NETWORK RESILIENCE AND ROBUSTNESS: THEORY AND APPLICATIONS

EDITED BY: Gaogao Dong, Saray Shai, Yongxiang Xia and Dongli Duan
PUBLISHED IN: Frontiers in Physics

frontiers Research Topics

ISSN 1664-8714
ISBN 978-2-88976-782-3
DOI 10.3389/978-2-88976-782-3

About Frontiers

Frontiers is more than just an open-access publisher of scholarly articles: it is a pioneering approach to the world of academia, radically improving the way scholarly research is managed. The grand vision of Frontiers is a world where all people have an equal opportunity to seek, share and generate knowledge. Frontiers provides immediate and permanent online open access to all its publications, but this alone is not enough to realize our grand goals.

Frontiers Journal Series

The Frontiers Journal Series is a multi-tier and interdisciplinary set of open-access, online journals, promising a paradigm shift from the current review, selection and dissemination processes in academic publishing. All Frontiers journals are driven by researchers for researchers; therefore, they constitute a service to the scholarly community. At the same time, the Frontiers Journal Series operates on a revolutionary invention, the tiered publishing system, initially addressing specific communities of scholars, and gradually climbing up to broader public understanding, thus serving the interests of the lay society, too.

Dedication to Quality

Each Frontiers article is a landmark of the highest quality, thanks to genuinely collaborative interactions between authors and review editors, who include some of the world's best academicians. Research must be certified by peers before entering a stream of knowledge that may eventually reach the public - and shape society; therefore, Frontiers only applies the most rigorous and unbiased reviews.
Frontiers revolutionizes research publishing by freely delivering the most outstanding research, evaluated with no bias from both the academic and social point of view. By applying the most advanced information technologies, Frontiers is catapulting scholarly publishing into a new generation.

What are Frontiers Research Topics?

Frontiers Research Topics are very popular trademarks of the Frontiers Journals Series: they are collections of at least ten articles, all centered on a particular subject. With their unique mix of varied contributions from Original Research to Review Articles, Frontiers Research Topics unify the most influential researchers, the latest key findings and historical advances in a hot research area! Find out more on how to host your own Frontiers Research Topic or contribute to one as an author by contacting the Frontiers Editorial Office: frontiersin.org/about/contact

NETWORK RESILIENCE AND ROBUSTNESS: THEORY AND APPLICATIONS

Topic Editors:
Gaogao Dong, Jiangsu University, China
Saray Shai, Wesleyan University, United States
Yongxiang Xia, Hangzhou Dianzi University, China
Dongli Duan, Xi'an University of Architecture and Technology, China

Citation: Dong, G., Shai, S., Xia, Y., Duan, D., eds. (2022). Network Resilience and Robustness: Theory and Applications. Lausanne: Frontiers Media SA.
doi: 10.3389/978-2-88976-782-3

Table of Contents

frontiers | Frontiers in Physics

TYPE Editorial
PUBLISHED 19 July 2022
DOI 10.3389/fphy.2022.972037

OPEN ACCESS

EDITED AND REVIEWED BY
Matjaz Perc,
University of Maribor, Slovenia

*CORRESPONDENCE
Gaogao Dong,
gago999@126.com
Dongli Duan,
mineduan@163.com
Yongxiang Xia,
xiayx@hdu.edu.cn

SPECIALTY SECTION
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

RECEIVED 17 June 2022
ACCEPTED 27 June 2022
PUBLISHED 19 July 2022

CITATION
Dong G, Duan D and Xia Y (2022), Editorial: Network resilience and robustness: Theory and applications. *Front. Phys.* 10:972037. doi: 10.3389/fphy.2022.972037

Editorial: Network resilience and robustness: Theory and applications

Gaogao Dong[1]*, Dongli Duan[2]* and Yongxiang Xia[3]*

[1]School of Mathematical Science, Jiangsu University, Zhenjiang, China, [2]School of Information and Control Engineering, University of Architecture and Technology, Xi'an, China, [3]School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China

KEYWORDS

network resilience, network robustness, network science, network application, network theory

Editorial on the Research Topic
Editorial: Network resilience and robustness: Theory and applications

Network science opens up a new perspective for studying complex networks in social, technological, biological, climate systems, and so on [1]. The structural robustness and dynamic resilience of systems play a key role in risk reduction and damage mitigation [2, 3]. The dynamic resilience of a system is characterized by its ability to adjust its activities to maintain its essential functions in the face of internal disturbances or changes in the external environment. Network robustness refers to the ability of a network to maintain a certain level of structural integrity and original functionality after an attack, and it is the key to whether a compromised network can continue to function properly [4]. In real-world scenarios, networks do not exist in isolation but are coupled together in different ways, including dependent, multi-support, and inter-connected patterns. And, when a coupled network suffers from structural instability or dynamic perturbations, the system with different coupling patterns shows rich phase transition behaviors [5]. The dynamic resilience of a system is characterized by its ability to adjust its activities to maintain its essential functions in the face of internal disturbances or changes in the external environment.

The main areas covered in the collection are the analysis of structural robustness, dynamic elasticity and stability. In particular, the subject focuses on critical phenomena, phase transitions, network dynamics, percolation behavior in network systems, and network applications [6]. This Research Topic also investigates network-specific percolation models, applications of network structure analysis, and applications of network dynamics [7]. The twenty papers it contains do indeed do that. Hopefully, the research papers among them spawn new work and the reviews are useful for those that considers entering this field.

We describe the papers in the order in which they have been published.

The first paper (Guo et al.) according to percolation approach to network reliability is applied to brain networks to study the resistance of the network to interference and

associated failure modes. Different forms of interference are applied to the brain network depending on the metrics characterizing the network structure for percolation. The results show that brain networks are mostly reliable to random or k-core-based percolation, but become vulnerable to degree-based percolation.

The second paper (Lin et al.) is based on the fact that alarm management is essential for high-quality performance of telecommunication systems. Building functional networks by observing pairwise similarities between time series is an effective way to filter and reduce alarm messages.

Paper three (Dongli et al.) reveals the functional importance and resilience patterns of nematode neurons, where the regulatory relationships between neurons and their topology are effectively coupled. By using theoretical approaches such as high-dimensional differential equations and mean fields, they can be used to reveal the influence of biological connectome.

Paper four (Fu et al.) compares four types of synthetic networks by Element Elimination Method (EEM), Resource Allocation method (RAM) and Structural Perturbation Method (SPM). The results show that EEM has higher reconstruction accuracy metrics on the four types of synthetic networks compared to RA and SPM.

Paper five (Huang et al.) studies the resilience enhancement of power systems with a high penetration of renewable energy sources in emergencies. An optimal decision-making approach is proposed to maximize the supply to critical loads and minimize the risk of instability due to the stochastic nature of renewable energy output power.

Paper six (Wu et al.) discusses the effect of intra-layer angular correlation on robustness in terms of embedding interdependent directed networks into hyperbolic spaces. They find that under targeted attacks, robustness decreases with increasing intra-layer angle correlation. Interdependent directed networks without intra-layer angular correlation are always more robust than networks with intra-layer angular correlation.

Paper seven (Du et al.) constructs an inter-provincial virtual water delivery network by combining a multi-regional input-output model and complex network theory, analyzes the overall structural characteristics of the network model, and identifies the structural role of each province. The results show that the "external degree" and "external strength" of the capacity of direct virtual water output have a significant positive impact on water consumption.

Paper eight (Zou et al.) proposes a grid division method considering generator nodes and network weights based on the cluster discovery method in complex network theory. The cascading failure survival capability of different types of networks under different strategies is simulated and analyzed. It is found that the proposed two attack strategies based on subnet division are better than two traditional intentional attack strategies.

Paper nine (Cai et al.) defines two robustness evaluation indicators based on maximum network traffic: traffic capacity robustness to evaluate the network's ability to withstand an attack, and traffic recovery robustness to evaluate the network's ability to rebuild the network after an attack and simulates four networks to analyze their robustness.

Paper ten (Dong et al.) presents coupled network models with different coupling modes developed from real scenarios in recent years to study the robustness of the system. For coupled networks with different coupling modes, the effect of coupling modes on network robustness is described based on network percolation theory.

Paper eleven (Wang et al.) emphasizes that financial crises are rooted in the lack of system resilience and robustness, which can cause severe economic and social losses. The different shapes of the network reveal higher-order correlation patterns in the financial system The proposed approach provides a new perspective for detecting key signals and can be extended to predict other crisis events in natural and social systems.

Paper twelve (Wang et al.) shows that most critical infrastructure networks are frequently subject to vicious attacks, which can lead to network failures. Game theory-based defense strategies are developed to enhance the robustness of networks. In the study, the purpose of protecting infrastructure networks is achieved by allocating limited resources to the targets for monitoring.

Paper thirteen (Song et al.) presents a new network robustness metric for epidemics that combines three characteristics: transmission speed, epidemic threshold, and steady-state infection density. In both homogeneous and heterogeneous networks, the network becomes more robust as the average degree grows.

Paper fourteen (Song et al.) demonstrates that homogeneous networks are more robust than heterogeneous networks at the beginning of the epidemic, while heterogeneous networks become more robust than homogeneous networks as the epidemic progresses. In addition, the irregularity of degree distribution reduces the network robustness of homogeneous networks. In both homogeneous and heterogeneous networks, the network becomes more robust as the average degree grows.

Paper fifteen (Zhan et al.) presents a framework for evaluating the resilience of UAV swarms, which takes into account the load balancing of UAV swarms subjected to disturbances, and demonstrates that topology also has a very important impact on the resilience of UAV swarms.

Paper sixteen (Cui et al.) discovers a framework for classifying normal and abnormal brain activity through a method for constructing multilayer aggregated functional networks, and also provides a general method for constructing more informative functional networks from multiple time series data.

Paper seventeen (Gross and Barth) notes some commonly overlooked complications in computing the size of giant

components. Derive simple formulas to capture the impact of common attack scenarios on arbitrary (configuration model) networks.

Paper eighteen (Li et al.) presents an improved reputation evaluation method by combining the structure of a two-sided rater-subject network with rating information and introducing penalty and reward factors. The results show that the method has better performance than the original correlation-based approach in the presence of spam attacks.

Paper nineteen (Liu and Li) derives closed-form form formulas for the resistance distance and Kirchhoff exponent in terms of the resistance distance and Kirchhoff exponent, respectively, using simple connection diagrams and Laplacian spectra in the general case.

Paper twenty (Sun and Yang) creates a connected graph G with vertex set V(G) and finds that the resistance distance between vertices in S (S⊂V(G)) can be given by the elements in the inverse matrix of the auxiliary matrix of the Laplace matrix of G [S] and deduces the reduction principle obtained in by algebraic methods.

Author contributions

All authors have made a substantial, direct and intellectual contribution to the work, and approved it for publication.

Funding

This research was supported by grants from National Natural Science Foundation of China (Grant Nos. 61973143, 71974080, and 71690242), the Young backbone teachers of Jiangsu Province.

Acknowledgments

We thank all authors contributions for this special issue.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

1. Gao J, Barzel B, Barabási A-L. Universal resilience patterns in complex networks. *Nature* (2016) 530(7590):307–12. doi:10.1038/nature16948

2. Dong G, Fan J, Shekhtman LM, Shai S, Du R, Tian L, et al. Resilience of networks with community structure behaves as if under an external field. *Proc Natl Acad Sci U.S.A* (2018) 115(27):6911–5. doi:10.1073/pnas.1801588115

3. Dong G, Wang F, Shekhtman LM, Danziger MM, Fan J, Du R. Optimal resilience of modular interacting networks. *Proc Natl Acad Sci U S A* (2021) 118(22): e1922831118. doi:10.1073/pnas.1922831118

4. Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. *Nature* (2010) 464(7291):1025–8. doi:10.1038/nature08932

5. Fan J, Dong G, Shekhtman LM, Zhou D, Meng J, Chen X, et al. Structural resilience of spatial networks with inter-links behaving as an external field. *New J Phys* (2018) 20(9):093003. doi:10.1088/1367-2630/aadceb

6. Ganin AA, Kitsak M, Marchese D, Keisler JM, Seager T, Linkov I. Resilience and efficiency in transportation networks. *Sci Adv* (2017) 3(12):e1701079. doi:10.1126/sciadv.1701079

7. Barzel B, Barabási A-L. Universality in network dynamics. *Nat Phys* (2013) 9(10):673–81. doi:10.1038/nphys2741

frontiers in Physics

ORIGINAL RESEARCH
published: 20 July 2021
doi: 10.3389/fphy.2021.698077

Percolation Analysis of Brain Structural Network

Shu Guo[1], Xiaoqi Chen[1], Yimeng Liu[1], Rui Kang[1,2], Tao Liu[3,4,5,6] and Daqing Li[1,2,4]*

[1]School of Reliability and Systems Engineering, Beihang University, Beijing, China, [2]National Key Laboratory of Science and Technology on Reliability and Environmental Engineering, Beijing, China, [3]School of Biological Science and Medical Engineering, Beihang University, Beijing, China, [4]Beijing Advanced Innovation Center for Big Data-Based Precision Medicine, Beijing, China, [5]Beijing Advanced Innovation Center for Biomedical Engineering, Beijing, China, [6]Hefei Innovation Research Institute, Beihang University, Hefei, China

The brain network is one specific type of critical infrastructure networks, which supports the cognitive function of biological systems. With the importance of network reliability in system design, evaluation, operation, and maintenance, we use the percolation methods of network reliability on brain networks and study the network resistance to disturbances and relevant failure modes. In this paper, we compare the brain networks of different species, including cat, fly, human, mouse, and macaque. The differences in structural features reflect the requirements for varying levels of functional specialization and integration, which determine the reliability of brain networks. In the percolation process, we apply different forms of disturbances to the brain networks based on metrics that characterize the network structure. Our findings suggest that the brain networks are mostly reliable against random or k-core-based percolation with their structure design, yet becomes vulnerable under betweenness or degree-based percolation. Our results might be useful to identify and distinguish brain connectivity failures that have been shown to be related to brain disorders, as well as the reliability design of other technological networks.

Keywords: Brain structural network, percolation, reliability, rich club, animal species

OPEN ACCESS

Edited by:
Dongli Duan,
Xi'an University of Architecture and Technology, China

Reviewed by:
Chen Feng,
Ocean University of China, China
Jingfang Fan,
Beijing Normal University, China

****Correspondence:***
Xiaoqi Chen
chenxq@buaa.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *20 April 2021*
Accepted: *03 June 2021*
Published: *20 July 2021*

Citation:
Guo S, Chen X, Liu Y, Kang R, Liu T and Li D (2021) Percolation Analysis of Brain Structural Network. Front. Phys. 9:698077. doi: 10.3389/fphy.2021.698077

INTRODUCTION

Network reliability measures the ability of a network to perform prescribed functions against disturbance. Whether it is a power grid, a transportation network, a brain network, or other functional networks, the losses caused by network failures are huge. The northeast blackout of 2003 in North America, with an estimated 50 million people affected [1], was a large-scale power grid paralysis due to a line trip. And traffic congestions due to network failure usually generate substantial costs every year, together with traffic accidents and disasters [2]. Recent studies have demonstrated that the structural properties of the network largely determine system reliability and resilience under various damage [3–5]. This is also true for brain networks, which are the critical infrastructure for complex biological systems. Many brain disorders, such as Alzheimer disease (AD), amyotrophic lateral sclerosis (ALS), and schizophrenia, etc., have been found related to network connectivity alterations [6], causing physical or psychological pain to patients and their families. Network reliability is of great significance to understand the design principle and failure mechanism of these complex systems.

Accordingly, the network reliability of technological networks is mainly focused on, such as transportation networks, communication networks, and power grids [7]. The study of network reliability involves two-terminal [8], k-terminal [9, 10], and all-terminal [11, 12] network connectivity,

which are defined as the probability that a subset of nodes are able to communicate with each other, and measured as integrity for many networks without distinguishing specific function. In addition, dedicated evaluation methods of reliability are proposed to address specific characteristics of the network. In the transportation network, network reliability mainly considers road destination reachability and commuter travel time. For example, connectivity reliability (CR) refers to the probability of network nodes staying connected, which is a static evaluation of the road network structure [13]. Travel time reliability (TTR), or congestion delay index (CDI), considers the probability of travel time from origin to a destination within a specified interval. And capacity related reliability (CRR) measures the probability that the traffic capacity can support a certain level of traffic demand [14]. In communication networks, note that CRR is also used in evaluating network reliability, with heterogeneous link capacities [15], to sustain the transmission requirements. Diameter-constrained reliability (DCR) is another probability metric about the maximum delay requirements after random failures, which limits the terminal set and path length [16]. In power grids, indicators for measuring network reliability proposed by the European Network of Transmission System Operators for Electricity (ENTSOE) [3] include energy not supplied (ENS), which is an estimation of the supply of energy that final consumers cannot obtain due to incidents. Total loss of power (TLP) is a measure of generation shortfall. And restoration time (RT) refers to the time it takes for the system to recover from the disturbance. The aforementioned research methods of network reliability have similarity to some extent: based on probability tools, they concern the state or efficiency of operative path "connectivity."

In this paper, we focus on the reliability of the brain network. The anatomic connections between the cerebral cortex regions form the structural network on which the neural activities unfold. Functional networks are formed by the dynamical interaction of neural activities among cortical areas [17]. At present, many studies aim at the structural and functional characteristics of brain networks [18], which establish anatomical or functional correlations, calculate features with neurological significance, and reveal the organization principles or operating rules of the brain from the unique perspective of complex networks. The organization of a structure and function network is interdependent. The topology, synchronization, and other dynamic properties of functional networks are strongly influenced by small world and other structural connectivity indicators. On the contrary, the dynamics can adjust the structure network topology in a slower timescale [19]. The coupling of the brain structure and functional network may lead to cascading failure between the two networks, which can be summarized by a universal model [20]. For example, in human brain networks [6], densely connected modules are formed by geometrically close neural elements, promoting the specific function of the local area. And the formation of long-range connections between these modules promotes the scheduling and integration of global function. It is suggested that this "modularity" or "integration" nature changes in the brain connectome with neuropsychiatric disorder. Functional separation refers to the processing of neurons between functional related areas in a community. There are two kinds of integration processes in the network, one is based on the efficiency of global communication, the other is based on the ability of network integration of distributed information [21]. For example, AD patients appear to have modular reorganization in the resting state networks [22], and patients with schizophrenia appear to have reduced density of rich club connections [23], which play a significant role in brain integrative processes, etc. These studies reflect that fact that brain disorders are also strongly related to network structural reliability.

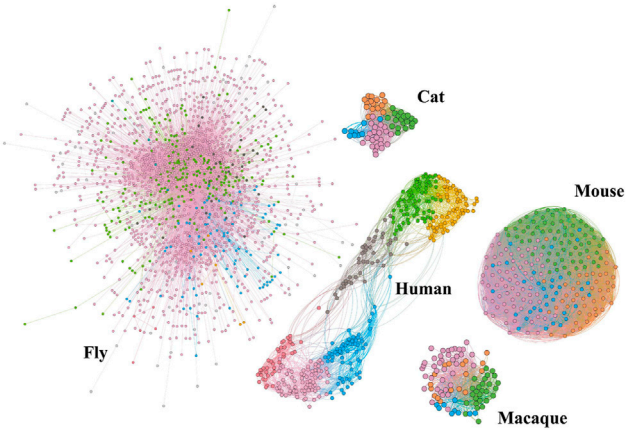


FIGURE 1 | Community topology of brain structural networks for different species, including cat, fly, human, mouse, and macaque. Among them, the networks of cat, fly, mouse, and macaque are from the Network Repository [28] http://networkrepository.com.

Here, we introduce the methods of engineering network reliability into brain network analysis and provide information on how the structural features affect the reliability, aiming at the failure mode of the brain network through the percolation method [24]. The percolation theory [25, 26] is originally used for the diffusion of forest fires or the distribution of oil and gas in porous stones. It has successfully been applied to describe a large variety of natural systems, such as the complex Earth system [27]. It is generalized for the shift of the network state between connected and disconnected at a critical point. We suppose that the critical state represents some inherent properties of the brain network, including the vulnerability of the brain network to varying degrees of external damage. Our study of the percolation process guides us to locate the vulnerable point that causes brain disorder, determine the stage of brain disease, and identify possible common characteristics of different brain disease manifestations.

STRUCTURE OF THE BRAIN NETWORK

To decompose the structure of the network intuitively, we show community topology of structural brain networks of different species in **Figure 1**, including fly, cat, mouse, macaque, and human. This community structural feature is shared by all of these brain networks. Comparatively, the cat and macaque networks belong to small-scale networks (dozens of nodes,

TABLE 1 | Overview of brain structure networks in different species.

Species	Number of nodes	Number of links
Cat	65	730
Fly	1781	9,016
Human	360	6,462
Mouse	91	582
Macaque	213	16,242

hundreds of edges), the human network belongs to medium-scale networks (hundreds of nodes, thousands of edges), and the fly and mouse networks belong to large networks (~tens of thousands of edges). The number of network nodes and edges is shown in **Table 1**. This may be due to the different anatomical resolution of different species. Note that the mouse network is densely connected, while the human network shows a clearer modular pattern with a few connections between different communities. These structural properties can determine the reliability and failure mode of the brain network to some extent.

