On the robustness of complex systems with multipartitivity structures under node attacks

Cai, Qing; Alam, Sameer; Liu, Jiming

2020

Cai, Q., Alam, S., & Liu, J. (2020). On the robustness of complex systems with multipartitivity structures under node attacks. *IEEE Transactions on Control of Network Systems*, 7(1), 106-117. doi:10.1109/TCNS.2019.2919856

<https://hdl.handle.net/10356/144365>

<https://doi.org/10.1109/TCNS.2019.2919856>

© 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 is available at: <https://doi.org/10.1109/TCNS.2019.2919856>

Downloaded on 26 Apr 2023 18:51:51 SGT

On the Robustness of Complex Systems with Multipartitivity Structures under Node Attacks

Qing Cai, Sameer Alam, *Member, IEEE*, and Jiming Liu, *Fellow, IEEE*

Abstract—Complex systems in the real world inevitably suffer from unpredictable perturbations which can trigger system disasters wreaking significant economical losses. To exploit the robustness of complex systems in face of disturbances is of great significance. One of the most useful methods for system robustness analysis comes from the field of complex networks characterized by percolation theories. Many percolation theories therefore have been developed by researchers to investigate the robustness of diverse complex networks. Nevertheless, extant percolation theories are primarily devised for multilayer or interdependent networks. Little endeavor is dedicated to systems with multipartitivity structures, i.e., multipartite networks, which are an indispensable part of complex networks. This paper fills this research gap by theoretically examining the robustness of multipartite networks under random or target node attacks. The generic percolation theory for robustness analysis of multipartite networks is accordingly put forward. To validate the correctness of the proposed percolation theory, we carry out simulations on computer generated multipartite networks with Poisson degree distributions. The results yielded by the proposed theory coincide well with the simulations. Both theoretical and simulation results suggest that complex systems with multipartitivity structures could be more robust than that with multilayer structures.

Index Terms—Complex systems, multipartite networks, percolation theory, network robustness, phase transition

I. INTRODUCTION

HISTORICALLY, a dramatic blackout occurred to Italy in 2003 [1]. It was reported that some power grid transmission lines were damaged because of a storm. Due to the disconnections of those power lines, the power control centres which rely on them stopped working and their power control and supply tasks failed. The dysfunction of those centres further triggered the cascading failures of other power grids and eventually a large area of blackout happened which caused immeasurable economical losses [2]. In reality, apart from power supplier systems, complex systems such as Internet communication systems, mobile device communication systems, metropolitan transportation systems, etc., are ubiquitous and are playing a fundamental role in our daily lives [3–6]. Complex systems facilitate our lives unprecedentedly [7]. However, nowadays with the ever increasing demands of humans, the structures of complex systems are becoming more and more intricate [8–11]. The historical event of Italian blackout enlightens us that ensuring the stabilities of those systems

in the presence of external and/or internal perturbations is of great significance, as failures of a small portion of system components can wreak havoc to the entire system [12–14].

Stabilities of complex systems have long been studied [15, 16]. Hitherto, many theories and technologies have been devised towards that goal [17–19]. Amongst the extant avenues, one of the most applied techniques comes from the field of network science [20–23]. Note that many systems in reality can be depicted by complex networks composed of nodes and edges where the nodes represent the system components while the edges denote the interactions between the components [6, 24–26]. Network modelling and analysis avail system control [27–30]. Complex networks not only can provide a holistic perspective towards problem solving but also can help unravel the fundamental principles governing complex systems [29, 31, 32]. Network theories and methods have been extensively applied to a number of fields and have proven to be effective [33–36].

Researches on network robustness aim to quantify the extent to which a network can withstand perturbations [37–40]. Tremendous endeavors have been made towards network robustness analysis [21, 22, 41–43] and a body of them are characterized by percolation theories together with the concept of largest connected component [44, 45]. Network robustness analysis based on percolation theories is appealing as it can mathematically explain the robustness behaviours of complex networks. In the subsections to come are the survey on percolation theories for network robustness analysis and the contribution and organization of this paper.

A. Literature Survey

1) Percolation on Single Layer Networks Studies on network robustness have long been exploited [46]. Primitive studies on percolation theories for complex networks were mainly single networks oriented [37, 38, 47]. Percolation on networks is dedicated to mathematically measuring the robustness of networks in face of perturbations. Because perturbations could occur to either the nodes or the edges or even clusters each of which contains nodes and edges of a focal network, extant percolation theories thus can be categorized into three classes which are respectively termed as site percolation [48–50] and bond percolation [45, 51] in the literature and community percolation¹ [56–58]. In this paper

This research is partially supported by Air Traffic Management Research Institute (NTU-CAAS) Grant No. M4062429.052.

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.

J. Liu is with the Department of Computer Science, Hong Kong Baptist University, Hong Kong, e-mail: jiming@comp.hkbu.edu.hk.

¹Plenty of complex networks display community structures [52–55]. A network community is generally referred to as a subgraph that is densely interconnected but sparsely connected to the rest of a network. The term ‘community percolation’ is utilized here for the first time just to keep in accordance with the terms ‘site-’ and ‘bond-’ percolation.

we only focus on site percolation on networks. For one thing, site percolation is more extensively studied in the literature than the other two situations. For another thing, the outcome of site percolation will provide technical supports to the studies on the other two situations.

Given a network denoted by $G = \{V, E\}$ with V and E respectively being the sets of nodes and edges of G . Assume that $1 - p$ fraction of nodes of G are under attacks and therefore are removed, percolation theory aims to work out the relation between P^∞ , i.e., the fraction of nodes in the largest connected component (LCC²) of G , p , and the degree distribution $P(k)$ of G . There exists a critical value p_c , once the node removal fraction surpasses $1 - p_c$, will lead to the collapse of G , i.e., $P^\infty = 0$. Percolation theory has discovered that, if network G is under random attacks, i.e., each node has the same probability $1 - p$ to be removed, then the critical value p_c has the simple form as $p_c = \langle k \rangle / (\langle k^2 \rangle - \langle k \rangle)$, where $\langle k \rangle = \sum kP(k)$ and $\langle k^2 \rangle = \sum k^2P(k)$ are respectively the first and second moments of $P(k)$.

For a single layer network, if one draws the values of P^∞ with respect to p , then a continuous curve will be observed in which P^∞ approaches zero continuously at the critical point p_c . Therefore, single layer networks are robust to node perturbations [7, 24]. Since the expression of p_c involves the second moment, the robustness of single layer networks is said to present second-order phase transition [44].

2) Percolation on Multilayer Networks Note that complex networks in reality are not independent but on the contrary interdependent [44, 59]. Complex networks often are structured in a multilayer way [60–62]. Multilayer networks increase the complexity of networks. Intuitively, complexity augments the stability of a network thereby eliciting the taken-for-granted assertion that multilayer networks are more robust to network perturbations than single layer networks do. Nevertheless, this assertion has proven to be wrong by the seminal work in [2] in which multilayer networks are reported to be vulnerable to perturbations.

The distinguished work of [2] investigated the robustness of two-layer networks with one-to-one (O2O) correlations, i.e., one node in one network relies and only relies on one node in its coupled network. Given a two-layer network consisting of networks G_1 and G_2 with O2O correlations. Assume that G_1 and G_2 have the same network size and degree distribution. When randomly removing $1 - p$ fraction of nodes from G_1 , the corresponding percolation theory has found the simple form of the critical value p_c as $p_c = 2.4554 / \langle k \rangle$. Multilayer networks are universally reported to present first-order phase transition in which P^∞ approaches zero discontinuously at the critical point p_c [44]. Multilayer networks are therefore fragile to perturbations.

The work in [2] sparked the research enthusiasm on the robustness of multilayer networks [63–65]. To cite some examples, the work in [44] perfected the percolation theories to the case of multilayer networks organized in diverse structures; the work in [48, 66] exploited the case of multilayer networks

with one-to-many (O2M) correlations, i.e., one node in one network relies on multiple nodes in its coupled network; the work in [67] investigated the situation of directed multilayer networks; the work in [68] probed the percolation on dynamic multilayer networks; the work in [45] allied site and bond percolation; the latest work in [69] studied the percolation on multilayer networks under recovery strategies. Other work can be found in [70–73].

B. Contribution and Paper Organization

Contribution Albeit the mature of percolation theories for multilayer networks, little attention is paid to multipartite networks which are an essential part of complex networks [74, 75]. Multipartite network modelling avails problem solving in various fields like economy [74], ecology [76], biology [77], to name but a few. Understanding the robustness properties of multipartite networks is pivotal to system control and society development, while existing percolation theories are not amenable to multipartite networks. To fill this research gap, this paper studies the robustness of multipartite networks under node attacks. The main contributions of this paper are summarized in what follows:

- 1) This paper introduces a generic node attack model for multipartite networks. The introduced attack model covers situations of random attacks and target attacks.
- 2) This paper establishes the network cascading model for depicting the dynamical process on multipartite networks subject to node failures.
- 3) This paper develops a network surrogate model. When a multipartite network is under target attacks, the developed model is then used to generate a surrogate multipartite network, such that the target attacks to the original multipartite network is converted into the random attacks to the surrogate multipartite network.
- 4) This paper proposes the generic percolation theory for analyzing the robustness of multipartite networks. The proposed theory reveals the first-order phase transition phenomenon on the robustness of multipartite networks.

Organization The paper is structured as follows. Section II presents the problem to be addressed as well as the research motivations. Section III delineates in detail the proposed dynamic model and percolation theory for computing the robustness of multipartite networks under node attacks. Section IV verifies the correctness of the proposed theory by carrying out simulations on artificial multipartite networks. Section V concludes the paper.

