{23} \rangle t_2 (u_{23} - 1)} e^{\langle k_{21} \rangle t_2 (u_{21} - 1)}) \\ P_3^\infty = 1 - e^{\langle k_{32} \rangle t_2 (u_{12} - 1)} \end{cases}, \quad (79)$$

where $t_2 = \ln p_2 / (\langle k_{21} \rangle + \langle k_{23} \rangle) + 1$.

When intentionally removing $1 - p_i$ fraction of nodes from V_i for all $i \in [1, 3]$ of a tripartite network with Poisson degree distributions, the percolation theory for analyzing its robustness could be simplified as follows

$$\begin{cases} u_{21} = 1 - p_1 + p_1 e^{\langle k_{12} \rangle t_2 t_{12} (u_{12} - 1)} \\ u_{23} = 1 - p_3 + p_3 e^{\langle k_{32} \rangle t_2 t_{32} (u_{12} - 1)} \\ u_{12} = 1 - p_2 + p_2 e^{\langle k_{23} \rangle t_2 t_{32} (u_{23} - 1)} e^{\langle k_{21} \rangle t_2 t_{12} (u_{21} - 1)} \end{cases}, \quad (80)$$

$$\begin{cases} P_1^\infty = p_1 (1 - e^{\langle k_{12} \rangle t_2 t_{12} (u_{12} - 1)}) \\ P_2^\infty = p_2 (1 - e^{\langle k_{23} \rangle t_2 t_{32} (u_{23} - 1)} e^{\langle k_{21} \rangle t_2 t_{12} (u_{21} - 1)}) \\ P_3^\infty = p_3 (1 - e^{\langle k_{32} \rangle t_2 t_{32} (u_{12} - 1)}) \end{cases}, \quad (81)$$

where $t_2 = \ln p_2 / (\langle k_{21} \rangle + \langle k_{23} \rangle) + 1$, $t_{12} = \ln p_1 / \langle k_{12} \rangle + 1$ and $t_{32} = \ln p_3 / \langle k_{32} \rangle + 1$.

The theoretical and experimental results on the robustness of tripartite networks under target node attacks are reflected in Fig. 10. The results once again validate the correctness of our proposed percolation theory. Fig. 10 indicates that multipartite

Fig. 10. Robustness of tripartite networks with Poisson degree distributions under target attacks. The first and second columns respectively represent the situation where node attacks occur to V_2 and that to V_1 , V_2 and V_3 . Lines denote theoretical results while symbols represent simulation results which are averaged over 100 trials.

networks are still robust to target node attacks as the robustness curves are smooth and no abrupt jump occurs.

E. Further Discussion

The above simulations have validated the correctness of the proposed theory for calculating the robustness of multipartite networks to node attacks. One may observe from the above simulations that the results shown in the upper part of Fig. 9 display some deviations. Note that this kind of deviations are inevitable. The reasons are twofold. Firstly, we can clearly see from Section IV that the proposed percolation theory is derived in the limit of $N_i \rightarrow \infty$. Therefore, the proposed theory may not work well with small sized multipartite networks. Although the size of a tested network in the simulations is of a magnitude of 10^4 , it is still finite. Secondly, in order to make sure that during the simulations each of the removed $1 - p_i$ fraction of nodes approximately has the removal probability as calculated by Eq. 13, the simulations have to be implemented for a large number of times. However, for the sake of computations, the simulations have only been done for 100 times. Therefore, the deviations as exhibited in Fig. 9 will be mitigated if the simulations are done for a larger number of times.

Note that the proposed percolation theory is generic and therefore can be applied to multipartite networks with arbitrary degree distributions. In the simulations only artificial multipartite networks with Poisson degree distributions are tested. On

the one hand, generating multipartite networks with arbitrary degree distributions is challenging. On the other hand, real-world multipartite networks which are available online are very small in size. How to develop effective percolation theories for small scale networks is still an open issue.

VI. CONCLUSION

Researches on network robustness are instrumental to assess the stabilities of complex networks in the presence of perturbations. Percolation theories are one of the most potent tools for theoretically quantifying the robustness of complex networks. Hitherto, a large body of work has been done towards network robustness and a handful of elegant percolation theories have been developed for multilayer or interdependent networks. It is universally reported that the robustness of multilayer networks display the so called first order phase transition phenomenon, which indicates that multilayer networks are fragile to disturbances.