Next, we calculate the distributions of topological features to compare different species networks, from micro and macro perspectives (shown in **Figure 2**), as well as the meso perspective (shown in **Figure 3**). Degree defines the number of adjacent edges belonging to a given node from a micro perspective. The degree k_i of node i can be calculated according to the adjacency matrix of the network (see **Eq. 1**).

$$k_i = \sum_{j=1}^{n} A_{ij} \tag{1}$$

As shown in **Figure 2A**, degree is normalized by $N-1$ to facilitate comparisons between species brain networks of different scales, where N is the number of nodes in the network. For degree distribution, most nodes in fly, human, and macaque networks have a low degree. For mouse and cat networks, degrees in the mouse network are generally high. Betweenness centrality c_B measures the extent to which all-pairs shortest paths pass through a given node i (see **Eq. 2**) from a macro perspective.

$$c_B(i) = \sum_{st} \frac{g_{st}(i)}{g_{st}} \tag{2}$$

where g_{st} is the number of shortest paths between s, t and $g_{st}(i)$ is the number of those path passing through node i. The betweenness is normalized by $N*(N-1)/2$, as shown in

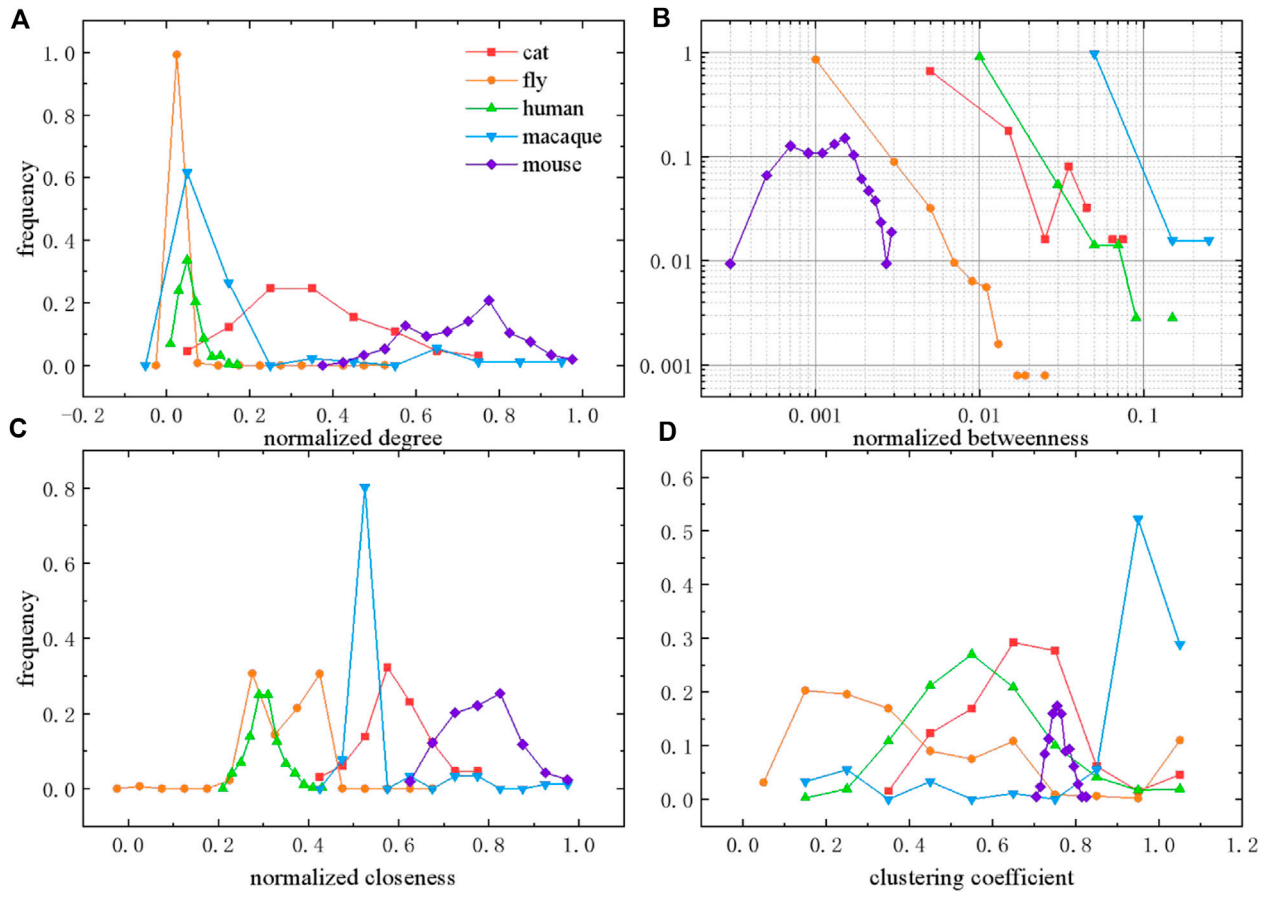


FIGURE 2 | Distributions of topological features in different species brain networks. **(A)** Degree distribution normalized by $N-1$. **(B)** Betweenness distribution normalized by $N*(N-1)/2$. **(C)** Closeness distribution normalized by $1/(N-1)$. **(D)** Clustering coefficient distribution.

Figure 2B. It is suggested that the distributions of different species networks seem to follow a scale free distribution, with the mouse network showing certain deviation. The macaque network has the largest betweenness due to its heterogeneous structure, given its relatively small degree and a few large degree nodes. And the betweenness of the mouse network is the smallest, due to its dense connections. Closeness centrality is another important topological metric from a macro perspective, which is defined as the inverse of the average distance from a given node to others (see **Eq. 3**).

$$c_i = \frac{n-1}{\sum_{j=1}^{n-1} d_{ij}} \tag{3}$$

where d_{ij} is the shortest path length between i and j. The closeness distributions of all species networks, normalized by $1/(N-1)$, are shown in **Figure 2C**. It is shown that the nodes in the mouse network have the highest closeness, and the lowest closeness is in the fly network. The clustering coefficient measures the fraction of two neighbors of a given node that are also connected (see **Eq. 4**).

$$C_i = \frac{2E_i}{k_i(k_i-1)} \tag{4}$$

where node i has degree k_i, and E_i are edges that actually exist between those k_i neighboring nodes. As shown in **Figure 2D**, the distribution of the human network is symmetrical with a characteristic value around 0.6. The macaque network has the largest mean value compared with other distributions, showing strong local connections. Therefore, the structural properties of the network are not completely measured by a single metric, and need comprehensive consideration from different angles.

In the case of the meso perspective, we calculate the rich club coefficient of these species networks with normalization to the null model [29]. The rich club phenomenon, existing in scientific collaboration networks and air transportation networks, is also studied to understand global efficiency in both unweighted and weighted structural brain networks of the human connectome [30], while brain network comparison with other species are rarely involved. Rich club coefficient $\Phi(k)$ (see **Eq. 5**), which quantifies the proximity between nodes with high degrees, is defined as the ratio of the actual number of edges between nodes with degree $>k$ to the total edges.

$$\Phi(k) = \frac{2E_{>k}}{N_{>k}(N_{>k}-1)} \tag{5}$$

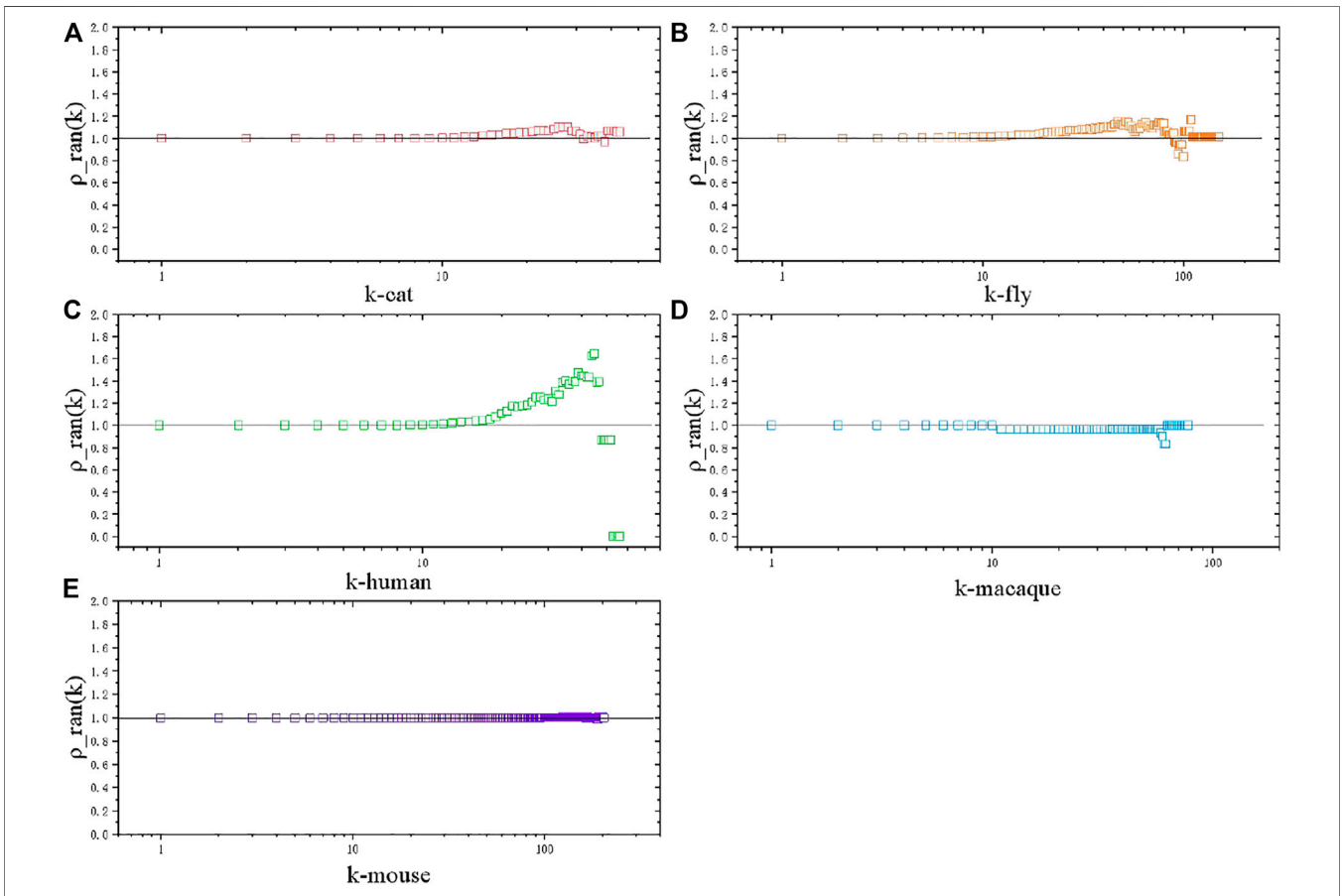


FIGURE 3 | Rich club coefficient, normalized by the null model. **(A)** Cat brain network. **(B)** Fly brain network. **(C)** Human brain network. **(D)** Macaque brain network. **(E)** Mouse brain network.

Considering that nodes with high degrees have higher probability of interconnection with each other by definition, we usually need a null model to obtain normalized rich club coefficient $\rho_{ran}(k)$ (see **Eq. 6**) by comparing original rich club coefficient $\Phi(k)$ with rich club coefficient $\Phi_{ran}(k)$ of the random network (null model) [23, 31].

$$\rho_{ran}(k) = \frac{\Phi(k)}{\Phi_{ran}(k)} \tag{6}$$

The null model is created by performing a link shuffle to randomize the original network, keeping the same degree distribution. $\rho_{ran}(k)$ greater than 1 reflects the rich club phenomenon of a network. As shown in **Figure 3**, the rich club phenomenon is significant in the human network (**Figure 3C**), indicating that nodes with high degrees tend to connect with each other, which may enable global functional communication and integration of distributed brain regions. Our results suggest also that brain networks of other species do not show significantly similar routing principles of integration. It is found that cat and fly networks display a very weak rich club effect (**Figures 3A,B**), and rich club coefficients in macaque and mouse networks are almost close to 1 (**Figures 3D,E**). We suppose that the human brain network, compared to other species, has more complicated and diverse functions with higher integration requirements, leading to a much higher rich club coefficient. Meanwhile, the structural properties may affect the reliability of the brain network, which will be discussed in the next section. Actually, networks with rich clubs are usually more vulnerable [32], because the removal of a few rich club members can destroy the overall global connectivity. Here we focus on the connectivity performance of the brain network under different disturbances, through percolation analysis.

PERCOLATION ON THE BRAIN NETWORK

In this section, we perform different types of percolation analysis, including degree-based percolation, betweenness-based percolation, k-core-based percolation, and random percolation. Percolation of different types may represent different external disturbances [33]. We remove nodes from the network with a fraction q according to the network structural features concerning degree, betweenness, and k-core. When the removal fraction is tuned increasingly from zero to unit, at a certain critical probability q_c, the state of the network shifts from connected to disconnected, and this critical phenomenon is called percolation. In the percolation case, we have no giant cluster for $q > q_c$ and one giant cluster at least for $q < q_c$. The critical probability q_c for networks with different topological properties may be different, determined by the structure of the network. We analyze the performance of networks during the percolation process, to reveal how the brain networks of different species

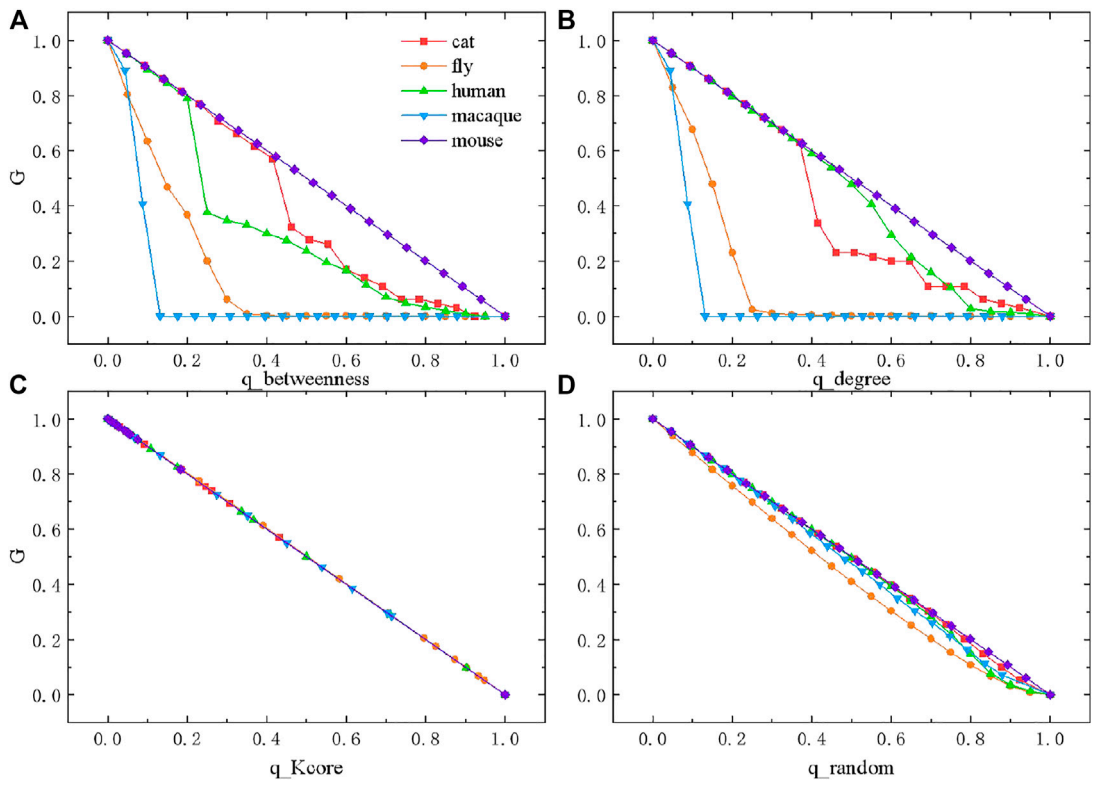


FIGURE 4 | Percolation on species brain networks under four forms of disturbances. **(A)** Percolation based on betweenness. **(B)** Percolation based on degree. **(C)** Percolation based on k-core. **(D)** Random percolation.

respond to disturbance. When different external types of disturbances are applied to the network, the reliability and failure modes of the network could be uncovered.

The giant component G (size of the largest connected component) of the network decreases with the removal fraction in **Figure 4**. As the nodes are removed gradually with a certain order, it will generate various damages to the original network. **Figure 4A** is the betweenness-based percolation, we remove nodes in descending order of betweenness. It is notable that G, for the macaque brain network, drops comparatively fast with a certain critical removed fraction around 0.1, which is because the macaque network has the largest betweenness. When approaching the critical point, we can observe a sharp decline in the giant component, which may be accompanied by a substantial or complete loss of network function. Other brain networks also decrease quickly at their critical point, except for the mouse brain network. For the strong robustness of the mouse network against disturbances, where the giant component is decreasing almost linearly, we can see from **Figure 2A** that the connections in the mouse network are particular dense, meaning that the network is highly connected globally. When one of the nodes is removed, other nodes can still maintain connections, which constitutes the high reliability of the mouse brain network. **Figure 4B** is the degree-based percolation, we remove nodes in descending order of degree. As the betweenness-based percolation, we can observe a similar trend for different species. The cat brain network decreases faster than the human brain network for degree-based percolation.

Next, we perform k-core-based percolation in **Figure 4C**. k-core decomposition is a method to decompose and analyze the hierarchy structure of the network [34]. When we remove nodes with a degree less or equal to $(k-1)$ from the network, all the remaining nodes with an updated degree larger or equal to k in the remaining graph are called k-core. Nodes belonging to k-core, yet not belonging to $(k+1)$-core, are defined as k-shell. In k-core-based percolation, we start with the smallest k-shell and remove the nodes from the network at each step. Differing from the above two percolation modes, the percolation based on k-core shows a distinct failure mode. All species brain networks follow a linear decrease pattern. This is due to the fact that a higher k-shell of networks will not become disconnected when small layers are removed.

In contrast to the above three percolation methods based on the network structural features, we also perform random percolation (**Figure 4D**). Without considering network topology, we randomly remove a fraction of nodes from the network at each step. Surprisingly, the change of G in the network during the random percolation process is almost uniform throughout, where every decrement is similar for each removal fraction. This is possibly because a few highly connected nodes in each network behave like a backbone and maintain the whole network.

CONCLUSION

We perform network reliability analysis on a brain network, which is the critical infrastructure for biological intelligence. Network reliability pursues the ability to meet the functional requirements in a specific operating environment. Therefore, the fragility of the network under disturbance is particularly important, that a network with high-reliability has the ability to offset the impact of disturbances and strives to maintain connectivity. Here, we pay attention to the global and local connectivity of the brain network, whose loss may cause biological dysfunction as brain disorders. We analyze the brain networks of different species, including cat, fly, human, mouse, and macaque, and explore similarities and differences in structural features and percolation patterns, which may reflect the causality from varying levels of functional specialization and integration.

While the properties of species brain networks are formed during evolution, one of the core tasks is to ensure high reliability, against various disturbances. High reliability of the network suggests balance between global connectivity and local connectivity. We find that brain networks are mostly reliable against random or k-core-based percolation with their structure design, yet they become vulnerable under betweenness or degree-based percolation. Furthermore, our study may be useful for building models for the inherent reliability of the brain network, and help to discover the operating rules and disease mechanisms that may exist during the process of operation. Although for the brain or other biological networks, it may be difficult to artificially revise the wiring rules of the network, we hope that an identified relation between the brain organization principles and external disturbances can help guide the avoidance of brain disorders, as reference for other technological networks.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. This data can be found here: http://networkrepository.com/bn.php.

ETHICS STATEMENT

Ethical review and approval was not required for the animal study because our data comes from a public data set.

AUTHOR CONTRIBUTIONS

SG, XQC, and YML performed the analysis. XQC validated the analysis and drafted the manuscript. RK and TL reviewed the manuscript. DQL designed the research. All authors have read and approved the content of the manuscript.

FUNDING

We acknowledge support from National Natural Science Foundation of China Grants 71822101, 71890973/71890970, 61961146005, and 71771009.

REFERENCES

1. Minkel JR. The 2003 Northeast Blackout–Five Years Later[J]. *Scientific American* (2008) 13.
2. Iida Y. Basic Concepts and future directions of road network reliability analysis. *Atr* (1999) 33(2):125–34. doi:10.1002/atr.5670330203
3. Martinez-Anido CB, Bolado R, De Vries L, Fulli G, Vandenbergh M, and Masera M. European power grid reliability indicators, what do they really tell? *Electric Power Syst Res* (2012) 90:79–84.
4. Moreno Y, Nekovee M, and Vespignani A. Efficiency and reliability of epidemic data dissemination in Complex networks. *Phys Rev E* (2004) 69(5):055101. doi:10.1103/physreve.69.055101
5. Zeng G, Li D, Guo S, Gao L, Gao Z, Stanley HE, et al. Switch between Critical percolation modes in City traffic dynamics. *Proc Natl Acad Sci USA* (2019) 116(1):23–8. doi:10.1073/pnas.1801545116
6. Van den Heuvel MP, and Sporns O. A Cross-disorder Connectome landscape of brain dysconnectivity. *Nat Rev Neurosci* (2019) 1.
7. Duan D-L, Ling X-D, Wu X-Y, and Zhong B. Reconfiguration of distribution network for loss reduction and reliability improvement based on an enhanced genetic algorithm. *Int J Electr Power Energ Syst* (2015) 64:88–95. doi:10.1016/j.ijepes.2014.07.036
8. Ramirez-Marquez JE, and Coit DW. A Monte-Carlo simulation approach for approximating multi-state two-terminal reliability. *Reliability Eng Syst Saf* (2005) 87(2):253–64. doi:10.1016/j.ress.2004.05.002
9. Hardy G, Lucet C, and Limnios N. K-terminal network reliability measures with binary decision diagrams. *IEEE Trans Rel* (2007) 56(3):506–15. doi:10.1109/tr.2007.898572
10. Yeh F-M, Lu S-K, and Kuo S-Y. OBDD-based evaluation of k-terminal network reliability. *IEEE Trans Reliability* (2002) 51(4):443–51.
11. Sharafat AR, and Ma'rouzi OR. All-terminal network reliability using recursive truncation algorithm. *IEEE Trans Rel* (2009) 58(2):338–47. doi:10.1109/tr.2009.2020120
12. Srivaree-Ratana C, Konak A, and Smith AE. Estimation of all-terminal network reliability using an artificial neural network. *Comput Operations Res* (2002) 29(7):849–68. doi:10.1016/s0305-0548(00)00088-5
13. Bell MG, and Iida Y. *Transportation Network analysis*. New York: Chichester (1997). doi:10.1002/9781118903032
14. Chen A, Yang H, Lo HK, and Tang WH. A Capacity related reliability for transportation networks. *Atr* (1999) 33(2):183–200. doi:10.1002/atr.5670330207
15. Soh S, and Rai S. An efficient Cutset approach for evaluating Communication-network reliability with heterogeneous link-Capacities. *IEEE Trans Rel* (2005) 54(1):133–44. doi:10.1109/tr.2004.842530
16. Cancela H, and Petingui L. Diameter Constrained network reliability: exact evaluation by factorization and bounds. *Reportes Técnicos* (2001) 01-03.
17. Honey CJ, Kötter R, Breakspear M, and Sporns O. Network structure of Cerebral Cortex shapes functional Connectivity on multiple time scales. *Proc Natl Acad Sci* (2007) 104(24):10240–5. doi:10.1073/pnas.0701519104
18. Rubinov M, and Sporns O. Complex network measures of brain Connectivity: uses and interpretations. *Neuroimage* (2010) 52(3):1059–69. doi:10.1016/j.neuroimage.2009.10.003
19. Bullmore E, Ed, and Complex brain networks: graph theoretical analysis of structural and functional systems, O Sporns. Complex brain networks: graph theoretical analysis of structural and functional systems. *Nat Rev Neurosci* (2009) 10(3):186–98. doi:10.1038/nrn2575
20. Duan D, Lv C, Si S, Wang Z, Li D, Gao J, et al. Universal behavior of Cascading failures in interdependent networks. *Proc Natl Acad Sci USA* (2019) 116(45):22452–7. doi:10.1073/pnas.1904421116
21. Sporns O. Network attributes for segregation and integration in the human brain. *Curr Opin Neurobiol* (2013) 23(2):162–71. doi:10.1016/j.conb.2012.11.015
22. Chen G, et al. Modular reorganization of brain resting state networks and its independent validation in Alzheimer's disease patients. *Front Hum Neurosci* (2013) 7:456. doi:10.3389/fnhum.2013.00456
23. Van den Heuvel MP, Sporns O, Collin G, Scheewe T, Mandl RCW, Cahn W, et al. Abnormal rich Club organization and functional brain dynamics in schizophrenia. *JAMA psychiatry* (2013) 70(8):783–92. doi:10.1001/jamapsychiatry.2013.1328
24. Li D, Zhang Q, Zio E, Havlin S, and Kang R. Network reliability analysis based on percolation theory. *Reliability Eng Syst Saf* (2015) 142:556–62. doi:10.1016/j.ress.2015.05.021
25. Stauffer D, and Aharony A. *Introduction to percolation theory*. United Kingdom: Taylor & Francis (2018). doi:10.1201/9781315274386
26. A Bunde and S Havlin, editors. *Fractals and Disordered Systems*. Germany: Springer Science & Business Media (2012).
27. Fan J, Meng J, Ludescher J, Chen X, Ashkenazy Y, Kurths J, et al. Statistical physics approaches to the Complex Earth system. *Phys Rep* (2020) 8:961–84. doi:10.1016/j.physrep.2020.09.005
28. Rossi R, and Ahmed N. The network data repository with interactive graph analytics and visualization. in Twenty-Ninth AAAI Conference on Artificial Intelligence; Austin, TX, United States. AAAI Press (2015).
29. Colizza V, Flammini A, Serrano MA, and Vespignani A. Detecting rich-Club ordering in Complex networks. *Nat Phys* (2006) 2(2):110–5. doi:10.1038/nphys209
30. Van den Heuvel MP, and Sporns O. Rich-club organization of the human Connectome. *J Neurosci* (2011) 31(44):15775–86. doi:10.1523/jneurosci.3539-11.2011
31. McAuley JJ, da Fontoura Costa L, and Caetano TS. Rich-club phenomenon across Complex network hierarchies. *Appl Phys Lett* (2007) 91(8):084103. doi:10.1063/1.2773951
32. Zhou S, and Mondragón RJ. The rich-Club phenomenon in the Internet topology. *IEEE Commun Lett* (2004) 8(3):180–2. doi:10.1109/lcomm.2004.823426
33. Fornito A, Zalesky A, and Breakspear M. The Connectomics of brain disorders. *Nat Rev Neurosci* (2015) 16(3):159–72. doi:10.1038/nrn3901
34. Carmi S, Havlin S, Kirkpatrick S, Shavitt Y, and Shir E. A model of Internet topology using k-shell decomposition. *Proc Natl Acad Sci* (2007) 104(27):11150–4. doi:10.1073/pnas.0701175104

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 11 August 2021
doi: 10.3389/fphy.2021.732835

Network Reconstruction in Terms of the Priori Structure Information

Jia-Qi Fu[1], *Qiang Guo*[1], *Kai Yang*[2] *and Jian-Guo Liu*[3,4]*

[1]Research Center of Complex Systems Science, University of Shanghai for Science and Technology, Shanghai, China, [2]College of Information Engineering, Yangzhou University, Yangzhou, China, [3]Institute of Accounting and Finance, Shanghai University of Finance and Economics, Shanghai, China, [4]Shanghai Engineering Research Center of Finance Intelligence, Shanghai University of Finance and Economics, Shanghai, China

In this paper, we investigate the reconstruction of networks based on priori structure information by the Element Elimination Method (EEM). We firstly generate four types of synthetic networks as small-world networks, random networks, regular networks and Apollonian networks. Then, we randomly delete a fraction of links in the original networks. Finally, we employ EEM, the resource allocation (RA) and the structural perturbation method (SPM) to reconstruct four types of synthetic networks with 90% priori structure information. The experimental results show that, comparing with RA and SPM, EEM has higher indices of reconstruction accuracy on four types of synthetic networks. We also compare the reconstruction performance of EEM with RA and SPM on four empirical networks. Higher reconstruction accuracy, measured by local indices of success rates, could be achieved by EEM, which are improved by 64.11 and 47.81%, respectively.