II. PROBLEM DEFINITION AND MOTIVATION

A. Problem Definition

This paper is dedicated to analyzing the robustness of multipartite networks under node attacks. To begin with, we first give the following related definitions.

Definition 1 (Degree k) *For a given network, the degree k of a node is defined as the number of edges attached to it.*

²The LCC of a network G refers to the connected subnetwork of G that contains the largest number of nodes.

Definition 2 (Degree Distribution $P(k)$) For a given network, the degree distribution, denoted by $P(k)$, is defined as the distribution of the probability for a node to have degree k .

Definition 3 (Multipartite Network) Given a network $\mathcal{G} = \{V, E\}$. Let e_{ab} be the edge between nodes a and b . Assume that the node set $V \subset \mathcal{G}$ is composed of L subsets, i.e., $V = \{V_1, V_2, \dots, V_L\}$. Let $n_i = |V_i|$ be the number of nodes in V_i and $N = \sum n_i$ be the total number of nodes in $\mathcal{G}$. If the following conditions are satisfied:

$$\begin{cases} V_i \cap V_j = \emptyset, & \forall i, j \wedge i \neq j \\ \exists e_{ab}, & \text{if } a \in V_i \wedge b \in V_j \wedge j = \{i-1, i+1\} \\ \neg \exists e_{ab}, & \text{if } a, b \in V_i \text{ for } \forall i \in \{1, L\} \end{cases} \quad (1)$$

then $\mathcal{G}$ is said to be a multipartite (or L -partite) network. Specifically, $\mathcal{G}$ is called a bipartite network when $L = 2$.

Definition 4 (Degree Distribution $P_{ij}(k)$) For an L -partite network $\mathcal{G}$, define $P_{ij}(k)$ as the degree distribution of the nodes in $V_i \subset \mathcal{G}_{ij}$ with $\mathcal{G}_{ij} \subset \mathcal{G}$ being the bipartite network that contains node sets V_i and V_j for $j = \{i-1, i+1\}$.

Remark 1 V_i of an L -partite network also can be called a partite set. If a network $\mathcal{G}$ is composed of L sub-networks, i.e., $\mathcal{G} = \{\mathcal{G}_1, \mathcal{G}_2, \dots, \mathcal{G}_L\}$, and if an edge can appear between two arbitrary nodes of $\mathcal{G}$, then $\mathcal{G}$ is referred to as a multilayer network (see [64, 65] for rigorous mathematical definitions).

Following the work in [2, 44, 67], we adopt the concept of LCC to assess the robustness of multipartite networks. The robustness of multipartite networks under node attacks is mathematically defined as follows.

Definition 5 (Network Stage) For a given network $\mathcal{G}$, a network stage refers to the remaining part of $\mathcal{G}$ after removing some nodes and edges from $\mathcal{G}$.

Definition 6 (Robustness of Multipartite Networks) Given an L -partite network $\mathcal{G}$. Assume that $\mathcal{G}$ is under attack and a fraction of nodes are removed from $\mathcal{G}$. Consider a network cascading model which defines the way how failures propagate on $\mathcal{G}$. Based on the cascading model, $\mathcal{G}$ reaches a stable stage in which no further failures are possible. Consider the LCC in the stable stage of $\mathcal{G}$ and define the robustness of $\mathcal{G}$ as

$$\begin{aligned} P^\infty &= |\text{LCC}|/N \\ P_i^\infty &= |\text{LCC}_i|/n_i \end{aligned} \quad (2)$$

with $\text{LCC}_i \subset \text{LCC}$ being the node set that only contains nodes from V_i , and $|\cdot|$ being the number of nodes in a node set.

Example 1 To better illustrate the definition of the robustness of multipartite networks, here we present a simple example shown in Fig. 1. The left panel of Fig. 1 displays a tripartite network $\mathcal{G}$ with three partite sets V_1 , V_2 and V_3 . Assume that $1 - p_1$ ($p_1 = 1/3$) fraction of nodes are removed from V_1 . Without loss of generality, we consider the case where nodes A1 and A2 are removed from V_1 . Consider a cascading model which defines that nodes in V_i for all $i \in [2, L-1]$ will be disconnected from $\mathcal{G}$ if nodes in V_i only have connections with nodes in either V_{i-1} or V_{i+1} . Based on this cascading

model, $\mathcal{G}$ reaches a stable stage as shown in the middle of Fig. 1. In the stable stage, the LCC contains four nodes, namely A3, B4, C1 and C3. Then the robustness of $\mathcal{G}$ is calculated as $P^\infty = 4/10$, $P_1^\infty = 1/3$, $P_2^\infty = 1/4$ and $P_3^\infty = 2/3$.

Fig. 1. A graphical example to the robustness definition for multipartite networks.

Definition 6 provides the way how we quantify the robustness of multipartite networks. With all the above definitions we define our research problem in what follows.

Definition 7 (Research Problem) For an L -partite network $\mathcal{G}$ with known degree distributions $P_{ij}(k)$, we remove $1 - p_i$ fraction of nodes from V_i for $\forall i \in [1, L]$ with $p_i \in [0, 1]$. The robustness analysis of $\mathcal{G}$ is to work out the mathematical relationship between P_i^∞ , $P_{ij}(k)$ and p_i with respect to a given network cascading model.

B. Motivation

In the literature, a handful of simulation-based studies have been done to investigate the robustness of multipartite networks [38, 57]. Simulation-based studies, although characterized by their simplicities in terms of idea and implementations, do not serve our research problem as given in Definition 7, since they figure out the relationship between P_i^∞ , $P_{ij}(k)$ and p_i based on simulations but not in a mathematical way. With regard to this, we need to turn to the theoretical studies characterized by percolation theories for multipartite networks. The work in [77–79] theoretically investigated the robustness of L -partite networks. However, the percolation theories developed in those studies only deal with L -partite networks with $L = 2$, i.e., bipartite networks. How multipartite networks behave in face of disturbance is unknown and how to develop the corresponding percolation theory is still challenging.

In order to solve our research problem, a promising way is to draw inspirations from well studied percolation theories for multilayer networks. Note that the development of percolation theories heavily relies on network dynamic models for describing the cascading failures on complex networks. In the literature, there are three representative network models for multilayer networks. Fig. 2 summarizes the core ideas of those three models.

Fig. 2(a) details the principle of the cascading model proposed in [2]. The two-layer network (consists of subnetworks A and B) displayed in Fig. 2(a) is O2O correlated. This model assumes that 1) if one node fails, then its coupled node will

Fig. 2. Illustrations to the state-of-the-art network cascading models for analyzing the robustness of multilayer networks under node failures. (a) The model proposed in [2]. (b) The model proposed in [48]. (c) The model proposed in [67].

also fail; 2) for each subnetwork nodes outside its LCC will be disconnected. As shown in Fig. 2(a), initially node A5 is under attack. In stage 1, node A5 is removed and node B5 is also removed due to the removal of A5. Based on the model's assumptions, in stage 2, nodes A3 and B3 are disconnected, and in the stable stage only four nodes are remained.

Because the model shown in Fig. 2(a) requires the subnetworks to be O2O correlated while realistic networks normally are O2M correlated, the work in [48] therefore established another model with its core idea being graphically explained in Fig. 2(b). This model allows one node to have multiple dependencies in its coupled network. A directed edge in the model points from the supplier node to the dependent node. Initially, node A1 is under attack. This model posits that a node without supplies or a node outside the LCC will be regarded as dysfunctional. Based on this assumption, in stage 1, node A1 together with its edges are removed and node A6 is disconnected as it is outside the LCC. In stage 2, B1 and B2 are disconnected as they have no suppliers. In the stable stage, only six nodes are remained as shown in the r.h.s of Fig. 2(b).

Both the models shown in Figs. 2(a) and (b) address undirected networks³ while many networks in reality are directed.

³The edge directions displayed in the model shown in Fig. 2(b) only represent the interdependency relations between two coupled networks, while each subnetwork itself is undirected.)

With regard to this, the work in [67] exploited the robustness of directed multilayer networks with its established model being depicted in Fig. 2(c). This model allows intra- and inter-layer edges to be directed. A directed edge points from the supplier node to the dependent node. This model possesses the same hypothesis as that of the model shown in Fig. 2(b). Initially the nodes in red are attacked. Based on its assumption, the focal directed two-layer network reaches the stable stage as displayed in the r.h.s of Fig. 2(c).

By comparing Fig. 1 and Fig. 2 we could observe that the three models analyzed above are not amenable to multipartite networks. The models presented in Figs. 2(a) and (c) share one thing in common that they are O2O correlated multilayer networks oriented. As a consequence, the percolation theories devised in [2, 67] are not applicable to multipartite networks.

The model illustrated in Fig. 2(b) deals with multilayer networks with O2M correlations which is very close to the situation of multipartite networks. However, for a multipartite network there are no “intra-layer” edges. This structural difference renders direct technology transfers from the corresponding percolation theory infeasible. Meanwhile, the percolation theory developed in [48] only analyzes two-layer networks. How to develop percolation theories for networks with more than two layers is still challenging [44]. New percolation theory for multipartite networks is therefore desirable.

III. MODEL AND THEORY

A. Node Attack Model

Note that the components of a network could suffer from random failures or target attacks. Following [80, 81] we therefore introduce the following node attack model to calculate the node removal probability for a multipartite network⁴

$$w_{\alpha,l} = \frac{(k_{il} + 1)^\alpha}{\sum_{i=0}^{n_l} (k_{il} + 1)^\alpha}, \quad (3)$$

with α being a constant, l being the l -th node set to be investigated, k_{il} being the degree of node $i \in V_l$ and $n_l = |V_l|$.