Albeit the mature of percolation theories for multilayer networks, little effort is made to exploit the robustness of multipartite networks which play an important role in network science. Nevertheless, extant percolation theories are mute to multipartite networks. This paper had remedied this research chasm by presenting the generic percolation theory for analyzing the robustness of multipartite networks under node attacks based on an established non-cascading network fragmentation model. Compared to existing studies which adopt simulation based methods to calculate the robustness of multipartite networks, this work mathematically uncovers the principles governing the robustness of multipartite networks in face of perturbations. Meanwhile, the proposed theory is superior to simulation based methods when analyzing the robustness of large scale multipartite networks as the latter would become computationally costly.

The newly cranked out percolation theory has uncovered the second order phase transition phenomenon on multipartite networks which indicates that multipartite networks are robust to turbulence. The percolation theory devised in this paper is based on the established non-cascading network fragmentation model. Although second order phase transition is discovered, it is likely to erect a cascading network fragmentation model for analyzing the robustness of multipartite networks thereby enabling the occurrence of first order phase transition on multipartite networks. Whether multipartite networks can present first order phase transition and how to derive the corresponding percolation theory still deserve in-depth dedication, while this paper sheds substantial light on these issues.

REFERENCES

- [1] Y. Shang, "Subgraph robustness of complex networks under attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, no. 99, pp. 1–12, 2017.
- [2] R. J. La, "Cascading failures in interdependent systems: Impact of degree variability and dependence," *IEEE Trans. Netw. Sci. Eng.*, vol. 5, no. 2, pp. 127–140, 2018.
- [3] Y. Liu, A. Liu, N. N. Xiong, T. Wang, and W. Gui, "Content propagation for content-centric networking systems from location-based social networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, 2019.
- [4] D. Ding, Z. Wang, Q. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 5, pp. 779–789, 2018.
- [5] L. Liu and H. Jia, "Trust evaluation via large-scale complex service-oriented online social networks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 11, pp. 1402–1412, 2015.
- [6] C. Gao and J. Liu, "Network-based modeling for characterizing human collective behaviors during extreme events," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 1, pp. 171–183, 2017.
- [7] M. E. J. Newman, *Networks: An Introduction*. Oxford University Press, 2010.
- [8] X. Yuan, Y. Hu, H. E. Stanley, and S. Havlin, "Eradicating catastrophic collapse in interdependent networks via reinforced nodes," *PNAS*, vol. 114, no. 13, pp. 3311–3315, 2017.
- [9] G. Bianconi, "Multilayer networks: Dangerous liaisons?" *Nat. Phys.*, vol. 10, no. 10, p. 712, 2014.
- [10] M. Zhou and J. Liu, "A two-phase multiobjective evolutionary algorithm for enhancing the robustness of scale-free networks against multiple malicious attacks," *IEEE Trans. Cybern.*, vol. 47, no. 2, pp. 539–552, 2017.