Keywords: network reconstruction, element elimination method, priori structure information, time-series information, evolutionary game

OPEN ACCESS

Edited by:
Mahdi Jalili,
RMIT University, Australia

Reviewed by:
Francisco Welington Lima,
Federal University of Piauí, Brazil
Ke Hu,
Xiangtan University, China

***Correspondence:**
Jian-Guo Liu
liujg004@ustc.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *29 June 2021*
Accepted: *27 July 2021*
Published: *11 August 2021*

Citation:
Fu J-Q, Guo Q, Yang K and Liu J-G (2021) Network Reconstruction in Terms of the Priori Structure Information. Front. Phys. 9:732835. doi: 10.3389/fphy.2021.732835

1 INTRODUCTION

Reconstructing a network based on priori structure information has attracted lots of attention for the network science [1]. Prior information about the connectivity patterns or potential interactions of the networks are accessible via public database [2, 3], high-throughput experiments [4], or data mining of interaction knowledge [5–7]. A wide diversity of methods based on priori structure information have been developed for the problem of network reconstruction [1, 8, 9]. Among various models, a few reconstruction models would provide a reliable estimate of a network's structure with priori structure information. Link prediction is a typical method which uses accessible structure to estimate the likelihood of existence of unobserved links or identifies spurious links in a network [10, 11]. The unknown structure of a network is then reconstructed by link prediction. A few link prediction models are validated in both synthetic networks and empirical networks, which are local similarity indices [12–14], maximum likelihood methods [11, 15] and methods based on predictability [16, 17].

The other method uses accessible structure information to reconstruct a class of networks with evolutionary games [18, 19]. Such model, known as compressive sensing reconstruction model (CSR), is initially proposed to solve the problems of global network reconstruction [20–22]. The CSR method provides theoretical framework to dealing with networks purely from measured time-series information. To reconstruct a network with N nodes, the CSR method reconstructs the adjacent matrix column by column and each column is a vector with N elements [23, 24]. Contrary to the CSR method, the adjacent matrix is reconstructed by the Element Elimination Method (EEM) in a similar fashion, but the number of elements in different column might be $N_i (N_i \leq N, i = 1, 2, \ldots, N)$ because EEM initially eliminates coupling nodes based on priori structure information. Exploiting the natural

sparsity of the vectors, the pioneering work has applied EEM to achieve a successful reconstruction in scale-free networks with a small fraction of hubs [25]. However, in many cases, examples of real-world networks are not characterized by scale-free [26], i.e., the collaboration network of film actors [27, 28], the neural network of the worm *Caenorhabditis elegans* [26], the power grid of the western United States [29, 30], and drug trafficking network [31], et al. In addition, unique structure could be observed in world airline networks [32, 33] and Apollonian networks [34–36], which are characterized by scale-free and also satisfies basic features of small-world. EEM for reconstructing networks characterized by other features has not been fully explored. We are interested in, to achieve a successful reconstruction, the detailed amount of time-series information required for EEM in spite of the priori structure information. This motivates us to investigate the application of EEM to other networks characterized by different features.

In this paper, we investigate the reconstruction of general networks, which are characterized by four types of synthetic networks as small-world networks, random networks, regular networks and Apollonian networks. Typically, the reconstruction accuracy of EEM is evaluated on four types of networks. We will show the performance of EEM, characterized by low information requirements and high reconstruction accuracy. Experiments on four synthetic networks demonstrate that comparing with the resource allocation (RA) [12] and the structural perturbation method (SPM) [16], EEM can effectively enhance the reconstruction accuracy. Further, three local indices of success rates demonstrate that the reconstruction accuracy obtained by EEM when reconstructing three separately local structure in a network is close. In addition, experiments on four empirical networks demonstrate that EEM outperforms RA and SPM. Compared with RA and SPM, EEM has higher reconstruction accuracy, measured by local indices of success rates, which are improved by 64.11 and 47.81%, respectively.

2 METHODS AND MODELS

2.1 The Procedure of the Network Reconstruction

Uncovering a network's structure has many potential applications so that we can assess the system's resilience [37–39], understand the dynamical mechanisms [40], identify significant nodes in a network [41, 42], detect community structure [43], locate diffusion sources Hu et al. [44, 45], and analyze the networks' properties [46–48]. In this paper, an Element Elimination Method (EEM) [25] is employed to reconstruct the structure of networks. We then give the illustration of the procedures of employing EEM to reconstruct synthetic networks: 1) Generate synthetic networks. 2) Extract time-series information from observed data. 3) Reconstruct the networks with EEM. Noting that the adjacent relationships between nodes in the network are sparse and would not change over time, we could explore the casual relationships between nodes' time-series information. Consequently, we could uncover the unknown link set $\boldsymbol{E}^P$ of the networks by EEM based on priori link set $\boldsymbol{E}^T$.

As illustrated in **Figure 1**, a procedure of network reconstruction is presented. Supposing the relationships between node 2 and other 5 nodes should be reconstructed, and only one adjacent relationship (a blue line in **Figure 1A**) is known. However, we are confused about which one is the original network from vastly different networks with possible connective relationships. Simultaneously, the network is evolving over the time, and a few time-series information of nodes' strategies and payoffs could be obtained. We then build a model to bridge node 2's strategies and its payoffs, as **Figure 1B** illustrated. Consequently, we can use EEM to reconstruct the network's structure and obtain the adjacent relationships as shown in **Figure 1C**.

2.2 Generation of Synthetic Network

In order to evaluate the reconstruction performance of EEM in small-world networks and networks characterized by other features, we generate four types of synthetic networks. Noting that small-world network is a model of network that can be tuned between random network and regular network [26], we also consider the networks when their connection topology is assumed to be completely regular or completely random. Besides, the performance on the Apollonian networks by EEM has seldom been evaluated. Then, we generate four types of synthetic networks which are small-world networks, random networks, regular networks and Apollonian networks. The precedent findings indicate that the assortative coefficient has a direct influence on the accuracy of network reconstruction [49]. Therefore, some statistical properties have to be tuned when the networks are generated.

Supposing a network is composed of N nodes and $|\boldsymbol{E}|$ links. To minimize the influence from different network structure, we fix a default mean assortative coefficient $\langle r\rangle$ for three types of synthetic networks, excluding Apollonian networks. Given wiring rules between nodes, we could generate vastly different networks with the given number of nodes N. Initially, the generated synthetic networks should have sufficient links that the total number of links of the network should exceed the number of links $|\boldsymbol{E}|$. Then we randomly delete some of the links so that the number of the residual links is equal to $|\boldsymbol{E}|$. In this way, the generated synthetic networks would have N nodes and $|\boldsymbol{E}|$ links. We select one network from the synthetic network set whose mean assortative coefficient is close to the value of default $\langle r\rangle$ (the absolute error is less than 10^{-3}). The other types of synthetic networks are generated by another wiring rules in a similar way. Actually, synthetic networks generated whose statistical properties are close to default value are limited. On the other hand, the generation procedure of the regular network and the Apollonian network results in merely one realization of the synthetic networks. In this paper, each synthetic network has performed only one realization for the experiments.

Due to privacy or confidentiality issues, the complete structure of a network is not accessible. In addition, it is an impossible mission for us to record nodes' complete time-series information. In spite of the difficulties, some priori information about the adjacent relationships between a few nodes, and discrete records of nodes' time-series information might be available. Despite the

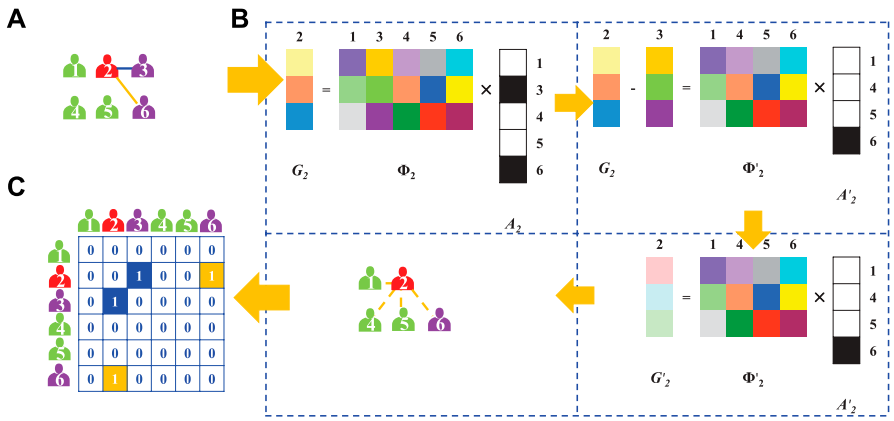


FIGURE 1 | (Color Online) An illustration of reconstructing the hidden structure of a node based on priori structure information. **(A)** Original adjacent relationships of a node. For a node 2 in red with two neighbors, node 3 and node 6 in purple, we can observe a priori relationship, represented with a blue line, between node 2 and node 3. **(B)** EEM. We establish vector $\boldsymbol{G}_2$ and matrix $\boldsymbol{\Phi}_2$ in the reconstruction form $\boldsymbol{G}_2 = \boldsymbol{\Phi}_2 \cdot \boldsymbol{A}_2$ from time-series information, where vector $\boldsymbol{A}_2$ captures the adjacent relationships between node 2 and the other nodes. After subtracting time-series information determined by node 2 and priori neighbor, node 3, on the both sides of the equation, the unknown connections of node 2 can be reconstructed by optimizing the solution of the following equation $\boldsymbol{G}'_2 = \boldsymbol{\Phi}'_2 \cdot \boldsymbol{A}'_2$ using EEM. **(C)** A reconstructed adjacent matrix. The unknown neighbors of node 2 could be uncovered by EEM. The adjacent matrix is presented, in which golden blocks represent reconstructed link.

limited information, the connective relationships between nodes has a direct effect on the individual node, which contributes to node's attitude or selection in the next time. The dependence from the network's structure on nodes' interactions provide information for us to utilize the time-series information of nodes to describe the adjacent relationships behind them [24, 50].

2.3 The Model of the Evolutionary Game

The main challenge lies in that the structure of the network is inaccessible, also in that merely limited nodes' time-series information is available. Since the time-series information is closely related to the connective relationships between nodes, we can reconstruct the unknown structure from the limited time-series information.

We use an evolutionary game model, the Prisoner Dilemma Game (PDG) model, to describe the nodes' dynamics [51–53]. In each round of the game, the nodes usually weigh the benefits against the risks and selects a strategy. Here, we use $\boldsymbol{SY}_i(t)$ to define the strategy of node i. We denote vector $\boldsymbol{SY}_i(t) = (1,0)^T$ to represent a cooperation strategy, while we denote $\boldsymbol{SY}_i(t) = (0,1)^T$ to represent a defection strategy. Here, T stands for 'transpose'.

When node i and node j trigger a game, the payoff of node i is dependent on both two nodes' strategies and a uniform payoff matrix $\mathbf{P}$, which is defined as:

$$\mathbf{P} = \begin{pmatrix} 1 & 0 \\ b & 0 \end{pmatrix} \tag{1}$$

where b $(1 < b < 2)$ is a parameter characterizing the volume of payoff when node i select a defection strategy. In the t round, node i would play with all its different neighbors with the same strategy. When node i encounters a neighbor j, node i would gain payoff from node j as:

$$F_{ij}(t) = \boldsymbol{SY}_i^T(t) \cdot \mathbf{P} \cdot \boldsymbol{SY}_j(t). \tag{2}$$

In the same round, node i's total payoffs $\boldsymbol{G}_i$ would be calculated, and it is the sum of the payoffs from all node i's neighbors.

In a new round, node i would attempt to maximize its payoffs by updating its strategy. According to Fermi rule [54], node i randomly select a node j from its neighbors after t round. In $t + 1$ round, node i would then adopt node j's strategy with the probability

$$W(\boldsymbol{SY}_i(t+1) \leftarrow \boldsymbol{SY}_j(t)) = \frac{1}{1 + exp[(TG_i(t) - TG_j(t))/\kappa]}, \tag{3}$$

where $TG_i(t)$ is node i's cumulative payoffs from 1 to t round. $TG_j(t)$ is similarly defined. Parameter κ characterizes node's rationality when it update strategies. Parameter $\kappa = 0$ corresponds to rational selection behavior of nodes.

Since game occurs among connected nodes, the information of the adjacent relationships between nodes are hidden in their dynamical records of strategies or payoffs in the game. Then we can utilize the information to uncover a networks' structure when we collect the time-series information about the strategies and payoffs of nodes. When we reconstruct a certain network, the limited time-series information is usually presented in a random sample of sufficient time-series information.

2.4 Element Elimination Method

Given limited time-series information of nodes, an EEM could be applied to reconstruct a network based on priori structure information. EEM is a variant of the CSR method, which utilizes priori structure information to exclude the priori connective relationships before reconstruction. Suppose that the relationships between nodes in a certain network can be represented by an adjacency matrix $\mathbf{A}$ with dimensions $N \times N$, where N is the number of nodes in the network. EEM decomposes the process of reconstructing the entire network into many subnetwork recovery

TABLE 1 | The statistical properties of four synthetic networks.

Networks	N	$\|E\|$	⟨k⟩	⟨r⟩	⟨C⟩	⟨D⟩
WS network	120	480	8	−0.05	0.50	3.38
RM network	120	480	8	−0.05	0.10	2.53
RG network	120	480	8	NAN	0.64	7.94
AP network	124	366	5.90	−0.27	0.81	2.57
WS network	250	1,000	8	−0.05	0.50	4.07
RM network	250	1,000	8	−0.05	0.10	Inf
RG network	250	1,000	8	NAN	0.64	16.06
AP network	367	1,095	5.97	−0.21	0.82	2.96

problems, and the network structure, namely, the adjacency matrix $\mathbf{A}$, is reconstructed column by column [55,56]. An adjacency vector $\boldsymbol{A}_i$ of a node is used to describe the adjacent relationships between node i ($i = 1, 2, \ldots, N$) and the other $N - 1$ nodes in the network, which contains no loop. The adjacency vector $\boldsymbol{A}_i = (a_{i1}, a_{i2}, \ldots, a_{i,i-1}, a_{i,i+1}, \ldots, a_{i,N})^T$ with element $a_{ij} = 1$ when node i and node j are connected, and $a_{ij} = 0$ otherwise. Suppose that N_i ($N_i \leq N - 1$) nodes in the adjacency vector $\boldsymbol{A}_i$ have undetermined relationships with node i. EEM is employed to find out node i's ($i = 1, 2, \ldots, N$) direct neighbors from N_i possible nodes, namely a shorter adjacency vector $\boldsymbol{A}_i = (a_{i1}', a_{i2}', \ldots, a_{i,N_i}')^T$ of node i ($i = 1, 2, \ldots, N$).

The training set $\boldsymbol{E}^T$ sheds light on the priori neighbor set $\boldsymbol{\Gamma}_i^K$ of node i, which contains $(N - N_i - 1)$ nodes. Then we could calculate the sum of payoffs $\boldsymbol{G}'_{\boldsymbol{\Gamma}_i^K}$ of node i obtained from the priori neighbors in neighbor set $\boldsymbol{\Gamma}_i^K$ according to **Eq. 2**. Subtracting payoffs $\boldsymbol{G}'_{\boldsymbol{\Gamma}_i^K}$ from $\boldsymbol{G}_i$, we obtain payoffs $\boldsymbol{G}_i'$ of node i. The payoffs $\boldsymbol{G}_i'$ implies the hidden adjacent relationships between node i and N_i other nodes because node i gains payoffs merely from its neighbors.

Most real-world networks are characterized by natural sparsity and the adjacency vector $\boldsymbol{A}_i$ of node i is sparse, which refers to vector $\boldsymbol{A}_i$ has only a few nonzero elements (i.e. $a_{ij} = 1$). Noting that the value of each element in node i's priori adjacency vector $\boldsymbol{A}_{\boldsymbol{\Gamma}_i^K}$ is 1, vector $\boldsymbol{A}_i'$ would still be sparse because the number of zero elements has not been changed but the number of nonzero elements has decreased when we remove the priori adjacency vector $\boldsymbol{A}_{\boldsymbol{\Gamma}_i^K}$ from vector $\boldsymbol{A}_i$. The sparsity of $\boldsymbol{A}_i'$ makes EEM applicable. Initially, the nodes' strategies and payoffs are recorded in discrete round $t_1, t_2, \ldots, t_M$. Since new payoffs are obtained from the game between node i and N_i nodes, we can build a model as **Eq. 4**. The sparse vector $\boldsymbol{A}_i'$ then can be reconstructed by solving the following convex optimization problem [57, 58]:

$$\begin{aligned} &\min \|\boldsymbol{A}_i'\|_1 \\ &\text{s. t. } \boldsymbol{G}_i' = \boldsymbol{\Phi}_i' \cdot \boldsymbol{A}_i', \end{aligned} \tag{4}$$

where $\|\boldsymbol{A}_i'\|_1 = \sum_{j=1}^{N_i} |a_{ij}'|$ is the L_1 norm of vector $\boldsymbol{A}_i'$. The available dynamical payoffs of node i can be expressed by $\boldsymbol{G}_i' = (G_i'(t_1), G_i'(t_2), \ldots, G_i'(t_M))^T$. The payoffs of node i obtained from the corresponding nodes in limited rounds can be expressed by an $M \times N_i$ sensing matrix $\boldsymbol{\Phi}_i'$ ($M \ll N_i$). In particular, we write $\boldsymbol{\Phi}_i' =$

$$\begin{pmatrix} F_{i1}(t_1) & F_{i,2}(t_1) & \ldots & F_{i,N_i}(t_1) \\ F_{i1}(t_2) & F_{i,2}(t_2) & \ldots & F_{i,N_i}(t_2) \\ \vdots & \vdots & \cdots & \vdots \\ F_{i1}(t_M) & F_{i,2}(t_M) & \ldots & F_{i,N_i}(t_M) \end{pmatrix}.$$

TABLE 2 | The statistical properties of four empirical networks.

Networks	N	$\|E\|$	⟨k⟩	⟨r⟩	⟨C⟩	⟨D⟩
FWMW [59]	97	1,446	29.81144	−0.1506	0.4683	1.6929
FWFW [59]	128	2075	32.4219	−0.1117	0.3346	1.7763
Jazz musicians [60]	198	2,742	27.6970	0.0202	0.6175	2.2530
C. elegans [26]	297	2,148	14.4646	−0.1632	0.2924	2.4553

The elements in matrix $\boldsymbol{\Phi}_i'$ could be calculated using the formula shown in **Eq. 2**. According to **Eq. 4**, we could obtain adjacency vector $\boldsymbol{A}_i' = (a_{i1}', a_{i2}', \ldots, a_{iN_i}')^T$ by solving the convex optimization problem. We could obtain the complete adjacency vector $\boldsymbol{A}_i = (a_{i1}, a_{i2}, \ldots, a_{iN})^T$ by combining the reconstructed vector $\boldsymbol{A}_i'$ and the priori neighbor set $\boldsymbol{A}_{\boldsymbol{\Gamma}_i^K}$ of node i. In a similar fashion, the neighbor-connection vectors of all the other nodes can be obtained, yielding the network's adjacency matrix $\mathbf{A} = (\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_N)$.

3 EXPERIMENTAL RESULTS

3.1 Datasets

In order to understanding the performance of EEM in reconstructing the synthetic networks, the experiments are conducted in four types of networks. The basic statistical properties of the synthetic networks are presented in **Table 1**. N and $|\boldsymbol{E}|$ are the number of nodes and links. $\langle k \rangle$ is the mean degree, $\langle r \rangle$ is the mean assortative coefficient, $\langle C \rangle$ is the mean clustering coefficient, and $\langle D \rangle$ is the mean shortest distance. Here, we use abbreviation WS, RM, RG and AP to represent small-world networks, random networks, regular networks and Apollonian networks, respectively.

We assume that the strategies and payoffs of each node in a certain round t is one piece of time-series information. In the experiments, we use M pieces of accessible time-series information obtained from discrete round t_1 to round t_M to reconstruct different networks. In this paper, we set N, namely the number of nodes in the network, as the maximum value of M. Then we use an index of information sufficiency $\eta (\eta \equiv M/N)$ to represent the size of the time-series information used in the network reconstruction. Intuitively, the time-series information is sufficient when the pieces of the accessible time-series information $M = N$, while the time-series information is insufficient when $0 < M < N$. Correspondingly, the accessible time-series information is sufficient when the index of information sufficiency $\eta = 1$ and the accessible time-series information is insufficient when $0 < \eta < 1$. The reconstruction models are also applied to reconstruct networks with different priori information of the structure, measured by a probability $P_s (0 \leq P_s \leq 1)$.

In addition, the performance of EEM is also evaluated in reconstructing the empirical networks. **Table 2** shows the basic statistical properties of all four networks. These networks are chosen because they are characterized by large clustering coefficient and short distance.

3.2 Metrics

To test the EEM's accuracy, the original existent link set, $\boldsymbol{E}$, are randomly divided into two parts: the priori set $\boldsymbol{E}^T$, and the probe

set $\boldsymbol{E}^P$. Clearly, $\boldsymbol{E} = \boldsymbol{E}^T \cup \boldsymbol{E}^P$ and $\boldsymbol{E}^T \cap \boldsymbol{E}^P = \varnothing$. In this paper, the priori set always contains P_s of links, and the remaining $1 - P_s$ of links constitute the probe set. We apply four standard indices to quantify the reconstruction accuracy: the success rates of existent links *SR*, the success rates of nonexistent links *SN* [24], precision *PRE* [61, 62] and the area under the receiver operating characteristic curve *AUC* [63] are applied. In addition, we apply local indices of success rates in the experiments.