Remark 2 The parameter α determines the probability for a node to be removed. Based on Eq. 3 we have:

- 1) If $\alpha > 0$, then a node with larger degree has higher probability to be removed.
- 2) If $\alpha < 0$, then a node with smaller degree has higher probability to be removed.
- 3) If $\alpha = 0$, then every node has the same probability to be removed, which corresponds to the situation that a network is under random node attacks.

B. Cascading Failure Model

One can notice from what are described in Section II that one of the most significant components for network robustness analysis lies in the network cascading model. Because the

⁴If node attacks occur to the whole network, then the summation in the denominator of Eq. 3 should run over all the nodes of the network, i.e., n_l should be replaced by N .

structures of multipartite networks differ from that of multilayer networks, therefore the models exhibited in Fig. 2 are impracticable to be directly applied to multipartite networks.

Inspired by the cascading models displayed in Fig. 2, here we put forward a cascading model for multipartite networks with its main idea being delineated in Fig. 3.

Fig. 3. Schematic of the proposed cascading model for analyzing the robustness of multipartite networks. Originally, node A2 from V_1 of a tripartite network $\mathcal{G}$ is under attack. The removal of node A2 breaks the bipartite network $\mathcal{G}_{12}$ comprised of node sets V_1 and V_2 into 3 parts. In compliance with the LCC concept, nodes A3, B4 and B5 are further removed as there are not in the LCC of $\mathcal{G}_{12}$, which further fragments the bipartite network $\mathcal{G}_{23}$ comprised of node sets V_2 and V_3 into 2 parts. Eventually, only nodes A1, B1, B2 and C1 survive as no failures are possible.

Remark 3 The proposed model depicted in Fig. 3 takes a bipartite network contained in a multipartite network as a fundamental unit. Specifically, for an L -partite network the proposed model sequentially calculates the LCC of the bipartite network consisting of node sets V_i and V_{i+1} , $\forall i \in [1, L-1]$. This process is repeated until the focal network reaches a stable stage in which further nodes and edges removals are impossible. The rationale of the devised model is built on the hypothesis that the failures of nodes in V_i of a multipartite network only affect nodes in its adjacent node sets V_{i-1} and V_{i+1} .

C. Network Surrogate Model

Directly calculating the robustness of complex networks in face of target node attacks is difficult, as it can be seen from Eq. 3 that nodes with different degrees have different probabilities to be removed. In the literature there exists an effective proxy which transfers the target node attack problem into the random attack situation which is relatively much easier to be addressed [80]. In line with this idea, here we exploit the robustness of multipartite networks under target node attacks by introducing a network surrogate model whereby the intentional node attack situation is converted into the case scenario of random attacks.

Example 2 Fig. 4 delineates the idea of the introduced surrogate model. In Fig. 4, a tripartite network $\mathcal{G}$ is under intentional attack and assume that node B4 from node set B is removed. The remaining part of $\mathcal{G}$ is denoted by $\mathcal{G}_r$. Assume that there exists another tripartite network $\tilde{\mathcal{G}}$ as exhibited in Fig. 4. Next we randomly remove the same amount of nodes from the same node set of $\tilde{\mathcal{G}}$ as that we did to $\mathcal{G}$. Specifically, we randomly remove one node (assume B3) from $\tilde{\mathcal{G}}$ and the remaining part of $\tilde{\mathcal{G}}$ is $\tilde{\mathcal{G}}_r$. As we can see from Fig. 4 that $\tilde{\mathcal{G}}_r$

Fig. 4. An example to illustrate the introduced network surrogate model for analyzing the robustness of multipartite networks under target node attacks.

has the same degree sequences as $\mathcal{G}_r$ does. Then we say that $\tilde{\mathcal{G}}$ is the surrogate network of $\mathcal{G}$. More generally, we define the surrogate network for our studied problem as follows.

Definition 8 (Surrogate Network) Given an L -partite network $\mathcal{G}$ with N nodes and assume that $1 - p_i$ fraction of nodes are removed from $V_i \subset \mathcal{G}$ for $\forall i \in [1, L]$ based on the node attack model presented in Eq. 3. We use token $\mathcal{G}_r$ to denote the surplus part of $\mathcal{G}$. Assume that there exists an L -partite network $\tilde{\mathcal{G}}$ and assume that $1 - p_i$ fraction of nodes are randomly removed from $V_i \subset \tilde{\mathcal{G}}$ for $\forall i \in [1, L]$. Let $\tilde{\mathcal{G}}_r$ be the remaining part of $\tilde{\mathcal{G}}$. We define $\tilde{\mathcal{G}}$ as the surrogate network of $\mathcal{G}$ if the following conditions are satisfied:

$$\begin{aligned} \tilde{P}_{ij}^r(k) &= P_{ij}^r(k), \forall i \in [1, L] \wedge j = \{i-1, i+1\} \\ |V_i \subset \mathcal{G}| &= |V_i \subset \tilde{\mathcal{G}}|, \forall i \in [1, L] \end{aligned} \quad (4)$$

where $P_{ij}^r(k)$ is the degree distribution of the nodes in V_i with $V_i \subset \mathcal{G}_{ij} \subset \mathcal{G}_r$, and $\tilde{P}_{ij}^r(k)$ is the degree distribution of the nodes in V_i with $V_i \subset \tilde{\mathcal{G}}_{ij} \subset \tilde{\mathcal{G}}_r$.

Definition 9 (Generating Function) Given a degree distribution function $P_{ij}(k)$, define its generating function as $G_{ij}(z) = \sum_{k=0}^{\infty} P_{ij}(k)z^k$, with z being an arbitrary placeholder.

Remark 4 The first condition of Eq. 4 can be represented in the form of generating functions as

$$\tilde{G}_{ij}^r(z) = G_{ij}^r(z), \forall i \in [1, L] \wedge j = \{i-1, i+1\}, \quad (5)$$

with $\tilde{G}_{ij}^r(z) = \sum_{k=0}^{n_j} \tilde{P}_{ij}^r(k)z^k$ and $G_{ij}^r(z) = \sum_{k=0}^{n_j} P_{ij}^r(k)z^k$. Generating functions are widely used for deriving the percolation theories for analyzing network robustness [67, 69]. We therefore will make heavy use of generating functions in the rest of the paper to simplify the mathematical deductions.

Theorem 1 Consider an L -partite network $\mathcal{G}$ as well as its surrogate network $\tilde{\mathcal{G}}$. The robustness analysis of $\mathcal{G}$ subject to

target node attacks with respect to the attack model presented in Eq. 3 is equivalent to the robustness analysis of $\tilde{\mathcal{G}}$ subject to random node attacks.

The proof of Theorem 1 is presented in Appendix.

D. Derivation of the Surrogate Network

The equivalent condition formulated in Eq. 5 determines the properties of the surrogate network $\tilde{\mathcal{G}}$ in terms of generating functions. In what follows we will present the detailed mathematical calculations for deriving the surrogate network. We start by first calculating the l.h.s of Eq. 5, i.e., $\widetilde{G}_{ij}^r(z)$. We start by presenting the following Lemma.

Lemma 1 Consider a bipartite network $\tilde{\mathcal{G}}$ with V_1 and V_2 respectively being its two node sets. Let $\widetilde{P}_1(k)$ and $\widetilde{P}_2(k)$ respectively be the degree distributions of nodes in V_1 and V_2 . If $1 - p_1$ fraction of nodes are randomly removed from V_1 , then the generating functions satisfy the following conditions

$$\begin{aligned}\widetilde{G}_1^r(z) &= \widetilde{G}_1(z) \\ \widetilde{G}_2^r(z) &= \widetilde{G}_2(1 - p_1 + p_1 z)\end{aligned}\quad (6)$$

The proof of Lemma 1 is presented in Appendix.

Theorem 2 Consider an L -partite network $\tilde{\mathcal{G}}$ with V_i being its i -th nodes set and $\widetilde{P}_{ij}(k)$ being the degree distribution of nodes in $V_i \subset \tilde{\mathcal{G}}_{ij} \subset \tilde{\mathcal{G}}$ for $j = \{i-1, i+1\}$. If $1 - p_i$ fraction of nodes are randomly removed from V_i for $\forall i \in [1, L]$, then the generating functions satisfy the following conditions

$$\begin{aligned}\widetilde{G}_{ji}^r(z) &= \widetilde{G}_{ji}(1 - p_i + p_i z) \\ \widetilde{G}_{ij}^r(z) &= \widetilde{G}_{ij}(1 - p_j + p_j z)\end{aligned}\quad (7)$$

The proof of Theorem 2 is omitted as it can be easily derived from Lemma 1.

In the next, we will delineate in detail the calculation of the r.h.s of Eq. 5, i.e., $G_{ij}^r(z)$. To do so, we have to derive the degree distribution $P_{ij}^r(k)$. In order to work out $P_{ij}^r(k)$, we provide the following definition and lemma.

Definition 10 (Function $\mathcal{F}_i(z)$) Given a degree distribution function $P_i(k)$. Let α be a constant and z be an arbitrary placeholder. Define function $\mathcal{F}_i(z)$ as $\mathcal{F}_i(z) = \sum_{k=0}^{\infty} P_i(k) z^{(k+1)^\alpha}$.