- [11] M. Gong, L. Ma, Q. Cai, and L. Jiao, "Enhancing robustness of coupled networks under targeted recoveries," *Sci. Rep.*, vol. 5, no. 8439, 2015.
- [12] S. Wang and J. Liu, "Constructing robust cooperative networks using a multiobjective evolutionary algorithm," *Sci. Rep.*, vol. 7, no. 41600, 2017.
- [13] 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.
- [14] S. Shao, X. Huang, H. E. Stanley, and S. Havlin, "Percolation of localized attack on complex networks," *New J. Phys.*, vol. 17, no. 2, p. 023049, 2015.
- [15] G. Dong, R. Du, L. Tian, and R. Liu, "Robustness of network of networks with interdependent and interconnected links," *Physica A*, vol. 424, pp. 11–18, 2015.
- [16] F. Radicchi and C. Castellano, "Breaking of the site-bond percolation universality in networks," *Nat. Comm.*, vol. 6, no. 10196, 2015.
- [17] L.-W. Kong, M. Li, R.-R. Liu, and B.-H. Wang, "Percolation on networks with weak and heterogeneous dependency," *Phys. Rev. E*, vol. 95, no. 3, p. 032301, 2017.
- [18] L. Lü, D. Chen, X.-L. Ren, Q.-M. Zhang, Y.-C. Zhang, and T. Zhou, "Vital nodes identification in complex networks," *Phys. Rep.*, vol. 650, pp. 1–63, 2016.
- [19] L. Tian, A. Bashan, D.-N. Shi, and Y.-Y. Liu, "Articulation points in complex networks," *Nat. Comm.*, vol. 8, no. 14223, pp. 1–9, 2017.
- [20] A. Zeng and W. Liu, "Enhancing network robustness against malicious attacks," *Phys. Rev. E*, vol. 85, no. 6, p. 066130, 2012.
- [21] J. Wu, M. Barahona, Y.-J. Tan, and H.-Z. Deng, "Spectral measure of structural robustness in complex networks," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 41, no. 6, pp. 1244–1252, 2011.
- [22] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *PNAS*, vol. 108, no. 10, pp. 3838–3841, 2011.
- [23] F. D. Malliaros and M. Vazirgiannis, "Clustering and community detection in directed networks: A survey," *Phys. Rep.*, vol. 533, no. 4, pp. 95–142, 2013.
- [24] Q. Cai, L. Ma, M. Gong, and D. Tian, "A survey on network community detection based on evolutionary computation," *Int. J. Bio-Inspired Comput.*, vol. 8, no. 2, pp. 84–98, 2016.
- [25] L. Ma, M. Gong, Q. Cai, and L. Jiao, "Enhancing community integrity of networks against multilevel targeted attacks," *Phys. Rev. E*, vol. 88, no. 2, p. 022810, 2013.
- [26] Q. Cai and J. Liu, "The robustness of ecosystems to the species loss of community," *Sci. Rep.*, vol. 6, no. 35904, 2016.
- [27] Z. Wang, D. Zhou, and Y. Hu, "Group percolation in interdependent networks," *Phys. Rev. E*, vol. 97, no. 3, p. 032306, 2018.
- [28] 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.
- [29] X. Liu, H. E. Stanley, and J. Gao, "Breakdown of interdependent directed networks," *PNAS*, vol. 113, no. 5, pp. 1138–1143, 2016.
- [30] R.-R. Liu, M. Li, and C.-X. Jia, "Cascading failures in coupled networks: The critical role of node-coupling strength across networks," *Sci. Rep.*, vol. 6, p. 35352, 2016.
- [31] M. De Domenico, A. Solé-Ribalta, E. Omodei, S. Gómez, and A. Arenas, "Ranking in interconnected multilayer networks reveals versatile nodes," *Nat. Comm.*, vol. 6, p. 6868, 2015.
- [32] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Networks formed from interdependent networks," *Nat. Phys.*, vol. 8, no. 1, pp. 40–48, 2012.
- [33] S. Boccaletti, G. Bianconi, R. Criado, C. I. Del Genio, J. Gómez-