Both the success rates of existent links *SR* and the success rates of nonexistent links *SN* estimate the similarity of the reconstructed networks and the original networks. The success rates of existent links *SR* denotes the ratio of the number of links reconstructed by the reconstruction models to the number of real existent links in the network. The success rates of nonexistent links *SN* denotes the ratio of the number of nonexistent links distinguished by the reconstruction models to the number of real nonexistent links in the network. We obtain

$$SR = \frac{1}{N}\sum_{i=1}^{N}\frac{|\boldsymbol{\Gamma}_{io} \cap \boldsymbol{\Gamma}_{ir}|}{|\boldsymbol{\Gamma}_{io}|} \tag{5}$$

$$\frac{SN = \frac{1}{N}\sum_{i=1}^{N}|\bar{\boldsymbol{\Gamma}}_{io} \cap \bar{\boldsymbol{\Gamma}}_{ir}|}{|\bar{\boldsymbol{\Gamma}}_{io}|} \tag{6}$$

where $\boldsymbol{\Gamma}_{io}$ and $\boldsymbol{\Gamma}_{ir}$ denote real neighbor set of node i and neighbor set of node i reconstructed by the reconstruction models, respectively. $|\cdot|$ denotes the number of elements in a set $\cdot$. $\bar{\boldsymbol{\Gamma}}_{io}$ and $\bar{\boldsymbol{\Gamma}}_{ir}$ are the supplementary set of set $\boldsymbol{\Gamma}_{io}$ and $\boldsymbol{\Gamma}_{ir}$. Each node in set $\bar{\boldsymbol{\Gamma}}_{io}$ is not adjacent to node i. Correspondingly, each node in reconstructed set $\bar{\boldsymbol{\Gamma}}_{ir}$ is not adjacent to node i. A successful reconstruction is achieved when the success rates of existent links SR ($0 \le SR \le 1$) and the success rates of nonexistent links SN($0 \le SN \le 1$) are close to the value of 1.

Precision *PRE* is defined as the ratio of existent links reconstructed by models to the number of the whole unknown existent links. In our case, to calculate precision we need to rank all the unknown links in decreasing order according to existent possibilities computed by reconstruction models. Then we focus on the top-L (here $L = |\boldsymbol{E}^P|$) links. If there are H links successfully reconstructed, then

$$PRE = \frac{H}{L} \tag{7}$$

The area under the receiver operating characteristic curve *AUC* evaluates the reconstruction models' performance according to the whole unknown link list. Provided the existent possibility of all unknown links, *AUC* can be interpreted as the probability that a randomly chosen unknown existent link is given a higher existent possibility than a randomly chosen nonexistent link. In the implementation, the value of *AUC* is calculated with a function perfcurve by Matlab.

Clearly, a higher value of the success rates of existent links *SR*, the success rates of nonexistent links *SN*, precision *PRE* or the area under the receiver operating characteristic curve *AUC* means a higher reconstruction accuracy. We conduct 50 times independent simulation for averaging the indices of reconstruction accuracy as the mean success rates of existent links $\langle SR\rangle$, the mean success rates of nonexistent links $\langle SN\rangle$, the mean precision $\langle PRE\rangle$ and the mean area under the receiver operating characteristic curve $\langle AUC\rangle$.

To understand the reconstruction performance of EEM when reconstructing local structure of the network divide the structure of each type of network into separately local structure. Supposing that the roles of nodes in the network are leaders, brokers and peripheral executors. We denote leaders are nodes with small degrees and the number of leaders in each type of network is 6. In addition, the subnetwork composed of leaders is a connected subgraph. Then brokers are nodes which are connected with leaders, and the residual nodes are peripheral executors. The sets of leaders, brokers and peripheral executors are not overlapped. We use letters L, B and P to represent the adjacent relationships between leaders, the adjacent relationships between leaders and brokers, and the adjacent relationships among peripheral executors and brokers, respectively. Then, we could obtain the success rates of existent links of each local structure normalized by the number of real existent links $|\boldsymbol{\Gamma}_{io}|$ of the network.

$$SR_{Lr} = \frac{1}{N}\sum_{i=1}^{N}\frac{|\boldsymbol{\Gamma}_{Lio} \cap \boldsymbol{\Gamma}_{Lir}|}{|\boldsymbol{\Gamma}_{io}|} \tag{8}$$

$$SR_{Br} = \frac{1}{N}\sum_{i=1}^{N}\frac{|\boldsymbol{\Gamma}_{Bio} \cap \boldsymbol{\Gamma}_{Bir}|}{|\boldsymbol{\Gamma}_{io}|} \tag{9}$$

$$SR_{Pr} = \frac{1}{N}\sum_{i=1}^{N}\frac{|\boldsymbol{\Gamma}_{Pio} \cap \boldsymbol{\Gamma}_{Pir}|}{|\boldsymbol{\Gamma}_{io}|} \tag{10}$$

The sum of three local success rates of existent links is equal the global success rates of existent links.

$$SR = SR_{Lr} + SR_{Br} + SR_{Pr} \tag{11}$$

Correspondingly, the maximum of three local success rates of existent links would be

$$SR_{Lo} = \frac{1}{N}\sum_{i=1}^{N}\frac{|\boldsymbol{\Gamma}_{Lio}|}{|\boldsymbol{\Gamma}_{io}|} \tag{12}$$

$$SR_{Bo} = \frac{1}{N}\sum_{i=1}^{N}\frac{|\boldsymbol{\Gamma}_{Bio}|}{|\boldsymbol{\Gamma}_{io}|} \tag{13}$$

$$SR_{Po} = \frac{1}{N}\sum_{i=1}^{N}\frac{|\boldsymbol{\Gamma}_{Pio}|}{|\boldsymbol{\Gamma}_{io}|} \tag{14}$$

when the original network is successfully reconstructed. To quantify the success rates of three different local structure, we define local indices of success rates as follows:

$$APP_{SRL} = \frac{SR_{Lr}}{SR_{Lo}} \tag{15}$$

$$APP_{SRB} = \frac{SR_{Br}}{SR_{Bo}} \tag{16}$$

$$APP_{SRP} = \frac{SR_{Pr}}{SR_{Po}} \tag{17}$$

Similarly, a higher value of local index of success rates APP_{SRL}, APP_{SRB}, or APP_{SRP} means a higher reconstruction accuracy. We

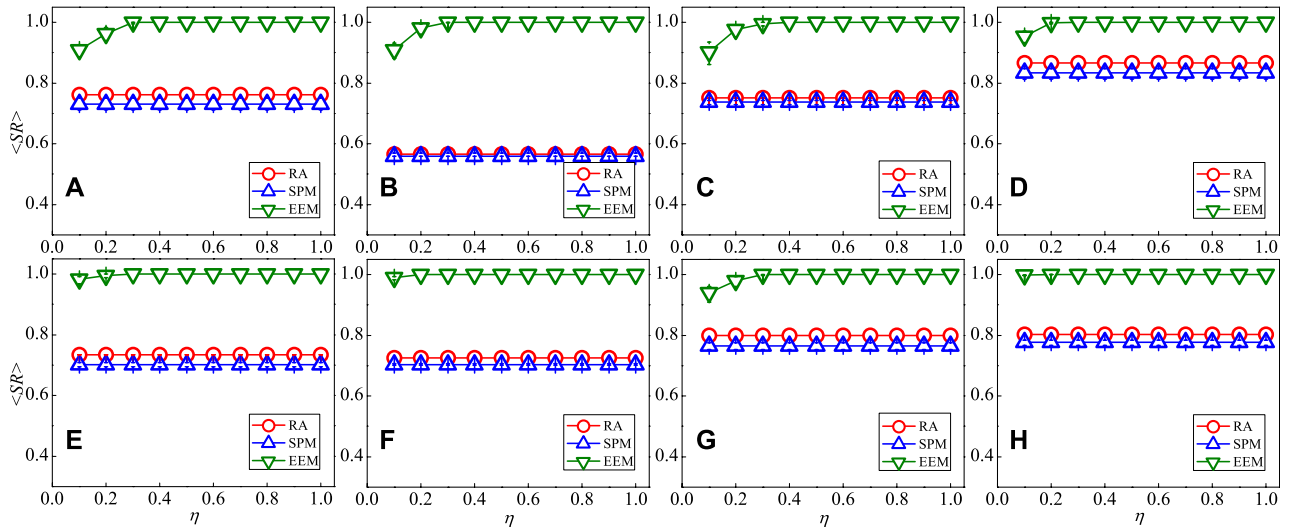


FIGURE 2 | (Color Online) The mean success rates of existent links $\langle SR \rangle$ of reconstructing four types of networks: **(A)** small-world network with 120 nodes, **(B)** random network with 120 nodes, **(C)** regular network with 120 nodes, **(D)** Apollonian network with 124 nodes, **(E)** small-world network with 250 nodes, **(F)** random network with 250 nodes, **(G)** regular network with 250 nodes, **(H)** Apollonian network with 367 nodes, hosting a PDG dynamical process. The lines with circle, triangle and inverted triangle symbols are the mean success rates of existent links $\langle SR \rangle$ obtained by RA, SPM and EEM based on 90% priori structure information. The mean reconstruction accuracy indices are achieved by averaging over 50 independent experimental results. For each experiment, measurements are randomly picked from a time series of temporary evolution. The index of information sufficiency rate η indicates the amount of the available time-series information used in the reconstruction. The payoff parameter for the PDG is b = 1.2.

conduct 50 times independent simulation for averaging the indices of success rates $\langle APP_{SRL} \rangle$, $\langle APP_{SRB} \rangle$ and $\langle APP_{SRP} \rangle$.

3.3 Experimental Results on Synthetic and Empirical Networks

In order to understand the performance of EEM, four types of synthetic networks hosting a PDG dynamical process are considered in our paper. **Figure 2A** depicts the index of reconstruction accuracy for a synthetic small-world network, measured by the mean success rates of existent links $\langle SR \rangle$, based on 90% priori structure information. The mean success rates of existent links $\langle SR \rangle$ increases monotonously when the index of information sufficiency η is varying from 0.1 to 0.4. Especially the mean reconstruction accuracy $\langle SR \rangle$ reaches the maximum value of 1 when the index of information sufficiency η = 0.4. The increment rate of the mean reconstruction accuracy $\langle SR \rangle$ is 9.97%. Then the mean reconstruction accuracy $\langle SR \rangle$ keeps the value of 1 when the index of information sufficiency η is larger than 0.4. As shown in **Figures 2B–H**, the mean reconstruction accuracy $\langle SR \rangle$ increases monotonously when the index of information sufficiency η is less than 0.4. In addition, the mean reconstruction accuracy $\langle SR \rangle$ reaches 1 for the different types of synthetic networks when the index of information sufficiency η exceeds 0.4.

Moreover, we compare the experimental results between EEM and two link prediction models which are the resource allocation (RA) and the structural perturbation method (SPM). **Figures 2A–H** show that when the index of information sufficiency η is low (i.e., η = 0.1), the mean success rates of existent links $\langle SR \rangle$ obtained by EEM on small-world networks, random networks, regular networks and Apollonian networks reaches 0.9093, 0.9085, 0.9021, 0.9361, 0.9823, 0.9897, 0.9402 and 0.9982, respectively. Compared with RA and SPM, EEM's mean success rates of existent links $\langle SR \rangle$ are higher, which is improved by at least 8.07 and 12.22% on the networks with 120–124 nodes, respectively. Compared with RA and SPM, EEM's mean success rates of existent links $\langle SR \rangle$ are higher, which is improved by at least 17.53 and 22.81% on the networks with 250–367 nodes, respectively. The experimental results of **Figure 2** indicate that EEM has a well tradeoff that provides high quality reconstruction accuracy while requiring less time-series information.

Intuitively, a network's structure would be accurately reconstructed when more priori information about the structure of the network are presented. **Figure 3** shows the dependence of the values of $\langle SR \rangle$ on probability P_s, the priori information of the structure, where we see that, in the cases of lower index of information sufficiency η ($\eta \leq 0.4$), $\langle SR \rangle$ increases monotonously when the probability P_s increases. On the other hand, the mean success rates of existent links $\langle SR \rangle$ approaches the maximum value of 1 when the index of information sufficiency η is larger than 0.4. In terms of the probability P_s, the highest performance is achieved for the highest P_s. The intuitive reason for the relatively superior performance with the four synthetic networks lies in the sufficiency of the available information of the networks' structure.

In the following, we verify the performance of EEM in local structure of the networks. We divide the structure of each type of network into three separately local structure with subscript L, B, P

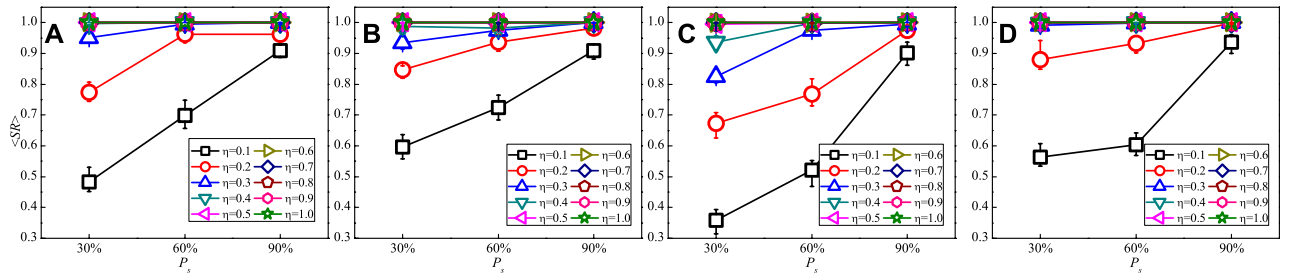


FIGURE 3 | (Color Online) The mean success rates of existent links $\langle SR \rangle$ of reconstructing four types of networks: **(A)** small-world network with 120 nodes, **(B)** random network with 120 nodes, **(C)** regular network with 120 nodes, **(D)** Apollonian network with 124 nodes, hosting a PDG dynamical process. The lines with different symbols are the mean success rates of existent links $\langle SR \rangle$ obtained by EEM when the index of information sufficiency rate η catches different values. The mean reconstruction accuracy indices are achieved by averaging over 50 independent experimental results. For each experiment, measurements are randomly picked from a time series of temporary evolution. The priori information of the structure, measured by a probability P_s, indicates the amount of available priori information of the structure used in the reconstruction. The payoff parameter for the PDG is b = 1.2.

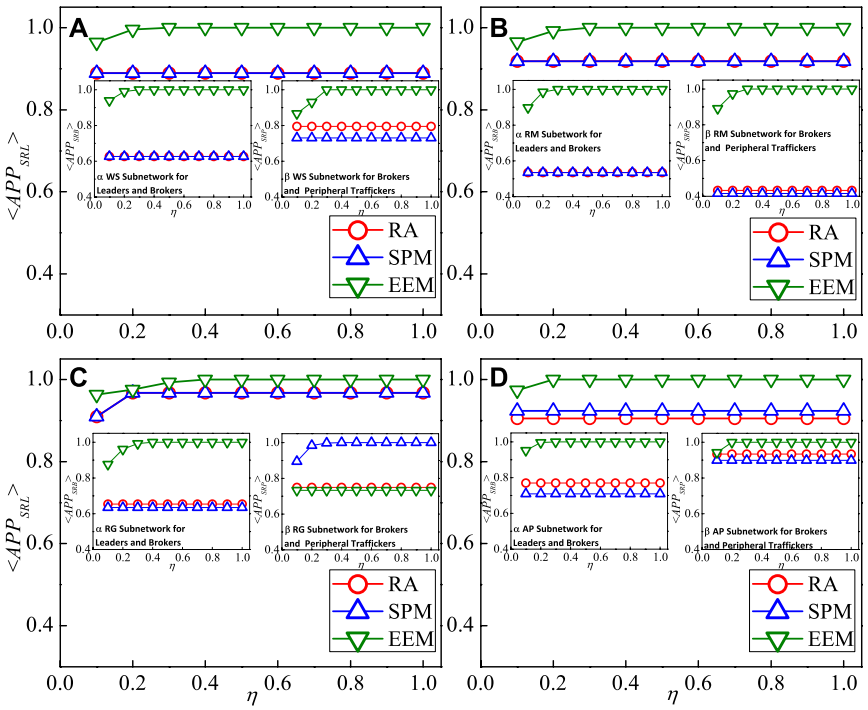


FIGURE 4 | (Color Online) The mean local indices of success rates $\langle APP_{SRL} \rangle$, $\langle APP_{SRB} \rangle$, and $\langle APP_{SRP} \rangle$ of reconstructing four types of networks: **(A)** small-world network with 120 nodes, **(B)** random network with 120 nodes, **(C)** regular network with 120 nodes and **(D)** Apollonian network with 124 nodes, hosting a PDG dynamical process. The lines with circle, triangle and inverted triangle symbols are the mean local indices of success rates $\langle APP_{SRL} \rangle$, $\langle APP_{SRB} \rangle$, and $\langle APP_{SRP} \rangle$ obtained by RA, SPM and EEM based on 90% priori structure information. The mean reconstruction accuracy indices are achieved by averaging over 50 independent experimental results. For each experiment, measurements are randomly picked from a time series of temporary evolution. The index of information sufficiency rate η indicates the amount of the available time-series information used in the reconstruction. The payoff parameter for the PDG is b = 1.2.

for them. **Figure 4A** depicts reconstruction success rate of a small-world network, measured by the mean local index of success rates $\langle APP_{SRL} \rangle$, $\langle APP_{SRB} \rangle$, and $\langle APP_{SRP} \rangle$, based on 90% priori structure information.

As illustrated in the main graph in **Figure 4A**, the mean local index of success rates $\langle APP_{SRL} \rangle$ obtained by EEM is higher than RA or SPM. Especially the mean local index of success rates $\langle APP_{SRL} \rangle$ obtained by EEM reaches 96.41% when the index of information sufficiency η = 0.1, while the mean local index of success rates $\langle APP_{SRL} \rangle$ obtained by RA and SPM are both 88.95%. The mean local index of success rates $\langle APP_{SRB} \rangle$ and $\langle APP_{SRP} \rangle$ obtained by EEM are 93.95 and 86.68% when the index of information sufficiency η = 0.1, as shown in the subgraph (α)-(β) in **Figure 4A**. Correspondingly, the mean local index of

success rates $\langle APP_{SRB}\rangle$ and $\langle APP_{SRP}\rangle$ obtained by RA are 62.67 and 79.51%, $\langle APP_{SRB}\rangle$ and $\langle APP_{SRP}\rangle$ obtained by SPM are 62.67 and 73.06%. The similar experimental results could also be found in the cases of random network, regular network and Apollonian network in **Figures 4B–D**, which indicate that EEM can achieve higher reconstruction accuracy with low time-series information than RA or SPM.

The underlying reason that EEM could obtain higher reconstruction accuracy than RA or SPM might be twofold. Firstly, EEM is applicable to reconstruct networks with sparse connective relationships because Wang et al. developed a paradigm [19, 24, 25] to address the network reconstruction problems and Candès et al. provided the theoretical framework for this paradigm [57, 58]. Both EEM and two link prediction models utilize the identical priori structure information of the network to obtain direct information of the unknown structure. In addition, EEM bridges the relationships between the nodes' payoffs and strategies by virtue of time-series information because the payoffs can merely be obtained from each node's neighbors. Then EEM could extract indirect information of the unknown structure from the above relationships which strengthens the reliability of the experimental results. RA and SPM could also extract valuable indirect information of the unknown structure, but the valuable information still originates from the priori structure information of the network due to lack of a universal theoretical framework.

Secondly, both the reconstruction accuracy of the local structure and the reconstruction accuracy of the global structure obtained by EEM highly consist. As illustrated in **Figure 4**, the absolute error between three mean local index of success rates $\langle APP_{SRL}\rangle$, $\langle APP_{SRB}\rangle$ and $\langle APP_{SRP}\rangle$ obtained by EEM on each network is less than 0.1, which indicates that the reconstruction accuracy on three separate local structure obtained by EEM is almost the same. Consequently, the global reconstruction accuracy and the local reconstruction accuracy highly consist because the global reconstruction accuracy is the linear combination of three mean local index of success rates as: $\langle SR\rangle = SR_{Lo}\cdot\langle APP_{SRL}\rangle + SR_{Bo}\cdot\langle APP_{SRB}\rangle + SR_{Po}\cdot\langle APP_{SRP}\rangle$, where SR_{Lo}, SR_{Bo} and SR_{Po} are constant for each network. The high reconstruction accuracy of three separately local structure contribute to a high reconstruction accuracy of the global structure. We also observe that the reconstruction accuracy on three separate local structure obtained by RA or SPM fluctuates. Especially in the reconstruction experiments on synthetic random networks, the maximum absolute error between three mean local index of success rates obtained by RA or SPM reaches 0.3837. The experimental results indicate that the reconstruction accuracy obtained by RA and SPM is largely dependent on the priori structure information of the network. The reconstruction accuracy of RA or SPM would be high when the local priori structure is consistent with the global structure, and the reconstruction accuracy would be low otherwise.

Finally, we test the results for four empirical networks. As shown in **Table 3**, we reconstruct the network structure by EEM, RA and SPM with 90% priori structure information. The empirical results indicate that four indices of reconstruction accuracy obtained by EEM are higher than RA and SPM for four empirical networks when the index of information sufficiency rate $\eta = 0.1$. Four indices of reconstruction accuracy obtained by EEM are higher than RA and SPM. Compared with RA, EEM's reconstruction accuracy, measured by the mean success rates of existent links $\langle SR\rangle$, which are improved by 355.54, 456.38, 96.37 and 64.11%, corresponding to FWMW, FWFW, Jazz musicians, Neural network of *C. elegans*. Compared with SPM, EEM's reconstruction accuracy, measured by the mean success rates of existent links $\langle SR\rangle$, which are improved by 355.54, 154.07, 47.81 and 69.38%,corresponding to FWMW, FWFW, Jazz musicians, Neural network of *C. elegans*. Empirical results indicate that the empirical networks reconstructed by EEM are closer to the original networks than those reconstructed by RA and SPM.

TABLE 3 | The value of four indices of reconstruction accuracy for four empirical networks.

Network	Accuracy	RA	SPM	EEM	
				η = 0.1	η = 0.6
FWMW	*SR*	0.1833	0.1833	0.8351	0.9996
	SN	0.0016	0.0016	0.9577	0.9996
	PRE	0	0.0003	0.5730	0.9989
	AUC	0.6786	0.6968	0.8836	1
FWFW	*SR*	0.1575	0.3450	0.8765	1
	SN	0.9742	0.9712	0.9567	0.9999
	PRE	0.0385	0.2043	0.6143	0.9999
	AUC	0.4191	0.7816	0.9375	1
Jazz musicians	*SR*	0.4488	0.5962	0.8813	1
	SN	0.9902	0.9894	0.9723	0.9999
	PRE	0.2291	0.3486	0.5544	0.9980
	AUC	0.9151	0.9085	0.9807	1
C. elegans	*SR*	0.4770	0.4621	0.7828	0.9998
	SN	0.9927	0.9948	0.9965	0.9993
	PRE	0.0512	0.0446	0.4834	0.9539
	AUC	0.7817	0.7598	0.9243	0.9999

3.4 CONCLUSION

In summary, we have investigated the performance of EEM for reconstructing synthetic networks, which are characterized by four types of networks as small-world networks, random networks, regular networks and Apollonian networks, based on priori structure information. The mean success rates of existent links $\langle SR\rangle$ obtained by EEM could achieve at least 0.9021 when the index of information sufficiency η is 0.1. Compared with RA and SPM, EEM has higher mean success rates of existent links $\langle SR\rangle$, which is improved by 8.07 and 12.22% on the networks with 120–124 nodes, respectively. Compared with RA and SPM, EEM has higher mean success rates of existent links $\langle SR\rangle$, which is improved by 17.53 and 22.81% on the networks with 250–367 nodes, respectively. The experimental results also indicate that separately local structure in each type of network could be accurately reconstructed by EEM. In addition, EEM's reconstruction accuracy is also evaluated on four empirical networks. Compared with RA and SPM, EEM has higher mean

success rates of existent links $\langle SR \rangle$, which is improved by 64.11 and 47.81%, respectively. The reason that EEM obtain higher reconstruction accuracy than RA or SPM might lie in that EEM could utilize time-series information to strengthen the reliability of the experimental results and EEM's capability to reconstruct the local structure and the global structure highly consist. The evaluation of EEM on both synthetic networks and empirical networks suggest that EEM is applicable for networks with sparsely connective relationships and it has high reconstruction accuracy by low information requirements.