Lemma 2 Consider an L -partite network $\mathcal{G}$ with V_i being its i -th nodes set and $P_i(k)$ being the degree distribution of nodes in $V_i \subset \mathcal{G}$ for $\forall i = [1, L]$. If $1 - p_i$ fraction of nodes are intentionally removed from $V_i \subset \mathcal{G}$ for $i \in [1, L]$ based on Eq. 3, then the degree distribution of the remaining nodes in V_i , denoted by $P_i^r(k)$, satisfies the following condition

$$P_i^r(k) = \frac{1}{p_i} P_i(k) \mathcal{H}_i^{(k+1)^\alpha}, \quad (8)$$

where $\mathcal{H}_i = \mathcal{F}_i^{-1}(p_i)$ with $\mathcal{F}_i^{-1}(\cdot)$ being the inverse of $\mathcal{F}_i(\cdot)$.

The proof of Lemma 2 is presented in Appendix.

Lemma 2 provides the way to calculate the degree distribution $P_i^r(k)$. Keep in mind that our purpose is to figure out

$P_{ij}^r(k)$ so as to derive the expressions of $G_{ij}^r(z)$. To figure out $P_{ij}^r(k)$, we give the following definition and lemma.

Definition 11 (The t -th Moment of a Degree Distribution) For a given degree distribution $P(k)$, define its t -th moment as $\langle k^t \rangle = \sum_{k=0}^{\infty} k^t P(k)$.

Lemma 3 Consider an L -partite network $\mathcal{G}$ with V_i being its i -th nodes set and $P_{ij}(k)$ being the degree distribution of nodes in $V_i \subset \mathcal{G}_{ij} \subset \mathcal{G}$ for $\forall i = [1, L]$ and $j = \{i-1, i+1\}$. If $1 - p_i$ fraction of nodes are intentionally removed from $V_i \subset \mathcal{G}$ for $i \in [2, L-1]$ based on Eq. 3, then the degree distribution of the remaining nodes in the node set $V_i \subset \mathcal{G}_{ij} \subset \mathcal{G}$, i.e., $P_{ij}^r(k)$, is calculated as

$$P_{ij}^r(k) = \frac{1}{p_{ij}} P_{ij}(k) \mathcal{H}_{ij}^{(k+1)^\alpha}, \quad (9)$$

with $p_{ij} = p_i^{(k_{ij})/\langle k_i \rangle}$, $\mathcal{H}_{ij} = \mathcal{F}_{ij}^{-1}(p_{ij})$ and $\mathcal{F}_{ij}(p_{ij}) = \sum_{k=0}^{\infty} P_{ij}(k) p_{ij}^{(k+1)^\alpha}$.

The proof of Lemma 3 is presented in Appendix.

Theorem 3 Consider an L -partite network $\mathcal{G}$ with V_i being its i -th nodes set and $P_{ij}(k)$ being the degree distribution of nodes in $V_i \subset \mathcal{G}_{ij} \subset \mathcal{G}$ for $\forall i = [1, L]$ and $j = \{i-1, i+1\}$. If $1 - p_i$ fraction of nodes are intentionally removed from $V_i \subset \mathcal{G}$ for $\forall i \in [1, L]$ based on Eq. 3, then the generating functions $G_{ji}^r(z)$ and $G_{ij}^r(z)$ are calculated as

$$\begin{aligned}G_{ji}^r(z) &= \frac{1}{p_{ji}} \sum_{k=0}^{\infty} \sum_{m=0}^k P_{ji}(k) \mathcal{H}_{ji}^{(k+1)^\alpha} \binom{k}{m} (1 - q_{ji})^m q_{ji}^{k-m} z^k \\ G_{ij}^r(z) &= \frac{1}{p_{ij}} \sum_{k=0}^{\infty} \sum_{m=0}^k P_{ij}(k) \mathcal{H}_{ij}^{(k+1)^\alpha} \binom{k}{m} (1 - q_{ij})^m q_{ij}^{k-m} z^k\end{aligned}\quad (10)$$

with q_{ij} and q_{ji} respectively being calculated as

$$\begin{aligned}q_{ij} &= \sum_{k=0}^{\infty} k P_{ij}(k) \mathcal{H}_{ij}^{(k+1)^\alpha} / (p_i \sum_{k=0}^{\infty} k P_{ij}(k)) \\ q_{ji} &= \sum_{k=0}^{\infty} k P_{ji}(k) \mathcal{H}_{ji}^{(k+1)^\alpha} / (p_j \sum_{k=0}^{\infty} k P_{ji}(k))\end{aligned}\quad (11)$$

The proof of Theorem 3 is presented in Appendix.

E. Robustness of the Surrogate Network

The above section has elaborated the calculation of the generating functions for the surrogate multipartite network $\tilde{\mathcal{G}}$. In the section to come we elucidate our proposed percolation theory for analyzing the robustness of the surrogate network $\tilde{\mathcal{G}}$ under random node failures. To achieve this goal, we give the following definition and theorem.

Definition 12 (Probability Variable f_{ij}) Given an L -partite network $\tilde{\mathcal{G}}$ with V_i being its i -th node set. Assume that there is a node B in V_i and B has a neighbouring node A in V_{i-1} and a neighbouring node C in V_{i+1} . Define a set of probability variables f_{ij} for $j = \{i-1, i+1\}$. We respectively define $f_{i,i-1}$ and $f_{i,i+1}$ as the probabilities that node B is not connected to the LCC via its neighbouring nodes A and C . If $i = 1$, then define $f_{10} = 0$. If $i = L$, then define $f_{L,L+1} = 0$.

Theorem 4 Consider an L -partite network $\tilde{\mathcal{G}}$ with V_i being its i -th nodes set and $\widetilde{P}_{ij}(k)$ being the degree distribution of

nodes in $V_i \subset \widetilde{\mathcal{G}}_{ij} \subset \widetilde{\mathcal{G}}$ for $j = \{i-1, i+1\}$. Define a set of probability variables f_{ij} . If $1 - p_i$ fraction of nodes are randomly removed from V_i for $\forall i \in [1, L]$, and if the network cascading model as shown in Fig. 3 is of concern, then the robustness of $\widetilde{\mathcal{G}}$ is calculated as

$$P_i^\infty = p_i \left[1 - \widetilde{G}_{i,i-1}(f_{i,i-1}) \right] \left[1 - \widetilde{G}_{i,i+1}(f_{i,i+1}) \right], \quad (12)$$

with f_{ij} satisfying the following generic relation

$$f_{ij} = 1 - p_j \left[1 - \frac{\widetilde{G}_{ji}'(f_{ji})}{\widetilde{G}_{ji}(1)} \right] \left[1 - \frac{\widetilde{G}_{j,j+\Delta}'(f_{j,j+\Delta})}{\widetilde{G}_{j,j+\Delta}(1)} \right]. \quad (13)$$

If $\forall i \in [1, L-1]$ and $j = i+1$, then $\Delta = 1$. If $\forall i \in [2, L]$ and $j = i-1$, then $\Delta = -1$.

The proof of Theorem 4 is presented in Appendix.

IV. SIMULATIONS

A. Multipartite Network Data

In this section we will validate the effectiveness and correctness of the proposed models and theory for analyzing the robustness of multipartite networks. To do so, here we generate multipartite networks for simulation purpose. The detailed steps for generating an L -partite network is given as follows.

- 1) Define an integer vector $\mathbf{n} = (n_1, n_2, \dots, n_L)$;
- 2) Create L empty node sets $\{V_1, V_2, \dots, V_L\}$ with $|V_i| = n_i$ being the number of nodes in node set V_i ;
- 3) Define an integer vector $\mathbf{d} = (d_1, d_2, \dots, d_{L-1})$;
- 4) For $i = 1$ to $L-1$ do the following:
- 5) For any pair of nodes with one from V_i and the other one from V_{i+1} we connect them with an edge if $\text{rand} < r_i = \frac{d_i}{n_i + n_{i+1}}$ where $\text{rand} \in [0, 1]$ is a random number.

B. Degree Distribution Analysis

In this part we analyze the degree distributions $P_{ij}(k)$ of the above generated multipartite network. It is easy to figure out $P_{ij}(k)$ as follows

$$P_{ij}(k) = \binom{n_j}{k} r_i^k (1 - r_i)^{n_j - k} \approx e^{-\langle k_{ij} \rangle} \frac{\langle k_{ij} \rangle^k}{k!}, \quad (14)$$

where $\langle k_{ij} \rangle = n_j r_i = \frac{n_j}{n_i + n_j} d_i$.

Eq. 14 indicates $P_{ij}(k)$ follows the Poisson degree distribution. As the robustness analysis process involves the calculation of $P_i(k)$, we analogously could figure out $P_i(k)$ as

$$P_i(k) \approx e^{-\langle k_i \rangle} \frac{\langle k_i \rangle^k}{k!}, \quad (15)$$

where $\langle k_i \rangle = \langle k_{i,i-1} \rangle + \langle k_{i,i+1} \rangle$.

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

In the case of $\alpha = 0$, the node attack model presented in Eq. 3 becomes the random attack situation. We thus could directly apply Theorem 4 to calculate the robustness of a multipartite network under random node failures.

Without loss of generality, here we only investigate multipartite 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 have $G(z) = e^{\langle k \rangle(z-1)}$. Therefore, based on Theorem 4 we have

$$\begin{aligned} P_1^\infty &= p_1 (1 - e^{\langle k_{12} \rangle (f_{12} - 1)}) \\ P_2^\infty &= p_2 (1 - e^{\langle k_{21} \rangle (f_{21} - 1)}) (1 - e^{\langle k_{23} \rangle (f_{23} - 1)}) \\ P_3^\infty &= p_3 (1 - e^{\langle k_{32} \rangle (f_{32} - 1)}) \end{aligned} \quad (16)$$

with the corresponding variables being calculated as

$$\begin{aligned} f_{12} &= 1 - p_2 (1 - e^{\langle k_{21} \rangle (f_{21} - 1)}) (1 - e^{\langle k_{23} \rangle (f_{23} - 1)}) \\ f_{21} &= 1 - p_1 + p_1 e^{\langle k_{12} \rangle (f_{12} - 1)} \\ f_{23} &= 1 - p_3 + p_3 e^{\langle k_{32} \rangle (f_{32} - 1)} \\ f_{32} &= 1 - p_2 (1 - e^{\langle k_{23} \rangle (f_{23} - 1)}) (1 - e^{\langle k_{21} \rangle (f_{21} - 1)}) \end{aligned} \quad (17)$$

Note that P^∞ can always be obtained by the generic expression of $P^\infty = \sum \frac{n_i}{N} P_i^\infty$.