- Gardenes, M. Romance, I. Sendina-Nadal, Z. Wang, and M. Zanin, "The structure and dynamics of multilayer networks," *Phys. Rep.*, vol. 544, no. 1, pp. 1–122, 2014.
- [34] S. Pilosof, M. A. Porter, M. Pascual, and S. Kéfi, "The multilayer nature of ecological networks," *Nat. Ecol. Evol.*, vol. 1, p. 0101, 2017.
- [35] 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," *Sci. Rep.*, vol. 8, no. 1, p. 2111, 2018.
- [36] X. Tang, J. Liu, and M. Zhou, "Enhancing network robustness against targeted and random attacks using a memetic algorithm," *Europhys. Lett.*, vol. 111, no. 3, p. 38005, 2015.
- [37] J. A. Baggio, S. B. BurnSilver, A. Arenas, J. S. Magdanz, G. P. Kofinas, and M. De Domenico, "Multiplex social ecological network analysis reveals how social changes affect community robustness more than resource depletion," *PNAS*, vol. 113, no. 48, pp. 13 708–13 713, 2016.
- [38] A. G. Smart, L. A. Amaral, and J. M. Ottino, "Cascading failure and robustness in metabolic networks," *PNAS*, vol. 105, no. 36, pp. 13 223–13 228, 2008.
- [39] C. N. Kaiser-Bunbury, S. Muff, J. Memmott, C. B. Müller, and A. Cafilisch, "The robustness of pollination networks to the loss of species and interactions: a quantitative approach incorporating pollinator behaviour," *Ecol. Lett.*, vol. 13, no. 4, pp. 442–452, 2010.
- [40] D. M. Evans, M. J. Pocock, and J. Memmott, "The robustness of a network of ecological networks to habitat loss," *Ecol. Lett.*, vol. 16, no. 7, pp. 844–852, 2013.
- [41] H. Hooyberghs, B. Van Schaeuybroeck, and J. O. Indekeu, "Percolation on bipartite scale-free networks," *Physica A*, vol. 389, no. 15, pp. 2920–2929, 2010.
- [42] X. Huang, I. Vodenska, S. Havlin, and H. E. Stanley, "Cascading failures in bi-partite graphs: model for systemic risk propagation," *Sci. Rep.*, vol. 3, p. 1219, 2013.
- [43] A. Bashan, Y. Berezin, S. V. Buldyrev, and S. Havlin, "The extreme vulnerability of interdependent spatially embedded networks," *Nat. Phys.*, vol. 9, no. 10, pp. 667–672, 2013.
- [44] M. Di Muro, C. La Rocca, H. Stanley, S. Havlin, and L. Braunstein, "Recovery of interdependent networks," *Sci. Rep.*, vol. 6, p. 22834, 2016.
- [45] A. Vespignani, "Complex networks: The fragility of interdependency," *Nature*, vol. 464, no. 7291, pp. 984–985, 2010.
- [46] P. J. Mucha, T. Richardson, K. Macon, M. A. Porter, and J.-P. Onnela, "Community structure in time-dependent, multiscale, and multiplex networks," *Science*, vol. 328, no. 5980, pp. 876–878, 2010.
- [47] S. Gomez, A. Diaz-Guilera, J. Gomez-Gardenes, C. J. Perez-Vicente, Y. Moreno, and A. Arenas, "Diffusion dynamics on multiplex networks," *Phys. Rev. Lett.*, vol. 110, no. 2, p. 028701, 2013.
- [48] A. Solé-Ribalta, S. Gómez, and A. Arenas, "Congestion induced by the structure of multiplex networks," *Phys. Rev. Lett.*, vol. 116, no. 10, p. 108701, 2016.
- [49] M. De Domenico, C. Granell, M. A. Porter, and A. Arenas, "The physics of spreading processes in multilayer networks," *Nat. Phys.*, vol. 12, no. 10, p. 901, 2016.
- [50] W. Ellens and R. E. Kooij, "Graph measures and network robustness," *arXiv preprint arXiv:1311.5064*, 2013.
- [51] G. Dong, J. Gao, R. Du, L. Tian, H. E. Stanley, and S. Havlin, "Robustness of network of networks under targeted attack," *Phys. Rev. E*, vol. 87, no. 5, p. 052804, 2013.
- [52] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," *Phys. Rev. E*, vol. 83, no. 6, p. 065101, 2011.
- [53] Y. Hu, B. Ksherim, R. Cohen, and S. Havlin, "Percolation in interdependent and interconnected networks: Abrupt change from second- to first-order transitions," *Phys. Rev. E*, vol. 84, no. 6, p. 066116, 2011.
- [54] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Cascade of failures in coupled network systems with multiple support-dependence relations," *Phys. Rev. E*, vol. 83, no. 3, p. 036116, 2011.

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 artificial intelligence, complex network analytics, recommender systems, air traffic management and population ecology.

Sameer Alam received the M.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, Canberra, Australia, in 2008. He is currently an Associate Professor with the School of Mechanical and Aerospace Engineering, Nanyang Technological University. His research interests include simulation, modelling, 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.

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. His research interests involve machine learning, computational intelligent, evolutionary computation, fuzzy logic, neural network and evolving adaptive systems. He currently serves as the 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).

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 Modelling, 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.