Although the efficiency of EEM has been measured in reconstructing network's structure with both synthetic networks and empirical networks, there are still a lot of questions to be considered further. For example, the results show that EEM can give remarkably higher reconstruction accuracy on a network hosing a PDG dynamical process, but the performance of EEM has not been validated under another dynamical process. Although EEM could also be extended to cases with large-scale network, the computing time might increase exponentially. In addition, EEM's capability to identify spurious links has not been explored. Noting that EEM can well capture the adjacent relationships from limited information and thus give more accurate reconstruction, such features make EEM appealing to reconstructing general networks with extremely low data requirement. Despite underlying challenges, we will make attempt to continue our research referring to the problems of network reconstruction.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

J-QF provided this topic and wrote the paper. QG, KY and J-GL guided, discussed and modified the manuscript. All authors contributed to manuscript and approved the submission version.

FUNDING

This work is supported by the National Natural Science Foundation of China (Grant Nos. 71771152 and 61773248), the National Social Science Fund of China (No.16BJY158), the Major Program of National Fund of Philosophy and Social Science of China (Nos. 20ZDA060 and 18ZDA088), and the Scientific Research Project of Shanghai Science and Technology Committee (Grant No. 19511102202).

ACKNOWLEDGMENTS

The authors acknowledge the valuable discussion with Huan-Mei Qin, Guang Liang, Ren-De Li, Hong-Yi Ding, Shao-Yong Han.

REFERENCES

1. Liao JC, Boscolo R, Yang Y-L, Tran LM, Sabatti C, and Roychowdhury VP. Network Component Analysis: Reconstruction of Regulatory Signals in Biological Systems. *Proc Natl Acad Sci* (2003) 100:15522–7. doi:10.1073/pnas.2136632100
2. Matys V, Fricke E, Geffers R, Gößling E, Haubrock M, and Hehl R. TRANSFAC(R): Transcriptional Regulation, from Patterns to Profiles. *Nucleic Acids Res* (2003) 31:374–8. doi:10.1093/nar/gkg108
3. Keseler IM, Collado-Vides J, Gama-Castro S, Ingraham J, Paley S, and Paulsen IT. Ecocyc: A Comprehensive Database Resource for Escherichia Coli. *Nucleic Acids Res* (2004) 33:D334–D337. doi:10.1093/nar/gki108
4. Lee TI, Rinaldi NJ, Robert F, Odom DT, Bar-Joseph Z, and Gerber GK. Transcriptional Regulatory Networks in Saccharomyces Cerevisiae. *Science* (2002) 298:799–804. doi:10.1126/science.1075090
5. Dong GG, Wang F, Shekhtmane LM, Danziger MM, Fan JF, and Du RJ. Optimal Resilience of Modular Interacting Networks. *Proc Natl Acad Sci USA*. (2021) 118:e1922831118. doi:10.1073/pnas.1922831118
6. Bussemaker HJ, Li H, and Siggia ED. Building a Dictionary for Genomes: Identification of Presumptive Regulatory Sites by Statistical Analysis. *Proc Natl Acad Sci* (2000) 97:10096–100. doi:10.1073/pnas.180265397
7. Bussemaker HJ, Li H, and Siggia ED. Regulatory Element Detection Using Correlation With Expression. *Nat Genet* (2001) 27:167–71. doi:10.1038/84792
8. Chang C, Ding Z, Hung YS, and Fung PCW. Fast Network Component Analysis (Fastnca) for Gene Regulatory Network Reconstruction From Microarray Data. *Bioinformatics* (2008) 24:1349–58. doi:10.1093/bioinformatics/btn131
9. Cugueró-Escofet MÀ, Quevedo J, Alippi C, Roveri M, Puig V, and García D. Model- vs. Data-Based Approaches Applied to Fault Diagnosis in Potable Water Supply Networks. *J Hydroinformatics* (2016) 18:831–50. doi:10.2166/hydro.2016.218
10. Lü L, and Zhou T. Link Prediction in Complex Networks: A Survey. *Physica A: Stat Mech Its Appl* (2011) 390:1150–70. doi:10.1016/j.physa.2010.11.027
11. Clauset A, Moore C, and Newman MEJ. Hierarchical Structure and the Prediction of Missing Links in Networks. *Nature* (2008) 453:98–101. doi:10.1038/nature06830
12. Zhou T, Lü L, and Zhang Y-C. Predicting Missing Links via Local Information. *Eur Phys J B* (2009) 71:623–30. doi:10.1140/epjb/e2009-00335-8
13. Lü L, Jin C-H, and Zhou T. Similarity Index Based on Local Paths for Link Prediction of Complex Networks. *Phys Rev E* (2009) 80:046122. doi:10.1103/PhysRevE.80.046122
14. Liben-Nowell D, and Kleinberg J. The Link-Prediction Problem for Social Networks. *J Am Soc Inf Sci* (2007) 58:1019–31. doi:10.1002/asi.20591
15. Guimerà R, and Sales-Pardo M. Missing and Spurious Interactions and the Reconstruction of Complex Networks. *Proc Natl Acad Sci* (2009) 106:22073–8. doi:10.1073/pnas.0908366106
16. Lü L, Pan L, Zhou T, Zhang Y-C, and Stanley HE. Toward Link Predictability of Complex Networks. *Proc Natl Acad Sci USA* (2015) 112:2325–30. doi:10.1073/pnas.1424644112
17. Sun J, Feng L, Xie J, Ma X, Wang D, and Hu Y. Revealing the Predictability of Intrinsic Structure in Complex Networks. *Nat Commun* (2020) 11:1–10. doi:10.1038/s41467-020-14418-6
18. Zhang H-F, and Wang W-X. Complex System Reconstruction. *Acta Physica Sinica* (2020) 69:088906. doi:10.7498/aps.69.20200001
19. Wang W-X, Lai Y-C, and Grebogi C. Data Based Identification and Prediction of Nonlinear and Complex Dynamical Systems. *Phys Rep* (2016) 644:1–76. doi:10.1016/j.physrep.2016.06.004
20. Xu M, Xu C-Y, Wang H, Li Y-K, Hu J-B, and Cao K-F. Global and Partitioned Reconstructions of Undirected Complex Networks. *Eur Phys J B* (2016) 89:1–6. doi:10.1140/epjb/e2016-60956-2

21. Barranca VJ, and Zhou D. Compressive Sensing Inference of Neuronal Network Connectivity in Balanced Neuronal Dynamics. *Front Neurosci* (2019) 13:1101. doi:10.3389/fnins.2019.01101
22. Li R-D, Guo Q, Ma H-T, and Liu J-G. Network Reconstruction of Social Networks Based on the Public Information. *Chaos* (2021) 31:033123. doi:10.1063/5.0038816
23. Shen Z, Wang W-X, Fan Y, Di Z, and Lai Y-C. Reconstructing Propagation Networks With Natural Diversity and Identifying Hidden Sources. *Nat Commun* (2014) 5:1–10. doi:10.1038/ncomms5323
24. Wang W-X, Lai Y-C, Grebogi C, and Ye J. Network Reconstruction Based on Evolutionary-Game Data via Compressive Sensing. *Phys Rev X* (2011) 1: 021021. doi:10.1103/PhysRevX.1.021021
25. Ma L, Han X, Shen Z, Wang W-X, and Di Z. Efficient Reconstruction of Heterogeneous Networks From Time Series via Compressed Sensing. *PLoS One* (2015) 10:e0142837. doi:10.1371/journal.pone.0142837
26. Watts DJ, and Strogatz SH. Collective Dynamics of 'Small-World' Networks. *Nature* (1998) 393:440–2. doi:10.1038/30918
27. Amaral LAN, Scala A, Barthélémy M, and Stanley HE. Classes of Small-World Networks. *Proc Natl Acad Sci* (2000) 97:11149–52. doi:10.1073/pnas.200327197
28. Ravasz E, and Barabási A-L. Hierarchical Organization in Complex Networks. *Phys Rev E* (2003) 67. doi:10.1103/PhysRevE.67.026112
29. Albert R, Albert I, and Nakarado GL. Structural Vulnerability of the North American Power Grid. *Phys Rev E Stat Nonlin Soft Matter Phys* (2004) 69: 025103. doi:10.1103/PhysRevE.69.025103
30. Crucitti P, Latora V, and Marchiori M. A Topological Analysis of the Italian Electric Power Grid. *Physica A: Stat Mech Its Appl* (2004) 338:92–7. doi:10.1016/j.physa.2004.02.029
31. Bright D, Koskinen J, and Malm A. Illicit Network Dynamics: The Formation and Evolution of a Drug Trafficking Network. *J Quant Criminol* (2019) 35: 237–58. doi:10.1007/s10940-018-9379-8
32. Barrat A, Barthélemy M, Pastor-Satorras R, and Vespignani A. The Architecture of Complex Weighted Networks. *Proc Natl Acad Sci* (2004) 101:3747–52. doi:10.1073/pnas.0400087101
33. Verma T, Araújo NAM, Nagler J, Andrade JS, Jr, and Herrmann HJ. Model for the Growth of the World Airline Network. *Int J Mod Phys C* (2016) 27: 1650141. doi:10.1142/S0129183116501412
34. Soares DJB, Andrade JS, Jr, Herrmann HJ, and da Silva LR. Three-Dimensional Apollonian Networks. *Int J Mod Phys C* (2006) 17:1219–26. doi:10.1142/S0129183106009175
35. Andrade RFS, Andrade JS, Jr, and Herrmann HJ. Ising Model on the Apollonian Network With Node-Dependent Interactions. *Phys Rev E* (2009) 79:036105. doi:10.1103/PhysRevE.79.036105
36. Araújo NA, Andrade RFS, and Herrmann HJ. Q-State Potts Model on the Apollonian Network. *Phys Rev E* (2010) 82:046109. doi:10.1103/physreve.82.046109
37. Dong G, Wang F, Shekhtman LM, Danziger MM, Fan J, and Du R. Optimal Resilience of Modular Interacting Networks. *Proc Natl Acad Sci USA* (2021) 118:e1922831118. doi:10.1073/pnas.1922831118
38. Dong G, Fan J, Shekhtman LM, Shai S, Du R, and Tian L. Resilience of Networks With Community Structure Behaves as if Under an External Field. *Proc Natl Acad Sci USA* (2018) 115:6911–5. doi:10.1073/pnas.1801588115
39. Gao J, Barzel B, and Barabási A-L. Universal Resilience Patterns in Complex Networks. *Nature* (2016) 530:307–12. doi:10.1038/nature16948
40. Xu X, Zhang J, and Small M. Superfamily Phenomena and Motifs of Networks Induced From Time Series. *Proc Natl Acad Sci* (2008) 105:19601–5. doi:10.1073/pnas.0806082105
41. Ren Z-M. Age Preference of Metrics for Identifying Significant Nodes in Growing Citation Networks. *Physica A: Stat Mech its Appl* (2019) 513:325–32. doi:10.1016/j.physa.2018.09.001
42. Liu J-G, Ren Z-M, and Guo Q. Ranking the Spreading Influence in Complex Networks. *Physica A: Stat Mech its Appl* (2013) 392:4154–9. doi:10.1016/j.physa.2013.04.037
43. Pan Y, Li D-H, Liu J-G, and Liang J-Z. Detecting Community Structure in Complex Networks via Node Similarity. *Physica A: Stat Mech its Appl* (2010) 389:2849–57. doi:10.1016/j.physa.2010.03.006
44. Hu Z-L, Shen Z, Tang C-B, Xie B-B, and Lu J-F. Localization of Diffusion Sources in Complex Networks With Sparse Observations. *Phys Lett A* (2018) 382:931–7. doi:10.1016/j.physleta.2018.01.037
45. Hu Z-L, Han X, Lai Y-C, and Wang W-X. Optimal Localization of Diffusion Sources in Complex Networks. *R Soc Open Sci* (2017) 4:170091. doi:10.1098/rsos.170091
46. Wang X, Su J, Ma F, and Yao B. Mean First-Passage Time on Scale-free Networks Based on Rectangle Operation. *Front Phys* (2021) 9:238. doi:10.3389/fphy.2021.675833
47. Ren Z-M, Zeng A, and Zhang Y-C. Bridging Nestedness and Economic Complexity in Multilayer World Trade Networks. *Humanit Soc Sci Commun* (2020) 7:1–8. doi:10.1057/s41599-020-00651-3
48. Buldyrev SV, Parshani R, Paul G, Stanley HE, and Havlin S. Catastrophic cascade of Failures in Interdependent Networks. *Nature* (2010) 464:1025–8. doi:10.1038/nature08932
49. Guo Q, Liang G, Fu JQ, Han JT, and Liu JG. Roles of Mixing Patterns in the Network Reconstruction. *Phys Rev E* (2016) 94:052303. doi:10.1103/PhysRevE.94.052303
50. Han X, Shen Z, Wang W-X, Lai Y-C, and Grebogi C. Reconstructing Direct and Indirect Interactions in Networked Public Goods Game. *Sci Rep* (2016) 6: 1–12. doi:10.1038/srep30241
51. Nowak MA, and May RM. Evolutionary Games and Spatial Chaos. *Nature* (1992) 359:826–9. doi:10.1038/359826a0
52. Rong Z, Yang H-X, and Wang W-X. Feedback Reciprocity Mechanism Promotes the Cooperation of Highly Clustered Scale-free Networks. *Phys Rev E* (2010) 82:047101. doi:10.1103/PhysRevE.82.047101
53. Tang Y, Jing M, and Yu Y. Conditional Neutral Reward Promotes Cooperation in the Spatial Prisoner's Dilemma Game. *Front Phys* (2021) 9:79. doi:10.3389/fphy.2021.639252
54. Szabó G, and Tőke C. Evolutionary Prisoner's Dilemma Game on a Square Lattice. *Phys Rev E* (1998) 58:69–73. doi:10.1103/PhysRevE.58.69
55. Wang W-X, Yang R, Lai Y-C, Kovanis V, and Harrison MAF. Time-Series-Based Prediction of Complex Oscillator Networks via Compressive Sensing. *Epl (Europhysics Letters)* (2011) 94:48006. doi:10.1209/0295-5075/94/48006
56. Han X, Shen Z, Wang WX, and Di Z. Robust Reconstruction of Complex Networks From Sparse Data. *Phys Rev Lett* (2015) 114:028701. doi:10.1103/PhysRevLett.114.028701
57. Candès EJ, Romberg J, and Tao T. Robust Uncertainty Principles: Exact Signal Reconstruction from Highly Incomplete Frequency Information. *IEEE Trans Inform Theor* (2006) 52:489–509. doi:10.1109/TIT.2005.862083
58. Candès EJ, and Wakin MB. An Introduction to Compressive Sampling. *IEEE Signal Process Mag* (2008) 25:21–30. doi:10.1109/msp.2007.914731
59. Baird D, Luczkovich J, and Christian RR. Assessment of Spatial and Temporal Variability in Ecosystem Attributes of the St marks National Wildlife Refuge, Apalachee bay, florida. *Estuarine, Coastal Shelf Sci* (1998) 47:329–49. doi:10.1006/ecss.1998.0360
60. Gleiser PM, and Danon L. Community Structure in Jazz. *Advs Complex Syst* (2003) 06:565–73. doi:10.1142/S0219525903001067
61. Zhou T, Ren J, Medo M, and Zhang YC. Bipartite Network Projection and Personal Recommendation. *Phys Rev E Stat Nonlin Soft Matter Phys* (2007) 76: 046115. doi:10.1103/PhysRevE.76.046115
62. Liu JG, Shi K, and Guo Q. Solving the Accuracy-Diversity Dilemma via Directed Random Walks. *Phys Rev E* (2012) 85:016118. doi:10.1103/PhysRevE.85.016118
63. Hanley JA, and McNeil BJ. The Meaning and Use of the Area under a Receiver Operating Characteristic (Roc) Curve. *Radiology* (1982) 143:29–36. doi:10.1148/radiology.143.1.7063747

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

frontiers in Physics

ORIGINAL RESEARCH
published: 09 September 2021
doi: 10.3389/fphy.2021.714910

Similarity Analysis of Alarm Sequences by a Shuffling Method

Yifan Lin[1], *Shengfeng Wang*[2]*, *Ye Wu*[3] *and Jinghua Xiao*[1]*

[1]School of Science, Beijing University of Posts and Telecommunications, Beijing, China, [2]School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China, [3]School of Journalism and Communication, Beijing Normal University, Beijing, China

Modern telecommunication systems produce large amounts of alarm messages, and alarm management is vital for telecommunication systems' high-quality performance. Building functional networks by observing the pair similarity between time series is a useful way to filter and reduce alarm messages. Because of the coexistence of positive and negative correlations among telecommunication devices, most of the similarity measures have troubles in computing the complex correlations. In this paper, we propose an index of measuring how much two-alarm series deviate from the uncorrelated situation to detect the correlation of both sides. Synthetic sequences verify our method. Furthermore, we apply our method to analyze telecommunication devices' alarm correlation in a province of China. Our index of pair similarities is capable of measuring other discrete event data.

Keywords: telecommunication alarm, similarity measure, alarm correlation network, event relationship network, time series

OPEN ACCESS

Edited by:
Gaogao Dong,
Jiangsu University, China

Reviewed by:
Jianguo Liu,
Shanghai University of Finance and Economics, China
Xiao-Pu Han,
Hangzhou Normal University, China
André L. M. Vilela,
Universidade de Pernambuco, Brazil

***Correspondence:**
Shengfeng Wang
sfwang@bupt.edu.cn
Jinghua Xiao
jhxiao@bupt.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *26 May 2021*
Accepted: *19 July 2021*
Published: *09 September 2021*

Citation:
Lin Y, Wang S, Wu Y and Xiao J (2021) Similarity Analysis of Alarm Sequences by a Shuffling Method. Front. Phys. 9:714910. doi: 10.3389/fphy.2021.714910

INTRODUCTION

According to the Ministry of Industry and Information Technology of China, the total number of mobile phone users reached 1.594 billion and more than 98 percent of administrative villages had access to optical fiber and 4G in China at the end of 2020. Numerous base stations and other kinds of equipment constitute huge telecommunication networks with complicated structures. These telecommunication systems produce a large number of alarm messages every day, which pose a challenge to faults management. In the course of the managing process, various telecommunication devices may affect each other [1, 2]. To effectively manage the system, it is critical to develop strategies for correlating alarm messages by the physical connections of network elements or knowledge derived from alarm experiences.

To perform fault management under a large number of alarm messages, it is important to reduce the number of alarm messages by correlating different devices' messages. In telecommunication networks, some expert systems are implemented to filter and correlate alarms. Italy [3], first uses expert system rules to recognize alarm correlation patterns and instantiate network fault hypotheses, and then applies a heuristic search to determine the best solution among the hypotheses. ALLINK™ Operations Coordinator from NYNEX [4] uses an expert system to filter network alarms. Most of the existing expert systems are for relating fault messages, and transferring the knowledge of human experts into an automated system. Other related methodologies were proposed. The work in [5, 6] is based on a formal language representation of the communication system. A. Bouloutas in [5] focuses on identifying errors in a known protocol: it is not an alarm correlation as such. The problem considered by A. Bouloutas and S. Calo in [6] is fault localization from alarms. It is a related although different problem. Such researches do not consider the occurring time of alarms, and assume knowledge of the network topology.

With the continuous development of telecommunication systems, telecommunication networks are becoming more complex, and features such as heterogeneous devices, network structures, and technologies are coexisting and cooperating within the system. This is a problem when domain-experts build management systems for root cause analysis or event relationship networks (ERNs). Data-driven fault management may be helpful [7]. Perng [8] utilized the event history logs in shorting the ERNs design process and perfecting the quality of ERNs. Besides constructing the ERNs, one can build device-device correlation networks from alarm logs. Particularly, telecommunication devices are deployed over large geographical area, and the device-to-device networks could be useful in understanding the performance of the whole systems. Based on the discrete alarm time of devices, device-to-device networks can be constructed by correlating alarm series to form a functional network. Functional structures are of great importance in aiding understanding of the properties of various man-made and natural networks [9, 10]. Differing from physical structures, functional structures are generally built by observing the similarity between time series. Depending on the application scenario and the type of data, there are various way of computing pair similarity. Euclidean Distance is the most basic measure, when two sequences are of equal length. To measure the similarity of unequal-length time series, Dynamic Time Warping (DTW) [11] is useful, and is used in many proposed optimizations [12–14]. If two time series have similar morphology in most time periods but only have certain differences in a very short time, Euclidean Distance and DTW cannot accurately measure the similarity between them, which can be solved by Longest Common Subsequence (LCSS) [15]. However, the measures mentioned above only focus on calculating how different the two series are, and ignore the probability of them being such different. Furthermore, due to the complexity of the system, recovering alarm messages sometimes needs to check both positively and negatively correlated devices. Most of the similarity measures may encounter troubles here.

To tackle the problem above we propose an index built on measuring to what extent the two series deviate from the corresponding shuffled series, to score the pair similarity. We then construct synthetic series to verify the method. Furthermore, we apply our method to analyze the alarm correlation of telecommunication devices in a province of China. Although our method focuses on the application of the telecommunication devices' alarm series, it can also be applied to general discrete event data.

METHODS

The Definition of the Similarity Score Between Alarm Sequences

This section defines an index to score the similarity.

Firstly, let S_i be the time sequence representing the alarm timing of ith device.

$$S_i = \left\{s_1^i,\ s_2^i,\ \cdots,\ s_k^i,\ \cdots,\ s_{|S_i|}^i\right\}, \tag{1}$$

where $|S_i|$ denotes the size of S_i. Given two sequences S_A, S_B and $n = |S_A \cap S_B|$ being the number of the same timestamps between them, we calculate the possibility of two sequences still having n same timestamps when they are randomly shuffled. In detail, let $|S_A| = m_1$, $|S_B| = m_2$, and the total time duration is assumed to be D seconds. This may be illustrated by comparing our method to a textbook example in probability. In this model, D balls are numbered and put in an opaque box. Person A first picked out m_1 balls randomly and put them back after recording their numbers. Then, person B picked m_2 balls out at random and recorded the number too. The probability of n balls being picked out twice can be expressed as

$$P_n = \frac{C_{m_1}^n C_{D-m_1}^{m_2-n}}{C_D^{m_2}},\ 0 \le n \le \min\{m_1,\ m_2\}, \tag{2}$$

where $C_D^{m_2}$ is the number of possible combinations of m_2 balls that person B can pick out from the box, and $C_{m_1}^n$ and $C_{D-m_1}^{m_2-n}$ compute the number of possible combinations in which B picks n balls in common with m_1 recorded balls and $m_2 - n$ from the $D - m_1$ unrecorded balls respectively. It is obvious that $\sum_{n=0}^{\min\{m_1,\ m_2\}} P_n = 1$. **Eq. 2** computes the probability of having n timestamps in common between S_A and S_B when they are randomly shuffled.