For a given tripartite network, in the simulations we randomly remove $1 - p_1$, $1 - p_2$ and $1 - p_3$ fraction of nodes respectively from V_1 , V_2 and V_3 . Subsequently, we let the cascading failures propagate on the network based on the dynamic model exhibited in Fig. 3. We then find out the LCC and count the number of remaining nodes in each partite set. Eventually we visualize the fraction P_i^∞ with respect to p_1 , p_2 and p_3 . Without loss of generality, we only demonstrate part of the simulations in which we set $p_1 = p_2 = p_3 = p$.

Fig. 5. Theoretical and simulation results on the robustness of tripartite networks with respect to the established cascading model and the introduced node attack model with $\alpha = 0$. A fraction $1 - p$ of nodes are removed from V_i , $\forall i \in [1, 3]$, of a focal tripartite network. The parameter settings for each tripartite network are $n_1 = n_2 = n_3 = 1 \times 10^4$ and $d_1 = d_2 = d$ with the value of d being prescribed in the figure's legend. The values of P_i^∞ and P^∞ are shown with respect to $p \in [0, 1]$ at an interval of 0.025.

We generate a network for 10 times. For each generated network, we carry out the node removal process for 50

independent trails. Thus, the simulation results are averaged over 500 trails. As long as the values of p and d are known, then we could figure out the robustness of a focal tripartite network based on Eqs. 16 and 17. During the calculation, we make heavy use of numerical analysis. Fig. 5 displays the theoretical and experimental results on the robustness of tripartite networks subject to random node attacks. It can be seen from the figure that the theoretical results coincide quite well with the experimental results. We can clearly see from the figure that the robustness of the tested tripartite networks present first-order phase transition phenomenon which indicates that tripartite networks are fragile to node failures. Fig. 5 also indicates that a large degree will augment the robustness of tripartite networks.

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

In the case of $\alpha = 1$, the equations presented in Theorem 3 have simplified forms. Then based on Theorems 2, 3 and 4 we can calculate the robustness of multipartite networks to target node attacks. In the following we also only investigate tripartite networks.

Consider the case that every node set of a tripartite network with Poisson degree distributions is under target attacks. Specifically, we intentionally remove $1 - p$ fraction of nodes from V_i , $\forall i \in [1, 3]$, of a tripartite network. Then Theorems 2, 3 and 4 lead to

$$\begin{aligned} P_1^\infty &= p \left(1 - e^{\mathcal{H}_1 \mathcal{H}_{21} \langle k_{12} \rangle (f_{12}-1)} \right) \\ P_2^\infty &= p \left(1 - e^{\mathcal{H}_1 \mathcal{H}_{21} \langle k_{21} \rangle (f_{21}-1)} \right) \left(1 - e^{\mathcal{H}_{23} \mathcal{H}_3 \langle k_{23} \rangle (f_{23}-1)} \right), \\ P_3^\infty &= p \left(1 - e^{\mathcal{H}_{23} \mathcal{H}_3 \langle k_{32} \rangle (f_{32}-1)} \right) \end{aligned} \quad (18)$$

with the four variables being respectively calculated as

$$\begin{aligned} f_{12} &= 1 - p (1 - e^{\mathcal{H}_{21} \mathcal{H}_1 \langle k_{21} \rangle (f_{21}-1)}) (1 - e^{\mathcal{H}_{23} \mathcal{H}_3 \langle k_{23} \rangle (f_{23}-1)}) \\ f_{21} &= 1 - p + p e^{\mathcal{H}_{21} \mathcal{H}_1 \langle k_{21} \rangle (f_{21}-1)} \\ f_{23} &= 1 - p + p e^{\mathcal{H}_{23} \mathcal{H}_3 \langle k_{32} \rangle (f_{32}-1)} \\ f_{32} &= 1 - p (1 - e^{\mathcal{H}_{23} \mathcal{H}_3 \langle k_{23} \rangle (f_{23}-1)}) (1 - e^{\mathcal{H}_{21} \mathcal{H}_1 \langle k_{21} \rangle (f_{21}-1)}) \end{aligned} \quad (19)$$

where $\mathcal{H}_1 = W(p \langle k_{12} \rangle e^{\langle k_{12} \rangle}) / \langle k_{12} \rangle$ with $W(\cdot)$ being the Lambert W function; $\mathcal{H}_{21} = W(p_{21} \langle k_{21} \rangle e^{\langle k_{21} \rangle}) / \langle k_{21} \rangle$; $\mathcal{H}_{23} = W(p_{23} \langle k_{23} \rangle e^{\langle k_{23} \rangle}) / \langle k_{23} \rangle$ with p_{21} and p_{23} respectively being calculated as $p_{21} = p^{\langle k_{21} \rangle / \langle k_2 \rangle}$ and $p_{23} = p^{\langle k_{23} \rangle / \langle k_2 \rangle}$; and $\mathcal{H}_3 = W(p \langle k_{32} \rangle e^{\langle k_{32} \rangle}) / \langle k_{32} \rangle$.

Fig. 6 displays the theoretical and simulation results on the robustness of tripartite networks subject to target node attacks. Once again the robustness curves drawn in Fig. 6 validate the correctness of our proposed percolation theory. The results recorded in Fig. 6 indicate that the robustness of multipartite networks presents first-order phase transition phenomenon. By comparing Figs. 6 and 5 we can observe that multipartite networks are extremely vulnerable in face of target attacks.

E. Robustness Analysis in the Case of $L > 3$

The above simulations are carried out on L -partite networks with $L = 3$. Here we investigate the robustness of L -partite networks with $L > 3$.

Fig. 6. Theoretical and simulation results on the robustness of tripartite networks with respect to the established cascading model and the introduced node attack model with $\alpha = 1$. A fraction $1 - p$ of nodes are removed from V_i , $\forall i \in [1, 3]$, of a focal tripartite network. The parameter settings for each tripartite network are $n_1 = n_2 = n_3 = 1 \times 10^4$ and $d_1 = d_2 = d$ with the value of d being prescribed in the figure's legend. The values of P_i^∞ and P^∞ are shown with respect to $p \in [0, 1]$ at an interval of 0.025.

Without loss of generality, we consider the situation where the node attacks occur to every partite set of an L -partite network. Specifically, we remove $1 - p$ fraction of nodes from V_i for all $i \in [1, L]$ based on the node attack model formulated in Eq. 3.

Fig. 7. Theoretical and simulation results on the robustness of L -partite networks with respect to the established cascading model and the introduced node attack model with $\alpha = 0$ for the left panel and $\alpha = 1$ for the right panel. A fraction $1 - p$ of nodes are removed from V_i , $\forall i \in [1, L]$ of a focal L -partite network. For each L -partite network, n_i is set to be $n_i = 1 \times 10^4$, $\forall i \in [1, L]$, and d_j is set to be $d_j = 12$, $\forall j \in [1, L - 1]$. The values of P^∞ are shown with respect to $p \in [0, 1]$ at an interval of 0.025.

In the simulations, for an L -partite network we range L from 4 to 7 with an interval of 1. Fig. 7 presents the theoretical and simulation results on the robustness of L -partite networks subject to target node attack based on model given in Eq. 3 respectively with respect to $\alpha = 0$ and $\alpha = 1$. The theoretical results are obtained by numerically solving the generic percolation theory presented in subsection III-D.

We can clearly see from Fig. 7 that, no matter whether an L -partite network is under random node failures or under target attacks, its robustness always displays first-order phase transition phenomenon. The theoretical results yielded by our proposed theory comply well with the simulations.

An interesting yet surprising phenomenon is discovered from Fig. 7. The robustness of an L -partite network is not sensitive to the variable L as the robustness curves recorded in Fig. 7 are very close to each other regardless of the value of L . Note that it has been widely reported that the robustness of interdependent L -layer networks deteriorates rapidly with the increase of L . The above phenomenon suggests that multipartite networks are more robust than multilayer networks.

V. CONCLUSION

Real-world complex systems will inevitably suffer from versatile perturbations and component failures can happen. Because a complex system usually contains a large body of interdependent components, therefore failures of some components will trigger the dysfunction of other components and cascading failures might propagate and bounce back. Note that cascading failures on a system could make the entire system out of control and breakdown. In order to avoid and mitigate system disasters, it is therefore of paramount importance to best understand the robustness of complex systems in face of disturbances.

The robustness of complex systems has been extensively studied in the past decade from the perspective of complex networks. As a consequence, manifold methods based on network theories have been developed, and amongst which are the percolation theories. Due to the multilayer nature of real-world complex systems, percolation theories for multilayer networks have been widely investigated. However, few attention is paid to complex systems with multipartitiveness structures which are depicted by multipartite networks. Multipartite networks are an indispensable component of complex networks and could have profound real-world applications.

In this paper we showed that existing percolation theories can hardly be applied to multipartite networks. With regard to this, we investigated the robustness of multipartite networks. We established the dynamic model for characterizing the cascading failures in multipartite networks. We finally developed the generic percolation theory for quantitatively analyzing the robustness of multipartite networks under node attacks. The proposed theory was validated through simulations on multipartite networks with Poisson degree distributions. Interestingly we discovered that multipartite networks are more robust than multilayer networks in face of node failures. The work presented here not only perfects percolation theories one step forward, but also sheds new light on robust structure design and risk evaluation of complex networks and networked systems.

REFERENCES

- [1] S. Corsi and C. Sabelli, "General blackout in Italy Sunday September 28, 2003, h. 03: 28: 00," in *Proceedings of 2004 IEEE Power Engineering Society General Meeting*. IEEE, 2004, pp. 1691–1702.
- [2] 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.
- [3] Y.-Y. Liu and A.-L. Barabási, "Control principles of complex systems," *Reviews of Modern Physics*, vol. 88, no. 3, p. 035006, 2016.
- [4] L. C. Stige and K. Ø. Kvile, "Climate warming drives large-scale changes in ecosystem function," *Proceedings of the National Academy of Sciences*, p. 201717090, 2017, doi:10.1073/pnas.1717090114.
- [5] Y. Baek, Y. Kafri, and V. Lecomte, "Dynamical symmetry breaking and phase transitions in driven diffusive systems," *Physical Review Letters*, vol. 118, no. 3, p. 030604, 2017.
- [6] A. Zeng, Z. Shen, J. Zhou, J. Wu, Y. Fan, Y. Wang, and H. E. Stanley, "The science of science: From the perspective of complex systems," *Physics Reports*, vol. 714, pp. 1–73, 2017.
- [7] M. E. J. Newman, *Networks: An Introduction*. Oxford University Press, 2010.
- [8] M. Barthélemy, "Spatial networks," *Physics Reports*, vol. 499, no. 1-3, pp. 1–101, 2011.
- [9] P. Holme and J. Saramäki, "Temporal networks," *Physics Reports*, vol. 519, no. 3, pp. 97–125, 2012.
- [10] X. Li and X. Li, "Reconstruction of stochastic temporal networks through diffusive arrival times," *Nature Communications*, vol. 8, 2017, doi:10.1038/ncomms15729.
- [11] H. Liao, M. S. Mariani, M. Medo, Y.-C. Zhang, and M.-Y. Zhou, "Ranking in evolving complex networks," *Physics Reports*, vol. 689, pp. 1–54, 2017.
- [12] R. Parshani, S. V. Buldyrev, and S. Havlin, "Critical effect of dependency groups on the function of networks," *Proceedings of the National Academy of Sciences*, vol. 108, no. 3, pp. 1007–1010, 2011.
- [13] P. T. Johnson, J. C. De Roode, and A. Fenton, "Why infectious disease research needs community ecology," *Science*, vol. 349, no. 6252, p. 1259504, 2015.
- [14] H. Salje, J. Lessler, K. K. Paul, A. S. Azman, M. W. Rahman, M. Rahman, D. Cummings, E. S. Gurley, and S. Cauchemez, "How social structures, space, and behaviors shape the spread of infectious diseases using chikungunya as a case study," *Proceedings of the National Academy of Sciences*, vol. 113, no. 47, pp. 13 420–13 425, 2016.
- [15] R. P. Rohr, S. Saavedra, and J. Bascompte, "On the structural stability of mutualistic systems," *Science*, vol. 345, no. 6195, p. 1253497, 2014.
- [16] S. Allesina, J. Grilli, G. Barabás, S. Tang, J. Aljadeff, and A. Maritan, "Predicting the stability of large structured food webs," *Nature Communications*, vol. 6, no. 7842, pp. 1–6, 2015.
- [17] 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.
- [18] J. G. T. Zañudo, G. Yang, and R. Albert, "Structure-based control of complex networks with nonlinear dynamics," *Proceedings of the National Academy of Sciences*, vol. 114, no. 28, pp. 7234–7239, 2017.
- [19] L. Su and G. Chesi, "Robust stability analysis and synthesis for uncertain discrete-time networked control systems over fading channels," *IEEE Transactions on Automatic Control*, vol. 62, no. 4, pp. 1966–1971, 2017.
- [20] J. Gao, B. Barzel, and A.-L. Barabási, "Universal resilience patterns in complex networks," *Nature*, vol. 530, no. 7590, pp. 307–312, 2016.
- [21] 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," *Proceedings of the National Academy of Sciences*, vol. 113, no. 48, pp. 13 708–13 713, 2016.
- [22] Y. Yang, T. Nishikawa, and A. E. Motter, "Small vulnerable sets determine large network cascades in power grids," *Science*, vol. 358, no. 6365, p. 3184, 2017.
- [23] N. Bof, G. Baggio, and S. Zampieri, "On the role of network centrality in the controllability of complex networks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 3, pp. 643–653, 2017.
- [24] M. E. J. Newman, A.-L. Barabási, and D. J. Watts, *The structure and dynamics of networks*. Princeton University Press, 2011.
- [25] N. Pržulj and N. Malod-Dognin, "Network analytics in the age of big data," *Science*, vol. 353, no. 6295, pp. 123–124, 2016.
- [26] M. Newman, "Network structure from rich but noisy data," *Nature Physics*, 2018, doi:10.1038/s41567-018-0076-1.
- [27] R. C. Dorf and R. H. Bishop, *Modern control systems*. Pearson, 2011.
- [28] Y.-Y. Liu, J.-J. Slotine, and A.-L. Barabási, "Controllability of complex networks," *Nature*, vol. 473, no. 7346, pp. 167–173, 2011.
- [29] F. Pasqualetti, S. Zampieri, and F. Bullo, "Controllability metrics, limitations and algorithms for complex networks," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 1, pp. 40–52, 2014.
- [30] 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.
- [31] S. L. Brunton, J. L. Proctor, and J. N. Kutz, "Discovering governing equations from data by sparse identification of nonlinear dynamical systems," *Proceedings of the National Academy of Sciences*, vol. 113, no. 15, pp. 3932–3937, 2016.
- [32] A. R. Benson, D. F. Gleich, and J. Leskovec, "Higher-order organization of complex networks," *Science*, vol. 353, no. 6295, pp. 163–166, 2016.

- [33] S. S. Morse, J. A. Mazet, M. Woolhouse, C. R. Parrish, D. Carroll, W. B. Karesh, C. Zambrana-Torrel, W. I. Lipkin, and P. Daszak, "Prediction and prevention of the next pandemic zoonosis," *The Lancet*, vol. 380, no. 9857, pp. 1956–1965, 2012.
- [34] P. Sah, S. T. Leu, P. C. Cross, P. J. Hudson, and S. Bansal, "Unraveling the disease consequences and mechanisms of modular structure in animal social networks," *Proceedings of the National Academy of Sciences*, 2017, doi:10.1073/pnas.1613616114.
- [35] A. Wesolowski, E. zu Erbach-Schoenberg, A. J. Tatem, C. Lourenço, C. Viboud, V. Charu, N. Eagle, K. Engø-Monsen, T. Qureshi, C. O. Buckee *et al.*, "Multinational patterns of seasonal asymmetry in human movement influence infectious disease dynamics," *Nature Communications*, vol. 8, no. 1, p. 2069, 2017.
- [36] S. J. Schreiber, R. Ke, C. Loverdo, M. Park, P. Ahsan, and J. O. Lloyd-Smith, "Cross-scale dynamics and the evolutionary emergence of infectious diseases," *Science*, 2017, doi.org/10.1101/066688.
- [37] 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.
- [38] 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.
- [39] H. Zhang, E. Fata, and S. Sundaram, "A notion of robustness in complex networks," *IEEE Transactions on Control of Network Systems*, vol. 2, no. 3, pp. 310–320, 2015.
- [40] D. Zelazo and M. Bürger, "On the robustness of uncertain consensus networks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 2, pp. 170–178, 2017.
- [41] G. Bianconi, "Multilayer networks: Dangerous liaisons?" *Nature Physics*, vol. 10, no. 10, p. 712, 2014.
- [42] S. Soltan, D. Mazauric, and G. Zussman, "Analysis of failures in power grids," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 2, pp. 288–300, 2017.
- [43] Q. Ba and K. Savla, "Robustness of dc networks with controllable link weights," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, pp. 1479 – 1491, 2018.
- [44] 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.
- [45] F. Radicchi and C. Castellano, "Breaking of the site-bond percolation universality in networks," *Nature Communications*, vol. 6, no. 10196, 2015.
- [46] 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.
- [47] 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.
- [48] 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.
- [49] Y. Hu, B. Ksherim, R. Cohen, and S. Havlin, "Percolation in interdependent and interconnected networks: Abrupt change from second- to first-order transitions," *Physical Review E*, vol. 84, no. 6, p. 066116, 2011.
- [50] X. Yuan, S. Shao, H. E. Stanley, and S. Havlin, "How breadth of degree distribution influences network robustness: Comparing localized and random attacks," *Physical Review E*, vol. 92, no. 3, p. 032122, 2015.
- [51] A. Zeng and W. Liu, "Enhancing network robustness against malicious attacks," *Physical Review E*, vol. 85, no. 6, p. 066130, 2012.
- [52] S. Fortunato and D. Hric, "Community detection in networks: A user guide," *Physics Reports*, vol. 659, pp. 1–44, 2016.
- [53] J. Kim and K.-H. Cho, "Robustness analysis of network modularity," *IEEE Transactions on Control of Network Systems*, vol. 3, no. 4, pp. 348–357, 2016.
- [54] M. Sales-Pardo, "The importance of being modular," *Science*, vol. 357, no. 6347, pp. 128–129, 2017.
- [55] X. Han, S. Cao, Z. Shen, B. Zhang, W.-X. Wang, R. Cressman, and H. E. Stanley, "Emergence of communities and diversity in social networks," *Proceedings of the National Academy of Sciences*, vol. 114, no. 11, pp. 2887–2891, 2017.
- [56] 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.
- [57] Q. Cai and J. Liu, "The robustness of ecosystems to the species loss of community," *Scientific Reports*, vol. 6, no. 35904, 2016.
- [58] Z. Wang, D. Zhou, and Y. Hu, "Group percolation in interdependent networks," *Physical Review E*, vol. 97, no. 3, p. 032306, 2018.
- [59] 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.
- [60] M. De Domenico, V. Nicosia, A. Arenas, and V. Latora, "Structural reducibility of multilayer networks," *Nature Communications*, vol. 6, p. 6864, 2015.
- [61] M. De Domenico, A. Solé-Ribalta, E. Omodei, S. Gómez, and A. Arenas, "Ranking in interconnected multilayer networks reveals versatile nodes," *Nature Communications*, vol. 6, p. doi: 10.1038/ncomms7868, 2015.
- [62] S. Pilosof, M. A. Porter, M. Pascual, and S. Kéfi, "The multilayer nature of ecological networks," *Nature Ecology & Evolution*, vol. 1, p. 0101, 2017.
- [63] X. Huang, S. Shao, H. Wang, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "The robustness of interdependent clustered networks," *Europhysics Letters*, vol. 101, no. 1, p. 18002, 2013.
- [64] 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," *Physics Reports*, vol. 544, no. 1, pp. 1–122, 2014.
- [65] M. Kivelä, A. Arenas, M. Barthélemy, J. P. Gleeson, Y. Moreno, and M. A. Porter, "Multilayer networks," *Journal of Complex Networks*, vol. 2, no. 3, pp. 203–271, 2014.
- [66] 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.
- [67] 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.
- [68] D. Li, B. Fu, Y. Wang, G. Lu, Y. Berezin, H. E. Stanley, and S. Havlin, "Percolation transition in dynamical traffic network with evolving critical bottlenecks," *Proceedings of the National Academy of Sciences*, vol. 112, no. 3, pp. 669–672, 2015.
- [69] 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.
- [70] G. Bianconi and S. N. Dorogovtsev, "Multiple percolation transitions in a configuration model of a network of networks," *Physical Review E*, vol. 89, no. 6, p. 062814, 2014.
- [71] Y. Berezin, A. Bashan, M. M. Danziger, D. Li, and S. Havlin, "Localized attacks on spatially embedded networks with dependencies," *Scientific Reports*, vol. 5, no. 8934, 2015.
- [72] 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.
- [73] R.-R. Liu, M. Li, and C.-X. Jia, "Cascading failures in coupled networks: The critical role of node-coupling strength across networks," *Scientific Reports*, vol. 6, p. 35352, 2016.
- [74] 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.
- [75] T. P. Peixoto, "Parsimonious module inference in large networks," *Physical Review Letters*, vol. 110, no. 14, p. 148701, 2013.
- [76] I. L. Boyd, "The art of ecological modeling," *Science*, vol. 337, no. 6092, pp. 306–307, 2012.
- [77] 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.
- [78] 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.
- [79] 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.
- [80] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," *Physical Review E*, vol. 83, no. 6, p. 065101, 2011.
- [81] 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.