We define the similarity index in terms of P_n. According toP_n's definition, its value would be no less than 0 and no more than 1. If a small P_n, such as less than 0.05, appears, it means that a rare event has occurred, which results from the appearance of a much larger or smaller n compared to its expectation of two uncorrelated sequences. When n is much larger than the expectation, it shows that two devices send alarm messages together more often than the random case, and vice versa. A large n means that one devices alarm may be caused by an alarm in the other, while a small n may mean that one devices alarm is caused by the normal function of the other. Both cases leads to the conclusion that devices A and B are correlated. Because a large P_n represents that the correlation between A and B has no difference from the random case, we define the index which scores the correlation of alarm sequences A and B as

$$c_{AB} = 1 - P_n, \tag{3}$$

which is symmetric, so that $c_{AB} = c_{BA}$.

Computational Processing

Large values of D, such as in several days of data, would make the similarity computation very expensive. Therefore we separated the total time duration into several windows with equal size and computed the c_{ij} of two devices within each window respectively. Then, the average value $\bar{c}_{ij}$ over each window is taken as the final similarity score that describes the degree of correlation between two devices.

Equation 2 is the probability mass function (pmf) of hypergeometric distribution. When the total seconds D is a large number, for instance, more than 10,000, it is hard to calculate the value of $C_D^{m_2}$ because the factorial of D is too large for computer to store as m_2 increases. Here, when both the value of m_1 and m_2 are more than 90, we use an

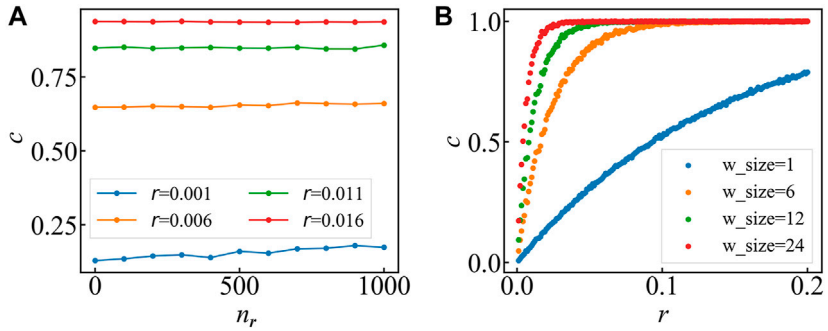


FIGURE 1 | (A) Average similarity scores at different correlation level. The sequences of device A and B are generated 10 times. The results showed in this figure are the average of 10 experiments when the window size is 24. Similarity score barely changes as n_r increases. The line moves upwards when actual correlation r increases. **(B)** Average similarity scores at different window size. The results are also the average of 10 experiments but when adding 1,000 random alarm timestamps into S_B. The range that probability score varies with r widens as the window size decreases.

approximation method proposed by Irving W. Burr [16], who found the approximation relation between the hypergeometric and Poisson distributions as

$$h(x; N, n, k) = p\left(x; \frac{kn}{N}\right)\left\{1 + \left(\frac{1}{2k} + \frac{1}{2n}\right)\left[x - \left(x - \frac{nk}{N}\right)^2\right] + O\left(\frac{1}{k^2} + \frac{1}{n^2}\right)\right\} \tag{4}$$

where $h(x; N, n, k)$ denotes hypergeometric probability for x in n given k in N and $p(x; kn/N)$ denotes Poisson probability with parameter kn/N. Thus, we use the adjustive factor below to approximate the hypergeometric probability by the Poisson probability when m_1 and m_2 are quite large.

The Verification of the Method

For verifying the validity of our method, we generated synthetic alarm series whose correlation can be set manually. Let $S_A = \{s_1^A, s_2^A, \cdots, s_k^A, \cdots, s_{|S_A|}^A\}$ be the series of device A which records 10,000 alarms within 58 days. Assuming that the probability of device B reporting an alarm message when device A reports is r, indicating the actual alarm correlation between two devices. We also add n_r random timestamps, which represent the random alarming of device B itself or correlating with other devices, into S_B to see if the score calculated by the method changes as the number of timestamps in S_B changes. **Figure 1A** shows the tendency of average similarity score with n_r under different correlation levels in 10 experiments. In the figure, similarity score barely changes as n_r increases, which means the proposed method is robust when the number of alarms changes. In addition, **Figure 1A** shows that the method is capable of distinguishing different r levels as the line moves upwards when actual correlation r increases.

We also study the influence of window size on the similarity scores. With random timestamps n_r fixed at 1,000, we calculated similarity scores at different r levels using the window size of 1 h, 6 h, 12 h and 24 h. In **Figure 1B**, when using window size of 24 h, the similarity score will be close to 1 if r is more than 0.04. It indicates that the method considers r being more than 0.04 as two sequences being strongly related. However, when we reducing the window size, the maximum value of the curve using the window size of 1 h is only near 0.8, meaning that the method could even distinguish r whose value is more than 0.2 which is not a small value when considering correlation between two devices. When analyzing real data, we can change the window size to make the distribution of scores as scattered as possible so that we can rank all the pairs of devices and find the most related ones.

EXPERIMENT

In this section, we use the method described above to analyze real data of device alarms in telecommunication networks and constructed a functional network that could help to locate faults by scoring the probability of every two devices being correlated when reporting alarm messages. Moreover, based on the location of devices, we construct a city-to-city alarm network (CCAN) and analyze its structure.

Data Description

The database is from a Chinese telecommunication company, including the alarm messages of about 500,000 telecommunication devices in a province of China from 26th August to 25th September in 2015. In the following, we anonymize the name of the province (named as G hereafter) and the related cities. Each message in the database includes device ID, alarm title, type, location, and other information. We pick out messages that recorded both device ID and location. **Figure 2** shows that the alarm number distribution of 508,636 devices follow a power law distribution. To obtain the main correlation structure, we preprocess the database and take devices that documented alarm messages between 600 and 50,000 times into account. After that, 6,527 devices are considered into the following analysis.

Result

Firstly, letting every device be the vertex, a fully connected network is formed. Here, an edge is equivalent to a pair of devices, and its weight equals the calculated similarity score. Then, we remove edges whose similarity scores are smaller than a threshold value, and the rest of the edges form the backbone of the alarm correlation network. Secondly, we use every device's

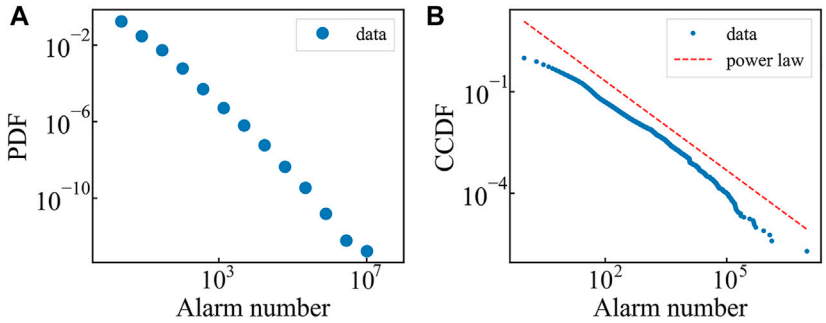


FIGURE 2 | (A) Probability density function (pdf) of alarm times with log-log coordinate. **(B)** Complementary cumulative distribution function (ccdf) of alarm times with log-log coordinate. The data follows a straight line in log-log coordinates, which indicates that the alarm number obeys the power law distribution.

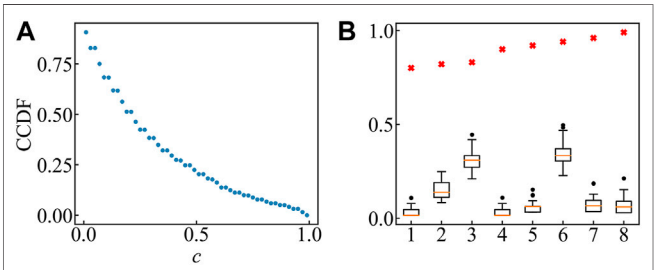


FIGURE 3 | (A) Complementary cumulative distribution function (ccdf) of the similarity scores. Each point shows the percentage of scores that are more than a certain value. When using a threshold that is no less than 0.8, more than 90% of the edges will be removed. **(B)** Boxplot of randomly shuffled alarm sequences. For every chosen pair of devices, shuffle their sequence for 100 times and calculate the similarity scores of them. Red crosses symbolize the original similarity score. The original scores are completely separated from the shuffled sequences scores' boxplots.

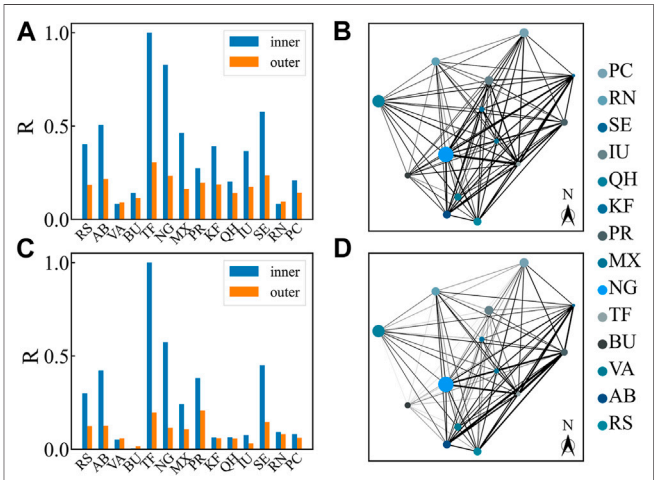


FIGURE 4 | Relative connection density and intercity alarm relevance network (CCAN): **(A)** Percentage of relative density inside and outside cities when using threshold 0.8. The inner relative density is painted blue and the outer is painted orange. Each R is normalized by the maximum value (0.1902) of inner relative density. **(B)** City-to-city network under threshold 0.8. Different cities are symbolized by dots with different colors. The size of dots represents the number of devices in every city. The width of edges is proportional to the value of relative density between cities. **(C)** Percentage of relative density inside and outside cities when using threshold 0.999. Each R is normalized by the maximum value (0.0664) of inner relative density. **(D)** City-to-city network under threshold 0.999. **(A,C)** show that when increasing the threshold of removing edges, the structure between cities starts emerging (still weaker than the connection inside cities). **(B,D)** show that cities lying in the southeast of the province are connected more strongly than otherwhere.

located city to analyze the relationship between the alarm numbers inside and outside the city and the network of cities.

After applying our method to the data, **Figure 3A** shows the complementary cumulative distribution function (CCDF) of the similarity scores. Each point shows the percentage of similarity scores that are more than a value. In **Figure 3A**, when we take 0.8 as a threshold of removing edges, there was less than 10% of the edges left in the network. In consideration of this, we use an approximation of hypergeometric distribution and the remaining term is of the same order as 0.0001, so choosing 0.999 as an upper bound for the analysis will not impact computation accuracy.

We randomly chose eight pairs of devices whose similarity scores are greater than 0.8 and shuffled their alarm times from the last 31 days to see if our index separates correlated devices from independent, uncorrelated ones. **Figure 3B** compares the scores of original alarm sequences with those of the shuffled sequences in 100 repetitions. The results show that the original scores are completely separated from the boxplots of the shuffled sequences scores, meaning that the device pairs left in the network are statistically correlated.

In the following, we show the devices' alarm correlation network in G province, China. To compare the connection strength inside and outside the cities, we normalize the connection by relative connection density. For every city in G province, the relative density inside the city is defined as

$$R_A^{in} = \frac{E_A}{|A| \times \frac{|A|-1}{2}}, \tag{5}$$

where E_A represents the number of edges (ignoring the similarity scores) and $|A|$ is the number of devices inside the city. The relative density outside the city is defined as

$$R_A^{out} = \frac{\sum_{B\in\mathcal{F},\ B\neq A} E_{AB}}{|A| \times \sum_{B\in\mathcal{F},\ B\neq A} |B|} \tag{6}$$

where $\mathcal{F}$ is a set of all the cities in province G, the numerator represents the number of edges between A and other cities, and the denominator represents the number of edges if all the devices inside city A are connected to all the devices inside other cities. We calculate the relative densities R after removing those whose similarity scores are less than 0.8, and present the percentage of the relative densities outside and inside the city in **Figure 4A**. Most of the cities' inner relative densities are more than the outer ones, which is consistent with our intuition. When increasing the threshold from 0.8 to 0.999, some structure between cities emerges, as shown by **Figure 4C**. Therefore, we draw the city-to-city network where the edges are weighted by the relative density between two cities which is defined as

$$R_{AB} = \frac{E_{AB}}{|A| \times |B|} \tag{7}$$

where E_{AB} is the number of edges between city A and B. The city-to-city networks under threshold 0.8 and 0.999 are exhibited in **Figures 4B,D**, where different cities are symbolized by colored dots, the size of dots represents the number of devices inside the city, and the width of the edges represents the relative densities between two cities. **Figure 4B** shows that the CCAN is a fully connected network. Devices from different cities connected more strongly than expected. Although the cities that lie in the north of G province, such as QH, RN and PC, have more devices than the cities in the southeast side, their connections with other cities are weaker than southeast cities. City NG and TF which are strongly connected to almost all cities in the province seem to be the center of the city-to-city network. However, when the threshold increases to 0.999, the center of the city-to-city network moves to the city PR whose device number is quite small when compared with other cities and PR is only connected strongly to the cities from the southeast. It seems that there are an alarm group consists of cities from the southeast area of the province.

CONCLUSION

Modern telecommunication systems produce large amounts of alarm messages. Correlating different alarm series in vital to effectively manage these alarm messages and maintain the performance of telecommunications networks. To measure the complex spatiotemporal correlation between telecommunication devices, we propose an index that uses the deviation of two alarm series from the random case to score the pair similarity in the device-to-device network. In **Figure 1**, synthetic series verify the validity of our index, and show that the similarity score can distinguish series pairs with different correlation levels and is robust when alarm numbers change. Moreover, the range that probability score vary with correlation level can be widened by reducing window size when calculating, as shown in **Figure 1B**. After verifying our method, we used it to analyze the telecommunication alarm database of devices in a Chinese province, and construct an alarm correlation network. In **Figure 4**, the results show that for most of the cities, the connection strength inside the cities is higher than outside. However, the connections outside cities are comparable with those inside cities. When increasing the edge removal threshold, cities' structures start to emerge (though still weaker than the connections within cities). By analyzing the CCAN, we find that cites lying in the southeast of the province connect more strongly than elsewhere. Our similarity score measures the pair similarity by deviating from the random case and has a potential for more general applications.

DATA AVAILABILITY STATEMENT

The data analyzed in this study is subject to the following licenses/restrictions: Because privacy issues are present, the data should not be shared. Requests to access these datasets should be directed to sfwang@bupt.edu.cn or linyifan13@foxmail.com.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct and intellectual contribution to the work, and have approved it for publication.

FUNDING

This research was supported by the National Key R&D Program of China (grant No. 2020YFF0305300).

REFERENCES

1. Haes Alhelou H, Hamedani-Golshan M, Njenda T, and Siano P. A Survey on Power System Blackout and Cascading Events: Research Motivations and Challenges. *Energies* (2019) 12(4):682. doi:10.3390/en12040682
2. Chung H-M, Li W-T, Yuen C, Chung W-H, Zhang Y, and Wen C-K. Local Cyber-Physical Attack for Masking Line Outage and Topology Attack in Smart Grid. *IEEE Trans Smart Grid* (2019) 10(4):4577–88. doi:10.1109/TSG.2018.2865316
3. Brugnoni S, Bruno G, Manione R, Montariolo E, and Sisto L. An Expert System for Real Time Fault Diagnosis of the Italian Telecommunications Network. *Integrated Network Management III*. In: Proceedings of the IFIP TC6/WG66 Third International Symposium on Integrated Network Management with participation of the IEEE Communications Society CNOM and with support from the Institute for Educational Services; 18-23 April; San Francisco, California, USA. AE Amsterdam, Netherlands: North-Holland Publishing Co., Div. of Elsevier Science Publishers B.V (1993). p. 617–28.
4. Jakobson G, and Weissman M. Alarm Correlation. *IEEE network* (1993) 7(6): 52–9. doi:10.1109/65.244794
5. Bouloutas AT. *Modeling Fault Management in Communication Networks [Ph.D Thesis]*. Columbia: Columbia University (1990).
6. Bouloutas AT, Calo S, and Finkel A. Alarm Correlation and Fault Identification in Communication Networks. *IEEE Trans Commun* (1994) 42(234):523–33. doi:10.1109/TCOMM.1994.577079

7. Dai X, and Gao Z. From Model, Signal to Knowledge: A Data-Driven Perspective of Fault Detection and Diagnosis. *IEEE Trans Ind Inf* (2013) 9(4):2226–38. PubMed PMID: 13843496. doi:10.1109/TII.2013.2243743
8. Perng C-S, Thoenen D, Grabarnik G, Ma S, and Hellerstein J. Data-driven Validation, Completion and Construction of Event Relationship Networks. In: Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining; August 24 - 27; Washington, DC, USA. New York, NY, United States: Association for Computing Machinery (2003). p. 729–34. doi:10.1145/956750.956848
9. Albert R, and Barabási A-L. Statistical Mechanics of Complex Networks. *Rev Mod Phys* (2002) 74(1):47–97. doi:10.1103/RevModPhys.74.47
10. Newman MEJ. The Structure and Function of Complex Networks. *SIAM Rev* (2003) 45(2):167–256. Epub May 2, 2003. doi:10.1137/S003614450342480
11. Sakoe H, and Chiba S, editors. *A Dynamic Programming Approach to Continuous Speech Recognition*. Budapest, Hungary: International Congress on Acoustics (1971).
12. Sakoe H, and Chiba S. Dynamic Programming Algorithm Optimization for Spoken Word Recognition. In: Waibel A and Lee K-F, editors. *Readings in Speech Recognition*. San Francisco: Morgan Kaufmann (1990). p. 159–65. doi:10.1016/b978-0-08-051584-7.50016-4
13. Keogh EJ, and Pazzani MJ. *Derivative Dynamic Time Warping*. Chicago: First SIAM international conference on data mining (2001).
14. Lahreche A, and Boucheham B. A Fast and Accurate Similarity Measure for Long Time Series Classification Based on Local Extrema and Dynamic Time Warping. *Expert Syst Appl* (2021) 168:114374. doi:10.1016/j.eswa.2020.114374
15. Golay X, Kollias S, Stoll G, Meier D, Valavanis A, and Boesiger P. A New Correlation-Based Fuzzy Logic Clustering Algorithm for FMRI. *Magn Reson Med* (1998) 40(2):249–60. doi:10.1002/mrm.1910400211
16. Burr IW. Some Approximate Relations between Terms of the Hypergeometric, Binomial and Poisson Distributions. *Commun Stat* (1973) 1(4):297–301. Epub 27 Jun 2007. doi:10.1080/03610927308827027

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 14 September 2021
doi: 10.3389/fphy.2021.743670

A Power Dispatch Optimization Method to Enhance the Resilience of Renewable Energy Penetrated Power Networks

Yuehui Huang[1], Pai Li[1], Xi Zhang[2], Bingchun Mu[2], Xuefei Mao[2] and Zhen Li[2]*

[1]China Electric Power Research Institute, Beijing, China, [2]Beijing Institute of Technology, Beijing, China

With the wide deployment of renewable energies, future power grids become more vulnerable to extreme environments. This paper investigates enhancing the resilience of power systems with high penetrations of renewable energies under emergencies. The resilience enhancement firstly is defined as maintaining as much electric energy to critical loads in a fixed number of post-disaster periods by properly coordinating the available resources. Then, an optimal decision-making method is proposed to maximize the power supply of critical loads and to minimize the instability risks due to the randomness of the output power of renewable energies. The power consumption of loads, charging/discharging power of power storage plants, power generation of generators, and spinning reserve ratios of the renewable energy at each period are taken as decision variables. Constraints include spinning reserve, power flow constraints, and power consumption/generation limits. The interior-point algorithm is used to solve the formulated optimization problem. Numerical simulations verified the effectiveness and superiority of the proposed optimization method in boosting grid resilience after disasters. It is also found that a balance should be sought between decreasing stability risks and increasing the power supply benefit in extreme environments.

Keywords: power network, resilience optimization, renewable energies, power dispatch, complex networks

OPEN ACCESS

Edited by:
Yongxiang Xia,
Hangzhou Dianzi University, China

Reviewed by:
Xingle Gao,
Hunan University, China
Xingtang Wu,
Beihang University, China

****Correspondence:***
Xi Zhang
xizhang@bit.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *19 July 2021*
Accepted: *25 August 2021*
Published: *14 September 2021*

Citation:
Huang Y, Li P, Zhang X, Mu B, Mao X and Li Z (2021) A Power Dispatch Optimization Method to Enhance the Resilience of Renewable Energy Penetrated Power Networks. Front. Phys. 9:743670. doi: 10.3389/fphy.2021.743670

1 INTRODUCTION

1.1 Backgrounds

Power networks are essential infrastructures that support almost all kinds of activities in modern society. Their ability to maintain a reliable electricity supply to the consumers under various emergencies is crucial to society's day-to-day operations. Due to the broad geographical coverage and exposure to wild and adverse environments, the power network is subject to various disturbances. Extreme environments will seriously affect the normal operation of the power network, reducing the network connectivity and functions. Damage to the network topology will lower the supply of load and seriously endangering economic development and social stability [1]. Thus, increasing the power grid resilience in face to extreme conditions has profound significance.

The study on network resilience has been an popular topic in the filed of complex networks since the publication of [2–6]. Being a typical complex network, the power network's resilience has also attracted the interest of many scholars [7, 8]. The resilience of the power network refers to the ability of the power grid to resist interference and restore power promptly under inclement weather such as

typhoons, heavy rain/snow, and earthquakes, or artificial attacks such as graphite bombs, high-altitude nuclear magnetic explosions, and computer viruses [9, 10]. Reference [11] comprehensively reviewed the evolution and current status of the U.S. power network, and exploreed ways to improve the resilience of the power network. Based on the understanding of the resilience recovery process of the power network, Refs. [12, 13] proposed a simulation model for the power system and addressed indexes to evaluate the network resilience. The model considered a series of equipment failures and repair events in the resilience process, in which the probability of equipment failure was expressed as a function of weather parameters, and the length of time from failure to repair of the failed equipment was set to obey an exponential distribution.

Motivated by energy and environmental requirements, the power network is entering a new era due to increasing penetrations of renewable energies. Making full use of existing available resources to achieve the maximum power supply capacity (the maximum power system sufficiency) by power dispatch and topology adjustments is an effective means to improve the resilience of the power system, and it is beneficial to alleviating the negative impact of extreme environments on social stability [14]. However current research on power network resilience fails to incorporate the increasing trend of the proportion of new energy sources connected to the power system and lacks sufficient control that considers the intermittent output of new energy sources and the reduction in the proportion of spinning reserve.

Differing from traditional power sources, the power outputs of renewable power units are random and fluctuant, which are determined by the weather. Renewable energy power units connect to the grid *via* electronic equipment with zero inertia and low tolerance. Though renewable energies bring huge environmental and social benefits, they also bring challenges to the safe operation of the power grid and the recovery of the system after severe damage under inclement weather. First, under inclement weather, the components and pieces of equipment of the power system are likely to be physically damaged, and it takes a long time to repair them or build new equipment [15]. Second, the randomness and fluctuantions of renewable power units are detrimental to maintaining the power balance in the power system, which requires traditional generators to keep an appropriate amount of reserve. In this case, higher amounts of reserve from traditional generators will reduce the power supplied to loads, while lower amounts of reserve from traditional generators will increase the operation risk.