VI. APPENDIX

Proof (Proof of Theorem 1) After removing $1 - p_i$ fraction of nodes from $V_i \subset \mathcal{G}$ for $\forall i \in [1, L]$ based on Eq. 3, we get $\mathcal{G}_r$, i.e., the remaining part of $\mathcal{G}$. Similarly, after randomly removing $1 - p_i$ fraction of nodes from $V_i \subset \tilde{\mathcal{G}}$ for $\forall i \in [1, L]$ we have $\tilde{\mathcal{G}}_r$.

From Definition 7 we know that $\mathcal{G}_r$ has the same number of nodes with $\tilde{\mathcal{G}}_r$ does. Moreover, we have $\tilde{P}_{ij}^r(k) = P_{ij}^r(k)$, $\forall i \in [1, L]$. Theorem 1 then can be proved by either of the following ways.

(i) The calculation of the LCC of network $\mathcal{G}_r$ or $\tilde{\mathcal{G}}_r$ is only related to its degree distribution (see [7], pages 1146-1148), therefore the number of nodes in the LCC of $\mathcal{G}_r$ is the same as that of $\tilde{\mathcal{G}}_r$. According to Definition 5, the robustness of $\mathcal{G}$ is thus the same as that of its surrogate network $\tilde{\mathcal{G}}$.

(ii) Although $\mathcal{G}$ is subject to target attacks while $\tilde{\mathcal{G}}$ is under random attacks, $\tilde{\mathcal{G}}_r$ has the same number of nodes as well as the same degree distributions with $\mathcal{G}_r$ does. According to the network model depicted in Fig. 3 we can see that, the robustness calculations of $\mathcal{G}$ and $\tilde{\mathcal{G}}$ are only concentrated on their remaining parts $\mathcal{G}_r$ and $\tilde{\mathcal{G}}_r$. Since $\mathcal{G}_r$ and $\tilde{\mathcal{G}}_r$ possess the same properties, the LCC of $\mathcal{G}_r$ therefore has the same properties with that of $\tilde{\mathcal{G}}_r$, and as a result the robustness of $\mathcal{G}$ is equal to that of $\tilde{\mathcal{G}}$.

Proof (Proof of Lemma 1) We first consider the situation that we remove nodes from V_1 but keep the edges attached to the removed nodes. From Definition 1 we see that nodes in V_1 are isolated from each other as they only have connections to nodes in V_2 . Therefore, the process of randomly removing $1 - p_1$ fraction of nodes from V_1 is equal to the process of uniformly removing elements from the degree sequence of nodes in V_1 . As a result, randomly removing nodes from V_1 will not alter $\tilde{P}_1(k)$, i.e., we have $\tilde{P}_1(k) = P_1^r(k)$. Thus, we have

$$\tilde{G}_1^r(z) = \sum_{k=0}^{n_2} \tilde{P}_1^r(k) z^k = \sum_{k=0}^{n_2} \tilde{P}_1(k) z^k = \tilde{G}_1(z). \quad (20)$$

We then consider the situation that we remove the edges attached to the removed nodes. It is obvious that the edge removal does not change $\tilde{P}_1(k)$ but $\tilde{P}_2(k)$. Note that each node in V_1 has the same probability, i.e., $1 - p_1$, to be removed. Since nodes in V_1 are connected to nodes in V_2 , thus an edge attached to a node in V_2 has the same probability $1 - p_1$ to be deleted. Consequently, $\tilde{P}_2^r(k)$ can be calculated by the following Bernoulli distribution

$$\tilde{P}_2^r(k) = \sum_{m=0}^k \tilde{P}_2(k) \binom{k}{m} (1 - p_1)^m p_1^{k-m}, \quad (21)$$

and based on which we further have

$$\begin{aligned} \tilde{G}_2^r(z) &= \sum_{k=0}^{n_2} \sum_{m=0}^k \tilde{P}_2(k) \binom{k}{m} (1 - p_1)^m p_1^{k-m} z^k \\ &= \tilde{G}_2(1 - p_1 + p_1 z) \end{aligned} \quad (22)$$

Proof (Proof of Lemma 2) We first consider the situation that we intentionally remove $1 - p_i$ fraction of nodes from $V_i \subset \mathcal{G}$ based on Eq. 3 but keep the edges attached to the removed nodes.

For the remaining nodes in V_i , let $n_i^{p_i}(k)$ be the number of nodes with degree k . Thus, we have the following relationship

$$n_i^{p_i}(k) = n_i \cdot p_i \cdot P_i^r(k). \quad (23)$$

Suppose we continue to intentionally remove one node from V_i . In this case, $n_i^{p_i}(k)$ changes to be $n_i^{p_i-1/n_i}(k)$ which can be calculated as

$$n_i^{p_i-1/n_i}(k) = n_i^{p_i}(k) - \frac{P_i^r(k)(k+1)^\alpha}{\sum_{k=0}^{n_i+n_j} P_i^r(k)(k+1)^\alpha}. \quad (24)$$

The above equation also could be rewritten as follows

$$-\frac{1}{n_i} \cdot \frac{n_i^{p_i-1/n_i}(k) - n_i^{p_i}(k)}{-\frac{1}{n_i}} = -\frac{P_i^r(k)(k+1)^\alpha}{\sum_{k=0}^{n_i+n_j} P_i^r(k)(k+1)^\alpha}. \quad (25)$$

In the limit of $n_i, n_j \rightarrow \infty$, we could rewrite Eq. 25 in the form of derivative. More specifically we have

$$\frac{dn_i^{p_i}(k)}{dp_i} = \frac{n_i P_i^r(k)(k+1)^\alpha}{\sum_{k=0}^{\infty} P_i^r(k)(k+1)^\alpha}. \quad (26)$$

By simultaneously calculating the derivatives of the l.h.s and the r.h.s of Eq. 23 we have

$$\frac{dn_i^{p_i}(k)}{dp_i} = n_i P_i^r(k) + n_i p_i \frac{dP_i^r(k)}{dp_i}. \quad (27)$$

Integrating Eqs. 26 and 27 we get

$$p_i \frac{dP_i^r(k)}{dp_i} + P_i^r(k) = \frac{P_i^r(k)(k+1)^\alpha}{\sum_{k=0}^{\infty} P_i^r(k)(k+1)^\alpha}. \quad (28)$$

Eq. 28 is the first-order nonlinear differential equation of $P_i^r(k)$. Based on Definition 8, we directly work out the solution $P_i^r(k)$ to be the one presented in Eq. 8.

Proof (Proof of Lemma 3) We see from Lemma 2 that the expression of $P_i^r(k)$ is mainly characterized by the proportion p_i . Because we have intentionally removed $1 - p_i$ fraction of nodes from $V_i \subset \mathcal{G}$, if we can figure out the equivalent fraction $1 - p_{ij}$ of the nodes from $V_i \subset \mathcal{G}_{ij}$ for $j = \{i-1, i+1\}$, then we could figure out $P_{ij}^r(k)$ in the same manner as presented in the Proof of Lemma 2.

Note that the number of edges in bipartite network $\mathcal{G}_{ij}$ is $|E_{ij}| = n_i \langle k_{ij} \rangle$ where $\langle k_{ij} \rangle = \sum_{k=0}^{\infty} k P_{ij}^r(k)$ is the mean degree of the nodes in $V_i \subset \mathcal{G}_{ij}$. The total number of edges in bipartite networks $\mathcal{G}_{i,i-1}$ and $\mathcal{G}_{i,i+1}$ is $|E_i| = n_i \langle k_i \rangle$. Therefore, the equivalent fraction p_{ij} could be calculated as follows

$$p_{ij} = p_i^{|E_{ij}|/|E_i|} = p_i^{\langle k_{ij} \rangle / \langle k_i \rangle}. \quad (29)$$

As a consequence, intentionally removing $1 - p_i$ fraction of nodes from $V_i \subset \mathcal{G}$ for $i \in [2, L-1]$ based on Eq. 3 is

equal to intentionally removing $1 - p_{ij}$ fraction of nodes from $V_i \subset \mathcal{G}_{ij} \subset \mathcal{G}$.

Analogous to the Proof of Lemma 2, we then have $P_{ij}^r(k) = \frac{1}{p_{ij}} P_{ij}(k) \mathcal{H}_{ij}^{(k+1)\alpha}$, with $\mathcal{H}_{ij} = \mathcal{F}_{ij}^{-1}(p_{ij})$ and $\mathcal{F}_{ij}(p_{ij}) = \sum_{k=0}^{\infty} P_{ij}(k) p_{ij}^{(k+1)\alpha}$.

Proof (Proof of Theorem 3) Consider the situation that we intentionally remove $1 - p_j$ fraction of nodes from $V_j \subset \mathcal{G}$ based on Eq. 3 but keep the edges attached to the removed nodes. According to Lemma 3 we have $P_{ji}^r(k) = \frac{1}{p_{ji}} P_{ji}(k) \mathcal{H}_{ji}^{(k+1)\alpha}$. Analogously, when intentionally removing $1 - p_i$ fraction of nodes from $V_i \subset \mathcal{G}$ based on Eq. 3 but keeping the edges attached to them, based on Lemma 3 we have $P_{ij}^r(k) = \frac{1}{p_{ij}} P_{ij}(k) \mathcal{H}_{ij}^{(k+1)\alpha}$.

Now consider the situation that we remove the edges associated to the removed nodes from V_i and V_j . Note that nodes in V_i are connected to nodes in V_j . Therefore, the edge removals will further change $P_{ji}^r(k)$ and $P_{ij}^r(k)$.

Before node deletions occur, there are totally $|E_{ij}| = n_i \sum k P_{ij}(k)$ edges connecting nodes in V_j and V_i . After the node deletions happen, the number of remnant edges becomes $|E_{ij}^r| = n_i \sum k P_{ij}^r(k)$. Consequently, we can get the following edge proportion

$$q_{ij} = \frac{|E_{ij}^r|}{|E_{ij}|} = \frac{\sum_{k=0}^{\infty} k P_{ij}(k) \mathcal{H}_{ij}^{(k+1)\alpha}}{p_i \sum_{k=0}^{\infty} k P_{ij}(k)}. \quad (30)$$

Analogously, we can have another edge proportion

$$q_{ji} = \frac{|E_{ji}^r|}{|E_{ji}|} = \frac{\sum_{k=0}^{\infty} k P_{ji}(k) \mathcal{H}_{ji}^{(k+1)\alpha}}{p_j \sum_{k=0}^{\infty} k P_{ji}(k)}. \quad (31)$$

The proportion q_{ij} represents the fraction of edges attached to the remaining nodes in V_i that belongs to bipartite network $\mathcal{G}_{ij}$. Putting it another way, when we remove the edges attached to the removed nodes in V_i , a fraction $1 - q_{ij}$ of edges will be randomly removed from $V_j \subset \mathcal{G}_{ij}$. By the same token, when we remove the edges attached to the removed nodes in V_j , a fraction $1 - q_{ji}$ of edges will be randomly removed from $V_i \subset \mathcal{G}_{ij}$.

Analogous to Lemma 1, after deleting the edges attached to the removed nodes from V_i and V_j , we can figure out the new degree distributions of $P_{ji}^r(k)$ and $P_{ij}^r(k)$ as

$$\begin{cases} P_{ji}^r(k) \leftarrow P_{ji}^r(k) \sum_{m=0}^k \binom{k}{m} (1 - q_{ij})^m q_{ij}^{k-m} \\ P_{ij}^r(k) \leftarrow P_{ij}^r(k) \sum_{m=0}^k \binom{k}{m} (1 - q_{ji})^m q_{ji}^{k-m} \end{cases} \quad (32)$$

Then by substituting the above equation into the expressions of $G_{ji}^r(z)$ and $G_{ij}^r(z)$ we have Theorem 3.

Proof (Proof of Theorem 4) Let us consider the event that node B is connected to the LCC via its neighbouring nodes. From Fig. 3 we know that this event only happens when node B is simultaneously connected to the LCC via its neighbours in V_{i-1} and V_{i+1} . Assume that B has k neighbours in V_{i-1} and k neighbours in V_{i+1} . Therefore, the probability for B to belong to the LCC is written as $(1 - f_{i,i-1}^k)(1 - f_{i,i+1}^k)$. With this in hand, we could formulate the relations between P_i^∞ , p_i and $\widetilde{P}_i(k)$ as follows

$$\begin{aligned} P_i^\infty &= p_i \left[1 - \sum_{k=0}^{\infty} \widetilde{P}_{i,i-1}(k) f_{i,i-1}^k \right] \left[1 - \sum_{k=0}^{\infty} \widetilde{P}_{i,i+1}(k) f_{i,i+1}^k \right] \\ &= p_i \left[1 - \widetilde{G}_{i,i-1}(f_{i,i-1}) \right] \left[1 - \widetilde{G}_{i,i+1}(f_{i,i+1}) \right] \end{aligned} \quad (33)$$

Variable $f_{i-1,i}$ denotes the probability for the event that, a node A in V_{i-1} is not connected to the LCC via its neighbouring node B in V_i , to happen. Note that the event that node A is not connected to the LCC via its neighbouring node B could happen under two scenarios:

S1) node B is removed from the network and A definitely does not belong to the LCC;

S2) node B is remained in the network but B itself is not connected to the LCC via its own neighbours.

It is apparent that the case scenario S1 happens with a probability $1 - p_i$. Now let us consider the case scenario S2. As we know that node B could simultaneously have neighbours in partite sets V_{i-1} and V_{i+1} , therefore if B does not belong to the LCC, then B should not be connected to the LCC via node A and C. Analogously, we assume that B has k neighbours in V_{i-1} and k neighbours in V_{i+1} . Thus, the probability for B not to be connected to the LCC can be written as $f_{i,i-1}^k + f_{i,i+1}^k - f_{i,i-1}^k \cdot f_{i,i+1}^k$. Therefore, we have

$$\begin{aligned} f_{i-1,i} &= 1 - p_i + p_i \left[\sum_{k=0}^{\infty} \widetilde{P}_{i,i-1}^{ex}(k) f_{i,i-1}^k + \sum_{k=0}^{\infty} \widetilde{P}_{i,i+1}^{ex}(k) \times \right. \\ &\quad \left. f_{i,i+1}^k - \sum_{k=0}^{\infty} \widetilde{P}_{i,i-1}^{ex}(k) f_{i,i-1}^k \cdot \sum_{k=0}^{\infty} \widetilde{P}_{i,i+1}^{ex}(k) f_{i,i+1}^k \right] \\ &\Rightarrow f_{i-1,i} = 1 - p_i \left[1 - \widetilde{G}_{i,i-1}^{ex}(f_{i,i-1}) \right] \left[1 - \widetilde{G}_{i,i+1}^{ex}(f_{i,i+1}) \right] \end{aligned} \quad (34)$$

where $\widetilde{P}_{i,i-1}^{ex}(k)$ and $\widetilde{P}_{i,i+1}^{ex}(k)$ are, in the literature, generally referred to as the excess degree distributions [7, 24].

The excess degree distribution $\widetilde{P}_{i,i-1}^{ex}(k)$ denotes the probability for node B to have k neighbours in V_{i-1} . $\widetilde{P}_{i,i-1}^{ex}(k)$ is generally calculated as

$$\widetilde{P}_{i,i-1}^{ex}(k) = \frac{(k+1) \widetilde{P}_{i,i-1}(k+1)}{\langle k_{i,i-1} \rangle}. \quad (35)$$

Substituting the above equation into the generating function we have

$$\widetilde{G}_{i,i-1}^{ex}(f_{i,i-1}) = \frac{\widetilde{G}_{i,i-1}'(f_{i,i-1})}{\widetilde{G}_{i,i-1}'(1)}. \quad (36)$$

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 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, 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. He received four Best Paper Awards in premier air traffic conferences, including the IEEE DASC in 2010, the ATM Research and Development in 2011, the ATM Research and Development in 2015, and the ICRAT in 2014.

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.