1.2 An Insight to Enhance the Grid Resilience

When the power network is affected by inclement weather, its load-supply capacity is reduced. Moreover, it is difficult to repair electrical components that are physically damaged in the short term after the impact of extreme conditions. Therefore, it is practically feasible to boost the resilience of the damaged power grid by making full use of the remaining available resources to maximize the power supply benefit of the damaged power system, which can help significantly alleviate the negative impact of extreme environments on social stability.

Under inclement weather, it is hard for the power network to satisfy the power supply requirements of all loads. Thus the power consumption of each node should be reorganized by the dispatch center to maximize the power supply benefit of the power network. At the same time, during the special period of insufficient power supply after disasters, the power supply should also be prioritized to some certain consumers, e.g., government, hospitals, etc., should be higher than the power supply priority of some factories. Therefore, the weighted sum of the loads, which serves as the main part of the power supply benefit, is the objective function of the optimization model considered in this paper.

To maintain safety and stability, a certain amount of spinning reserve needs to be reserved for the conventional generators to cope with randomness and intermittent in the power network. Under normal circumstances, there are two main sources of randomness and volatility in power networks with high penetrations of renewable energies: load and renewable energy generators. Under inclement weather, the system only needs to plan conventional generators to reserve a certain amount of spinning reserve to balance the fluctuation of the renewable energy generators if loads are controlled without randomness and volatility. The total power generation of renewable energy generators in the network and the spinning reserve ratio during each period serve as the spinning reserve capacity of the system for each period. Therefore, the amount of the spinning reserve ratio of the network at each time will also affect the power supply capacity of the system in extreme environments. For example, if the spinning reserve ratio is too large, the power of the conventional generators for load supply will be reduced, which will affect the power supply benefit. In contrast, if the ratio is too small, once the actual output of the renewable energy generators is much smaller than the planned output, the planned load power will not be supplied. As a result, the power network will even lose balance, and a series of cascading failures will occur, which will heavily deprive the power supply of the network in extreme environments. Therefore, it is necessary to optimize the spinning reserve ratio for each period. In addition, the spinning reserve ratio of the system for each period is also an important factor that needs to be considered for flexibility optimization.

Inspired by this, an optimization model is proposed to enhance the resilience of the power network with high penetrations of renewable energies. The main contributions are as follows:

- The resilience of the power network with high penetrations of renewable energies is studied. Specifically, the stochastic properties of the renewable power units' output are considered.
- A new resilience metric for the power network is proposed and defined as the amount of electric energy maintained to critical loads within a fixed number of periods. Then an optimization model aiming to maximize the power supply of critical loads and minimize the instability risks is proposed, and the power consumption of loads, power

generation of generators, and spinning reserve ratios of the renewable energy at each period are taking as decision variables to coordinate the available resources properly;
- Two cases study based on the real power network are implemented, showing that the proposed optimization method can effectively boost grid resilience after disasters.

The remainder of this paper is organized as follows. The detailed optimization model is formulated in **Section 2**; two cases studied are carried out in **Section 3** to verify the proposed model, and **Section 4** concludes this work.

2 MODEL FORMULATION

2.1 Disposal of the Uncertainty of Renewable Energy Power

In this paper, the time duration of the resilience optimization considered for the power system is a short time (a few hours) after disasters, so the uncertainty of the renewable energy output in a short time needs to be considered [16,17]. The current renewable energy power generation mainly consists of wind power and photovoltaic power generation. Wind power accounts for the highest proportion (about 70%) of renewable energy power, and the short-term forecast error models of wind power photovoltaic power are similar. Thus the disposal of the uncertainty of renewable energy power in this paper mainly refers to the short-term forecast error model of wind power output for simplicity.

As renewable energy power generation is affected by weather and other factors, it is random and volatile and cannot be accurately predicted. The forecast error of renewable energy output is defined as:

$$\tilde{P}_{re}(t) = P_{re}(t) + \Delta P_{re}(t), \tag{1}$$

where $\tilde{P}_{re}(t)$, $P_{re}(t)$ and $\Delta P_{re}(t)$ are the actual value, the forecasted value, and the forecasted error of renewable energy power output, respectively. The wind power output forecast errors basically follows the Gaussian distribution according to the statistitics [18, 19]. In this paper, the short-term forscast errors of the reneable energy follows the Gaussian distribution $N(0, \sigma_{re}^2)$, whose standard deviation is defined as:

$$\sigma_{re}(t) = K * P_{re}(t) + RE_I/50, \tag{2}$$

where K is the forecast error factor for renewable energy power, which is always set as 0.2; RE_I is the total installed capacity of renewable energy power supply.

2.2 Decision Variables

In the optimization model, the decision variables are composed of the following parts:

- The output of each conventional power generator node in each period $P_i(t)$
- The power of each load node in each period $P_l(t)$
- The output of each renewable energy generator node in each period $P_{re}(t)$

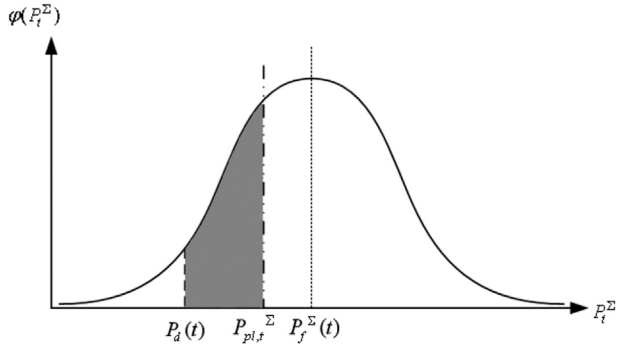


FIGURE 1 | Probability density distribution of the total output of the renewable energy during the period t.

- The power of each power storage node in each period $P_{sto}(t)$
- The spinning reserve ratio of the renewable energy in each period $r(t)$

2.3 Objective Function

The objective of the power system resilience optimization studied in this paper is to get the maximum power supply benefit by supplying power to various loads according to their priority in the short term under extreme environments without considering the cost through the remaining generation resources. Apart from the power supply to loads, the stability of the power system also plays an important role in the evaluation of the benefit. Therefore, due to the randomness of renewable energy power generation, conventional generator nodes are required to provide a certain amount of upward spinning reserve to deal with the situation where the actual output of the renewable energy is lower than the planned output to avoid causing the failure to supply load as planned power and cascading failure caused by power grid instability. In conclusion, the objective function of the optimization problem is:

$$\max \ F = \sum_{t=1}^{m} (P_L(t) - Q(t)) * \Delta t, \tag{3}$$

where $P_L(t)$ is the weighted sum of the power of all load nodes of the period t, $Q(t)$ is the loss rate of the power supply benefit caused by the insufficient actual output of renewable energy power generator nodes and insufficient spinning reserve of the period t, Δt is the duration of a period. The specific formula $P_L(t)$ is defined as follows:

$$P_L(t) = \sum_{l=1}^{L} w_l P_l(t) \tag{4}$$

where $P_l(t)$ is the planned power of load l during the period t, w_l is the power supply weight factor of the load l. The larger the value, the higher the power supply priority of the load under extreme environments.

The analysis of $Q(t)$, which is the loss rate of the power supply benefit caused by the insufficient actual output of the renewable energy and insufficient spinning reserve during the period t, is

shown in **Figure 1**. As shown in **Figure 1**, assuming that the actual power of renewable energy during the period t obeys the Gaussian distribution, the abscissa $P_t^{\sum}$ is the actual value of the total output of the renewable energy during the period t, and $P_f^{\sum}(t)$ is the average value, which is the forecasted output during the period t; $P_{pl,t}^{\sum}$ is the planned total output of the renewable energy power during the period t. The shaded part in the figure is the range of renewable energy output that can be balanced by the spinning reserve reserved by the system and $P_d(t)$ is the minimum value of the actual total output of the renewable energy allowed by the spinning reserve. Therefore, when the renewable energy output is less than $P_d(t)$, the spinning reserve is insufficient, resulting in the power supply to the load node not reaching the expected amount. Under extreme environmental conditions, failure to supply load as planned power is likely to cause serious economic losses and even cause more serious cascading failures. The specific formula $Q(t)$ is:

$$Q(t) = K_{loss} * \int_0^{P_d(t)} \varphi\left(P_t^{\sum}\right)\left(P_d(t) - P_t^{\sum}\right) dP_t^{\sum} \tag{5}$$

where K_{loss} is the benefit loss factor. The larger the value, the more serious the loss of the power supply benefit caused by insufficient renewable energy output and insufficient spinning reserve. $\varphi(P_t^{\sum})$ is the Gaussian distribution function of renewable energy power. $P_d(t)$ is the integral upper limit, which is the minimum value of the actual total output of the renewable energy allowed by the spinning reserve, and it can be calculated by the formula as follow:

$$P_d(\mathrm{t}) = (1 - r(t))\left(\sum_{re=1}^{RE} P_{re}(t)\right), \tag{6}$$

where $P_{re}(t)$ is the planned output of the renewable energy generator node re, and RE contains all the renewable energy generator nodes.

In summary, the reaction of $P_L(t)$ and $Q(t)$ in each period of the objective function to the change of the spinning reserve ratio in each period is the same. Still, the changes of the two variables have opposite effects on the value of the objective function. Therefore, the objective function of the optimization model in this paper will drive the optimization algorithm to find a balance value in the determination of the spinning reserve ratio in each period for the system so that the system can maximize its power supply capacity while maintaining a certain degree of reliability under extreme environments to achieve the greatest power supply benefit.

2.4 Constraints

Constraints include active power balance constraint (**Eq. 7**), spinning reserve constraint (**Eq. 8**), power flow constraint of lines (**Eq. 9**), output constraint of the conventional generator nodes (**Eq. 10**), constraints of the output rate of change of the conventional generator nodes (**Eqs 11**, **12**), load power constraint (**Eq. 13**), output constraint of renewable energy generator nodes (**Eq. 14**), power constraints of energy storage nodes (**Eq. 15**), and capacity constraints of power storage nodes (**Eq. 16**).

$$\sum_{i=1}^{N} P_i(t) + \sum_{re=1}^{\mathrm{RE}} P_{re}(t) + \sum_{sto=1}^{STO} P_{sto}(t) = \sum_{l=1}^{L} \mathrm{P}_l(t) \tag{7}$$

$$\sum_{i=1}^{N} \min\left(P_{i,\max} - P(t), P_{i,up} * \Delta t\right) \geq r(t) * \sum_{re=1}^{\mathrm{RE}} P_{re}(t) \tag{8}$$

$$-L_{ij,\max} \leq L_{ij}(t) \leq L_{ij,\max} \tag{9}$$

$$P_{i,\min} \leq P_i(t) \leq P_{i,\max} \tag{10}$$

$$P_i(t+1) - P_i(t) \leq \Delta P_{i,up} \tag{11}$$

$$\mathrm{P}_i(t) - P_i(t+1) \leq \Delta P_{i,down} \tag{12}$$

$$P_{l,\max} \leq P_l(t) \leq 0 \tag{13}$$

$$0 \leq P_{re}(t) \leq P_{re,f}(t) \tag{14}$$

$$P_{sto,\max}^{in} \leq P_{sto}(t) \leq P_{sto,\max}^{out} \tag{15}$$

$$0 \leq \sum_{t=1}^{t \leq t_1} P_{sto}(t) \cdot \Delta t \leq S_{sto,\max}, \quad t_1 \in T \tag{16}$$

where $P_{i,\max}$ and $P_{i,\min}$ are the upper limit and lower limit of output of conventional generator node i, respectively; $P_i(t)$ is the output of conventional generator node i during the period t; N contains the conventional generator nodes in the system; $\Delta P_{i,\text{up}}$ and $\Delta P_{i,\text{down}}$ are the maximum upward ramp rate and the maximum downward ramp rate of conventional generator node i, respectively; $P_{l,\max}$ is the maximum absorbed power of load node i, which is a negative value; $P_{re,f}(t)$ is the predicted output of the renewable energy power generator node re of the period t; $P_{sto,\max}^{\text{in}}$ and $P_{sto,\max}^{\text{out}}$ are respectively the maximum input and output power of the power storage node sto; $S_{sto,\max}$ is the maximum capacity of the power storage node sto; t is any period in the entire research time range T.

The spinning reserve constraint is specifically the upward spinning reserve constraint. The principle is that when the actual output of the renewable energy unit cannot reach the planned output, a certain amount of upward spinning reserve is required to make up for the lack of renewable energy output. Corresponding to downward rotation is upward rotation. To obtain the maximum power supply benefit within a short term, its planned output should be controlled below its forecasted output to avoid potential safety hazards of the power grid caused by the upward fluctuation of renewable energy output and the burden of the downward spinning reserve. Therefore, the downward spinning reserve is not taken into consideration in this paper.

3 CASES STUDY

Two kinds of cases are considered in this section to verify the effectiveness of the proposed model. The details are shown in follows.

3.1 Case 1 (Power System Without Power Storage Plants)

The simulations in this paper are based on the IEEE 39-Bus Test Case, as shown in **Figure 2**. Node 34, 35, 36, 37, 38 are selected as wind power generator nodes. It is assumed that nodes whose index are 23, 24, 31, 32, 33, 37, 38 are damaged due to extreme

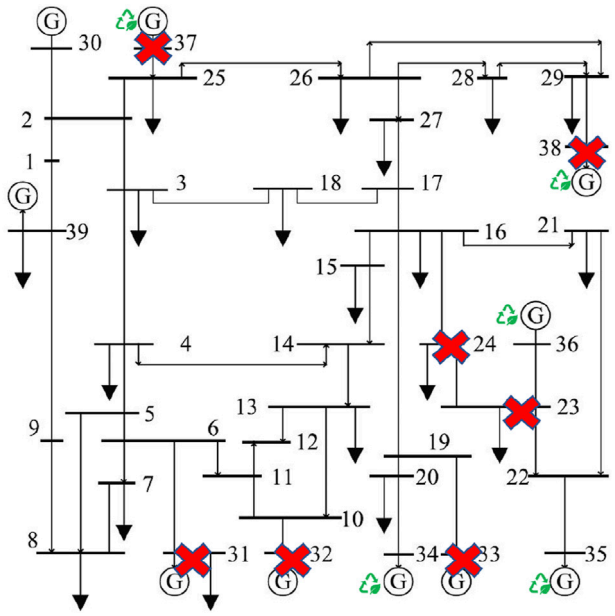


FIGURE 2 | The power network used based on the IEEE 39-Bus system.

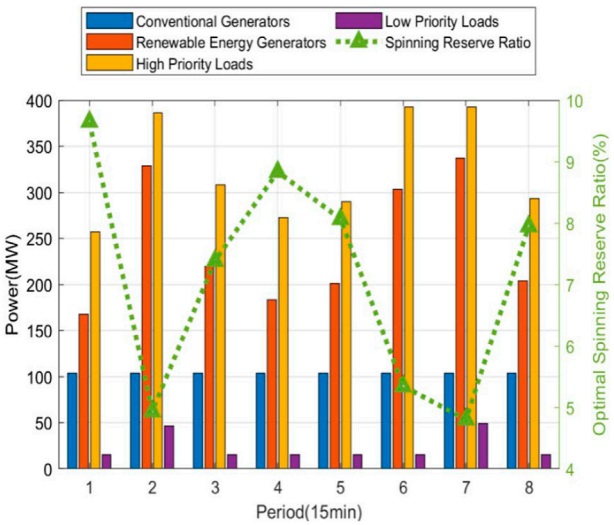


FIGURE 3 | Results of optimal variables.

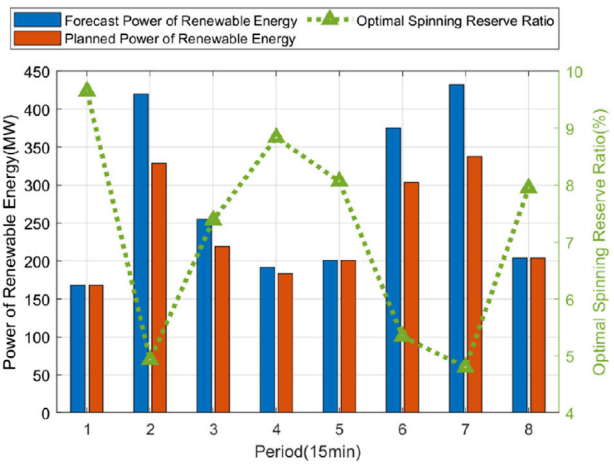


FIGURE 4 | The relationship between the optimal ratio of renewable energy reserve of each period and the forecast power and planned power of the renewable energy.

environments and are unavailable for the power dispatching center.

The DC power flow model is adopted in the simulation to improve the computational efficiency. The nodes in the system model are divided into four types: conventional power generator nodes, renewable energy generator nodes, load nodes, and power storage nodes (in case 2). The main parameters of conventional power generator nodes, load nodes, and power storage nodes are shown in **Supplementary Appendix Tables S2, S3, S4**.

A set of forecasted values of the renewable energy output is drawn up regarding the actual output data of the renewable energy in a certain place. The time scale of the renewable energy ultra-short-term forecast is 4-h and the time resolution is 15-min, and the time range studied in this paper is 2-h (8-period) after the disaster. The forecasted output values of renewable energy generator nodes are shown in **Supplementary Appendix Table S4** in the appendix. The simulation is coded in Matlab based on the functions provided by Matpower [20].

The benefit loss factor is set to 10, the load priority weight is set to two levels of 1 and 10, and the standard deviation of the short-term forecast error of renewable energy output is set to 0.2 times the output of renewable energy generation. The results of the optimization are as follows.

3.1.1 Results of Optimal Variables

The results of the spinning reserve ratio in each period and the planned power of nodes are shown in **Figure 3**.

The relationship between the optimal spinning reserve ratio in each period and the total output of renewable energy generator nodes are shown in **Figure 4**.

Through analyzing the results of the optimization variables, it can be seen that the optimal spinning reserve ratio in each period has an inverse relationship with the renewable energy output in that period. That is to say, the higher the renewable energy output in a period, the smaller the optimal spinning reserve ratio in that period. The reason is that when the renewable energy output is high during the period, the same reserve ratio means that more reserve capacity will be reserved by the conventional generators. The excessive spinning reserve will occupy the scarce conventional generation resources of the post-disaster power system, resulting in a decline in the power supply efficiency of the system. Therefore, the optimization method in this paper can flexibly determine the spinning reserve rate in each period when the output of renewable energy fluctuates in different periods under extreme environments to maximizes the power supply benefit. Besides,

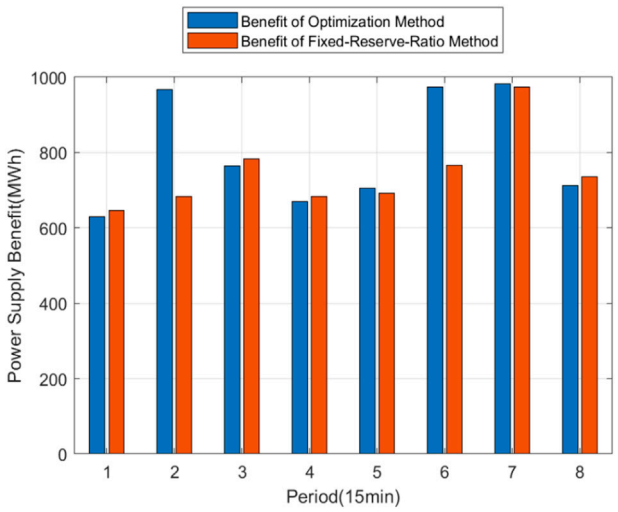


FIGURE 5 | Power supply benefits of the two methods in each period.

the results show that loads with high priority fluctuate less with renewable energy output and have a high degree of satisfaction. In contrast, loads with low priority fluctuate more with the output of renewable energy and are almost zero when renewable energy output is low.

Under extreme environments, renewable energy generator nodes' planned output is often lower than the forecast output to maximize the power supply benefit. The reason is that the topology of the post-disaster network is different from that of normal conditions, and constraints such as power flow constraint and active power balance constraint restrict the power of each node, including renewable energy generator nodes.

3.1.2 Improvement of Power Supply Benefit

The reserve ratio is set to a fixed value (between 5 and 10%) by the traditional reserve configuration method [20]. The optimization method in this paper is compared with the traditional reserve configuration with a fixed ratio of 5%. And the power supply benefits in each period of the two methods are shown in **Figure 5** for comparison.

As for the total power supply benefit of 8 periods, the total benefit of the optimization method is 6405.471 MWh, while the total benefit of the traditional fixed-reserve-ratio method is 5961.039 MWh. Compared with the traditional method, the method proposed in this paper has significantly improved the power supply benefit by attaining a 7.45% increase in the total power supply benefit. However, as for the power supply benefit in some periods (such as periods 1 and 3), the optimization method behaves worse than the fixed-reserve-ratio method. The reason is that the objective function of the optimization method is the total benefit of all periods, and there are constraints of the output rate of change of the conventional generator nodes (**Eqs 11**, **12**). As a result, the optimization method may try to obtain the optimal total benefit by sacrificing the benefit of some period.

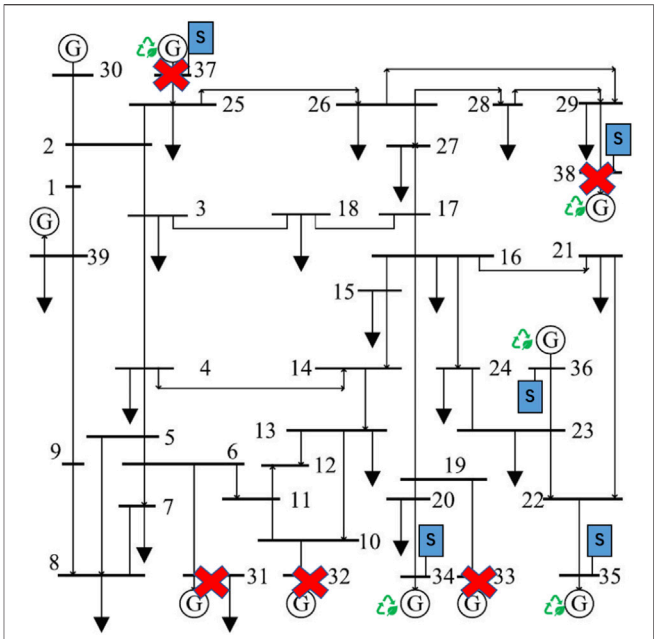


FIGURE 6 | The power network with power storage nodes based on the IEEE 39-Bus system for case 2.

TABLE 1 | Power Supply Benefit of the two systems.

System	Total power supply benefit (MWh)
System with Power Storage	6877
System without Power Storage	7166

3.2 Case 2 (Power System With Power Storage Plants)

To analyze the impact of power storage plants on the power supply benefits for power networks with high penetrations of renewable energies under extreme environments, this paper implements another case study on a power network with power storage plants. Based on the power network in case 1, power storage nodes attached to renewable energy generator nodes are added to the grid, and load nodes are not assumed to be destroyed by disasters. The main parameters of nodes are the same as in case 1. The power network for case 2 is shown in **Figure 6**.

3.2.1 Results of Optimal Variables

This paper compares the power supply benefits of the two systems and the input power of loads with different power supply priorities in each period to analyze the influence of power storage nodes. The results are shown in **Table 1**, **Figures 7**, **8**. The benefit loss factor is set to 10, the load priority weight is set to two levels of 1 and 10, and the standard deviation of the ultra short-term forecast error of the renewable energy output is set to 0.2 times the output of renewable energy generation. The optimized results are as follows.

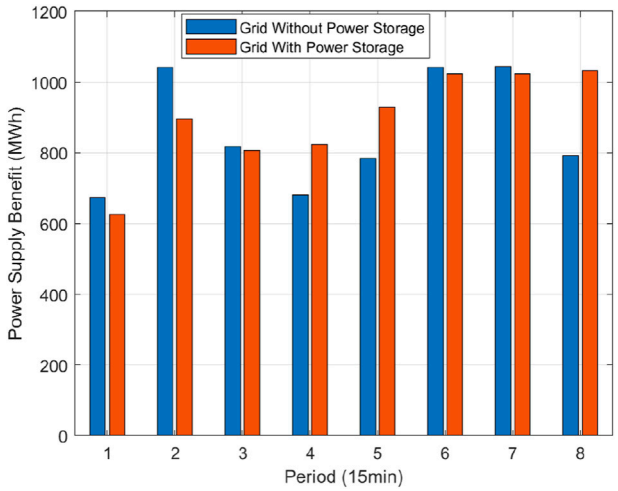


FIGURE 7 | Power supply benefits in each period of the two systems.

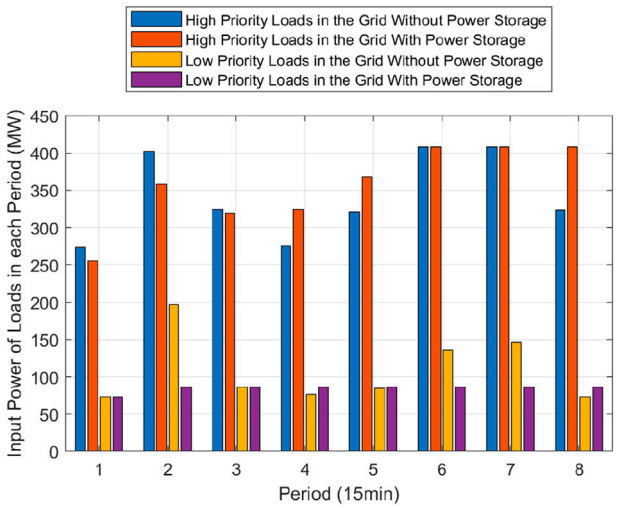


FIGURE 8 | Input power of loads in each period of the two systems.

From **Table 1** and **Figure 7**, it can be concluded that from the perspective of the power supply benefit in each period, the system with power storage does not always perform better than the original system without power storage. The reason is that a part of the generator nodes' power in the system with power storage is absorbed by power storage nodes in certain periods, so the power supply benefits of these periods are often lower than the original system without power storage. However, the total power supply benefit of the power network with power storage increased by 4.2% than that of the original power system, showing the advantages of adding power storage. Besides, it can be seen from **Figure 8** that the input power of high-priority loads in the system with power storage is higher than that of the system without power storage in most periods, while the input power of low-priority loads is lower than that of the system without power storage in most periods, indicating that loads with high power supply priority in the system with power storage account for a larger proportion of power supply. It can be concluded that the power system with power storage nodes guarantees the continuous power supply of critical loads at the expense of the power supply of low-priority loads, improving the total power supply benefit.

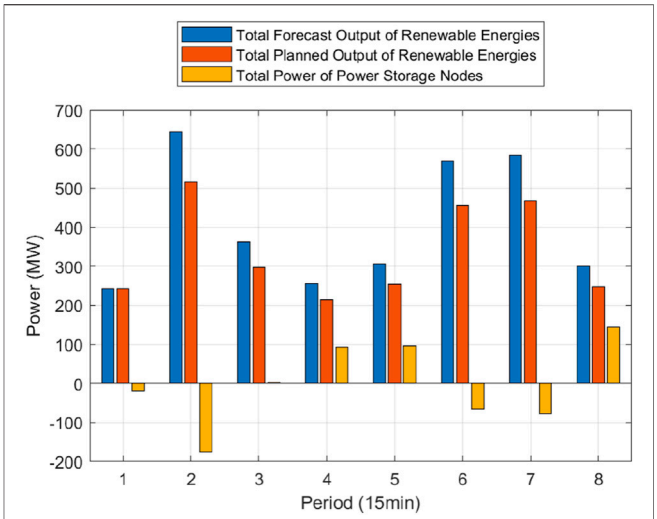


FIGURE 9 | Relationship between the output of renewable energy generator nodes and the power of power storage nodes in each period.

3.2.2 The Relationship Between the Output of Renewable Energy Generator Nodes and the Power of Storage Nodes in Each Period

To study the mechanism of how power storage plants improve the power supply benefit of power network with high penetration of renewable energies under extreme environments, this paper analyses the relationship among the forecasted output of renewable energy generator nodes, the planned output of renewable energy generator nodes, and the power of power storage nodes in the system with power storage nodes in each period, as shown in **Figure 9**.

It can be concluded from **Figure 9** that the power storage can help regulate the fluctuant output of the renewable energy generation, like "cutting the peak and filling the valley." When the output of the renewable energy generation is high, power storage plants act as loads by absorbing electricity power, while the output of the renewable energy generation is low, power storage plants act as generators by releasing electricity power. Unlike the power system under normal circumstances, the load is considered controllable in extreme environments, so the load is not volatile. The peak shaving effect of the power storage node in the optimization model is based on the extreme environment where the power supply is insufficient, and loads have a difference in power supply priority. When the output of the renewable energy generation is high, the power supply of the high-priority load may be saturated. During this time, the power supply benefit of supplying the remaining power to a low-priority load is poor.

Thus the power storage plants store the electric power, which is relatively sufficient. When the output of the renewable energy generation is low, the power storage plants act as generators by releasing power, which can help high-priority loads getting better power supply when the power supply capacity is insufficient, ensuring the continuous power supply of the critical load. As a result, the power storage plants can help promote the short-term power supply benefits after disasters.

4 CONCLUSION

The problem of optimizing the power supply to critical loads after disasters considering the uncertainty of renewable energy output for a power network is studied in this paper. The overall power supply benefit of the power network with high penetrations of renewable energies in several post-disaster periods is identified as a resilience indicator of the power system with the consideration of the priority of different loads and safety risks. An optimization model for obtaining the total maximum power supply benefit is established with the spinning reserve ratio in each period, and the power of each node is taken as decision variables. The priority difference of each load and the negative impact of the failure to supply load as planned caused by the insufficient actual output of the renewable energy and insufficient spinning reserve is comprehensively considered in the objective function. Simulations on the IEEE 39-Bus Test Case are performed to verify the superior performance of the proposed method. The results show that the optimization method can flexibly determine the spinning reserve ratio and the power of each node in extreme environments, and increase the total power supply by 7.45%. Besides, another case studied is implemented to analyze the impact of power storage plants on the power supply benefits for power networks with high penetrations of renewable energies in extreme environments. Results show that the system with power storage guarantees the continuous power supply of critical loads by sacrificing the power supply for low-priority loads and improving the system's total power supply benefit.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. This data can be found here: https://matpower.org/.

AUTHOR CONTRIBUTIONS

YH is responsible for the conceptualization and direction of the work. PL is for the problem formulation and validation of the method. XZ is responsible for the editing of the paper and funding acquisition. BM is responsible for the writing of the paper, data collection, and simulations. XM and ZL are responsible for simulation results analysis.

FUNDING

This paper is supported by Open Fund of State Key Laboratory of Operation and Control of Renewable Energy and Storage Systems (China Electric Power Research Institute) No. NYB51202001596.

SUPPLEMENTARY MATERIAL

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fphy.2021.743670/full#supplementary-material

REFERENCES

1. Panteli M, Trakas DN, Mancarella P, and Hatziargyriou ND. Power Systems Resilience Assessment: Hardening and Smart Operational Enhancement Strategies. *Proc IEEE* (2017) 105:1202–13. doi:10.1109/jproc.2017.2691357
2. Dong G, Gao J, Du R, Tian L, Stanley HE, and Havlin S. Robustness of Network of Networks under Targeted Attack. *Phys Rev E Stat Nonlin Soft Matter Phys* (2013) 87:052804. doi:10.1103/PhysRevE.87.052804
3. Gao J, Barzel B, and Barabási A-L. Universal Resilience Patterns in Complex Networks. *Nature* (2016) 530:307–12. doi:10.1038/nature16948
4. Dong G, Fan J, Shekhtman LM, Shai S, Du R, Tian L, et al. Resilience of Networks with Community Structure Behaves as if under an External Field. *Proc Natl Acad Sci USA* (2018) 115:6911–5. doi:10.1073/pnas.1801588115
5. Wu X, Dong H, Tse CK, Ho IWH, and Lau FCM. Analysis of Metro Network Performance from a Complex Network Perspective. *Physica A: Stat Mech its Appl* (2018) 492:553–63. doi:10.1016/j.physa.2017.08.074
6. Wu X, Dong H, and Chi KT. A Three-Layer Model for Studying Metro Network Dynamics. *IEEE Trans Syst Man, Cybernetics: Syst* (2019) 51:2665–75. doi:10.1109/tsmc.2019.2915928
7. Zhang X, Tu H, Guo J, Ma S, Li Z, Xia Y, et al. Braess Paradox and Double-Loop Optimization Method to Enhance Power Grid Resilience. *Reliability Eng Syst Saf* (2021) 215:107913. doi:10.1016/j.ress.2021.107913
8. Wu J, Chen Z, Zhang Y, Xia Y, and Chen X. Sequential Recovery of Complex Networks Suffering from Cascading Failure Blackouts. *IEEE Trans Netw Sci Eng* (2020) 7:2997–3007. doi:10.1109/tnse.2020.3008799
9. Council NR. *The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters: Summary of a Workshop*. Washington, D.C.: National Academies Press (2013).
10. Wu J, Fang B, Fang J, Chen X, and Tse CK. Sequential Topology Recovery of Complex Power Systems Based on Reinforcement Learning. *Physica A: Stat Mech its Appl* (2019) 535:122487. doi:10.1016/j.physa.2019.122487
11. National Academies of Sciences, E., Medicine. *Enhancing the Resilience of the Nation's Electricity System*. Washington, D.C.: National Academies Press (2017).
12. Panteli M, Pickering C, Wilkinson S, Dawson R, and Mancarella P. Power System Resilience to Extreme Weather: Fragility Modeling, Probabilistic Impact Assessment, and Adaptation Measures. *IEEE Trans Power Syst* (2016) 32:3747–57. doi:10.1109/tpwrs.2016.2641463
13. Panteli M, Mancarella P, Trakas DN, Kyriakides E, and Hatziargyriou ND. Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems. *IEEE Trans Power Syst* (2017) 32:4732–42. doi:10.1109/tpwrs.2017.2664141
14. Gao H, Chen Y, Mei S, Huang S, and Xu Y. Resilience-oriented Pre-hurricane Resource Allocation in Distribution Systems Considering Electric Buses. *Proc IEEE* (2017) 105:1214–33. doi:10.1109/jproc.2017.2666548
15. Zhang X, Guo J, Wang T, Zeng S, Ma S, and Wu G. Identifying Critical Elements to Enhance the Power Grid Resilience. In: 2020 IEEE International

Symposium on Circuits and Systems (ISCAS). IEEE (2020). p. 1–5. doi:10.1109/iscas45731.2020.9180814
16. Hodge B-M, and Milligan M. Wind Power Forecasting Error Distributions over Multiple Timescales. In: 2011 IEEE power and energy society general meeting. IEEE (2011). p. 1–8. doi:10.1109/pes.2011.6039388
17. Bludszuweit H, Domínguez-Navarro JA, and Llombart A. Statistical Analysis of Wind Power Forecast Error. *IEEE Trans Power Syst* (2008) 23:983–91. doi:10.1109/tpwrs.2008.922526
18. Chaiyabut N, and Damrongkulkamjorn P. Uncertainty Costs of Wind Power Generation Considering Expected Energy Not Supplied under Different Spinning reserve Levels. In: The Second IASTED International Conference OnPower and Energy Systems and Applications (2012). p. 1–5. PESA. doi:10.2316/p.2012.788-052
19. Bouffard F, and Galiana FD. Stochastic Security for Operations Planning with Significant Wind Power Generation. In: 2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century. Pittsburgh, PA: IEEE (2008). p. 1–11. doi:10.1109/pes.2008.4596307
20. Zimmerman RD, Murillo-Sánchez CE, and Thomas RJ. Matpower: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education. *IEEE Trans Power Syst* (2010) 26:12–9. doi:10.1109/tpwrs.2010.2051168

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

frontiers in Physics

ORIGINAL RESEARCH
published: 13 October 2021
doi: 10.3389/fphy.2021.755567

The Robustness of Interdependent Directed Networks With Intra-layer Angular Correlations

*Zongning Wu, Zengru Di and Ying Fan**

School of Systems Science, Beijing Normal University, Beijing, China

The robustness of interdependent networks is a frontier topic in current network science. A line of studies has so far been investigated in the perspective of correlated structures on robustness, such as degree correlations and geometric correlations in interdependent networks, in-out degree correlations in interdependent directed networks, and so on. Advances in network geometry point that hyperbolic properties are also hidden in directed structures, but few studies link those features to the dynamical process in interdependent directed networks. In this paper, we discuss the impact of intra-layer angular correlations on robustness from the perspective of embedding interdependent directed networks into hyperbolic space. We find that the robustness declines as increasing intra-layer angular correlations under targeted attacks. Interdependent directed networks without intra-layer angular correlations are always robust than those with intra-layer angular correlations. Moreover, empirical networks also support our findings: the significant intra-layer angular correlations are hidden in real interdependent directed networks and contribute to the prediction of robustness. Our work sheds light that the impact of intra-layer angular correlations should be attention, although in-out degree correlations play a positive role in robustness. In particular, it provides an early warning indicator by which the system decoded the intrinsic rules for designing efficient and robust interacting directed networks.

Keywords: robustness, interdependent directed networks, intra-layer geometric correlations, targeted attacks, network embedded

OPEN ACCESS

Edited by:
Gaogao Dong,
Jiangsu University, China

Reviewed by:
Chengyi Xia,
Tianjin University of Technology, China
Hao Peng,
Zhejiang Normal University, China

****Correspondence:***
Ying Fan
yfan@bnu.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *09 August 2021*
Accepted: *23 September 2021*
Published: *13 October 2021*

Citation:
Wu Z, Di Z and Fan Y (2021) The Robustness of Interdependent Directed Networks With Intra-layer Angular Correlations. Front. Phys. 9:755567. doi: 10.3389/fphy.2021.755567

1 INTRODUCTION

In the past few decades, increasing studies had proved that most real-world networks are multi-layered by dependency connectivity to interact with one another, and such structures are of great interest in the aspect of the robustness [1–6]. An emerging field is also called the robustness of interdependent networks, interconnected networks, or interdependent networks. Indeed, cascading failures of interdependent networks are possible to induce catastrophic consequences: the failure of a node in one network leads to the collapse of the dependent nodes in other networks, which in turn may cause further damage to the first network [7, 8]. Enhancing the understanding of the real-world dynamical process thus needs to focus on the structure of interdependent networks, which is of utmost importance for preventing crashes or for engineering more efficient and stalwart networked systems [9, 10].

The study of the robustness for interdependent networks has been widely investigated in across-layers and intra-layers features of topology structures, including the degree correlations [11, 19], the coupling strength between layers [12], the community structure [13, 14], the historic dependency

[15], the degree heterogeneity [16], and so on. In particular, the correlated structures affect the structural robustness in diverse fashions: strong degree correlations across layers suppress susceptibility to a social cascade process [17] and be robust against targeted attacks [18]. For another branch of studies, attentions have shifted to understanding the dynamical process of interdependent networks by hidden geometric correlations [19–21]. The geometric correlation contains two parts: one, the radial correlation is equal to degree correlation, which has been widely discussed on its contribution to systems robustness; and two, the angular correlation is a novel statistical property. Angular correlations across layers can produce the lower outbreak threshold [21] and mitigate the breakdown of mutual connectivity under targeted attacks [20].

Even though the robustness of interdependent networks has received much research interest, few studies focus on interdependent directed networks. Taking the real-world scenes into consideration, network structures are generally asymmetric, which may cause a more enriched phenomenon in the critical behaviors of the robustness [22, 23]. For instance, different measures characterize the feature of nodes in directed systems: in-degrees, out-degrees, and their correlations (i.e., in-out degree correlations). The robustness of many real-world systems increases as the in-out degree correlations [22]. An open question is whether other correlations indexes affect the robustness of interdependent directed networks, even in the state of the high in-out degree correlations, or not?

Inspired by those studies, we argue for a need to study the robustness of interdependent directed networks in hyperbolic space. Here, we expand the concept of geometric correlations [19] to interdependent directed networks, defined as intra-layer geometric correlations which are derived from directed structures. Specifically, each layer of interdependent directed networks is represented by four hidden geometric features in hyperbolic space: in-radius, out-radius, in-angles, and out-angles [24]. To this end, intra-layer geometric correlations include intra-layer radial correlations (i.e., equivalent to in-out degree correlations) and intra-layer angular correlations. In this study, we will simulate and investigate the effects of intra-layer angular correlations on the robustness of artificial interdependent directed networks. Meanwhile, we analyze the intra-layer geometric correlation and its contribution to robustness in real-world systems by mapping interdependent directed networks into hyperbolic space.

This paper is structured as follows. **Section 2** introduces the basic knowledge, including hyperbolic embedding methods, cascading failure model, and artificial geometric model for interdependent directed networks. In **section 3**, we analyze the influence of intra-layer angular correlations on robustness in both artificial networks and real-world networks. **Section 4** concludes the paper finally.

2 MATERIALS AND METHODS

2.1 Interdependent Networks

Interdependent networks can be defined as a sequence of graphs: $G = \{G_A, G_B \ldots\}$. Usually, nodes in two or more monoplex networks are adjacent to each other *via* edges that are called dependency edges [1]. In our paper, interdependent directed networks contain two layers in terms of a layer A and a layer B, and each layer is a directed and unweighted scale-free network with the size $N_A = N_B = N$, as shown in **Figure 1**. Thus, the degree distributions of in-degree and out-degree are the power-law distribution in interdependent directed networks, where γ_{in} and γ_{out} are the power-law exponent of in-degree and out-degree, respectively. In Mathematics, it is sufficient to provide the adjacency matrix to formally characterize interdependent directed networks. For each layer (e.g., network A), and an asymmetric $N \times N$ matrix $\mathbf{A}$ whose generic entry $a_{ij} = 1$ if a link from node i to j exists, otherwise $a_{ij} = 0$.

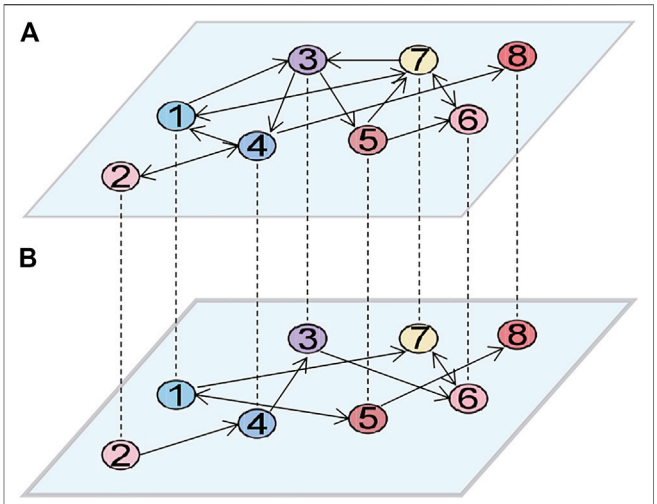


FIGURE 1 | Illustration of interdependent directed networks. Directed networks A and B are coupled by dependency links (dotted lines).

2.2 Cascading Failure Model

One may observe cascades in interdependent directed networks, i.e., avalanches of failures triggered by the failure of one or more nodes, as the nodes are removed gradually with a specific order K. K is defined by $K = max(k_A, k_B)$, where the degree of nodes in the network A or B are set by $k_A = k_{A,in} + k_{A,out}$ or $k_B = k_{B,in} + k_{B,out}$. In practice, we begin removing a fraction $1 - p$ in network A and a fraction $1 - p$ in network B, and removing all the links connected to these removed nodes. For interdependent nodes across layers, if node i fails to function due to being attacked or isolated, node i also fails in another layer. We continue this process until no further new failed nodes can occur.

To measure the robustness for interdependent directed networks under targeted attacks, we compute its mutually connected components (MCC) in each step of removing nodes with fraction $1 - p$. Each layer network fragments into MCC, within which each pair of nodes can reach each other by a path [7, 20]. Some nodes in the MCC of the layer A network will play an important function in the layer A network, but they may not exist in the MCC of layer B. Thus, we define the MCC of interdependent systems to be the average value of all layers. A similar definition also applies to calculate the second maximum connected component (2nd-MCC). By doing this, when the

reserved fraction p is tuned increasingly from zero to a unit, at a certain critical fraction p_c, the MCC of networks shifts from zero to non-zero. When $p < p_c$, the interdependent networks have no MCC, and otherwise $p > p_c$. The critical fraction p_c thus reveals the robustness of interdependent directed networks, i.e., the smaller p_c, the higher network robustness.

2.3 The Intra-layer Geometric Correlations

Intra-layer geometric correlations are composed of intra-layer radial correlations and intra-layer angular correlations in a certain layer, obtained by embedding interdependent directed networks into hyperbolic space. Therefore, we introduce the A-PSO (the asymmetric popularity and similarity optimization) model to map each layer of interdependent directed networks into hyperbolic space [24].

In this model, each node i is firstly split into two sets (a_i in the set a and b_i in the set b), and a directed link goes from a node i to a node j, which will be transformed a link between a_i and b_j. Then, each pair of nodes a_i and b_j correspond to polar coordinates $(\theta_{a,i}$ and $r_{a,i})$ and $(\theta_{b,i}$ and $r_{b,i})$, respectively. The radial coordinates can be calculated by $\kappa - r$ mapping: $r = R - 2ln(\kappa/\kappa_{min})$, where hidden variable $\kappa_{\star,i}(\star \in \{a, b\})$ is derived from $\rho(\kappa_\star) = (\gamma - 1)\kappa_{min}^{(\gamma-1)}\kappa_\star^{-\gamma}$, the minimum of hidden variable $\kappa_{min} = \bar{k}(\gamma_\star - 1)/(\gamma_\star - 2)$, and θ is drawn from uniform Probability Density Function (PDF). Finally, the directed link is created by any integrable function $f(\chi) = (1 + \chi^\beta)^{-1}$ in hyperbolic space, where hyperbolic distance $\chi = r_{a,i} + r_{b,j} + 2ln(d_{ai,bj}/2)$, β is a model parameter.

In practice, we do not know the nodes' coordinates by given the adjacency matrix $\mathbf{A}$ of a layer. We are interested in the conditional probability $\mathcal{P}(\theta, \kappa|A)$ that the possibility of assigning a coordinate to each node, giving our observed network data. Following Bayes' rule, we have

$$\mathcal{P}(\{\kappa, \theta\}|a_{ij}) \propto \mathcal{P}(a_{ij}|\{\kappa, \theta\})\mathcal{P}(\{\kappa, \theta\}). \tag{1}$$

where the posterior distribution $\mathcal{P}(\{\kappa, \theta\}|a_{ij})$ is proportional to two components: the likelihood $\mathcal{P}(a_{ij}|\{\kappa, \theta\})$ of the network data a_{ij}, the prior probability $\mathcal{P}(\{\kappa, \theta\})$ κ and θ are obtained by following some constraints mentioned above, and we write $P(\{\kappa, \theta\}) = 1$ if the constraint is satisfied and otherwise $P(\{\kappa, \theta\}) = 0$. Thus, the likelihood can be calculated as followed:

$$\mathcal{P}(a_{ij}|\{\kappa, \theta\}) = \prod_{1 \le i \ne j \le N} f(\chi)^{a_{ij}}[1 - f(\chi)]^{1-a_{ij}}, \tag{2}$$

where hidden variables are solved by $\kappa_i = k_i - \gamma_i\beta$ and angular coordinates are inferred by using the localized Metropolis-Hastings (LMH) algorithm [25, 26].

To this end, we have the angular coordinate $(\theta_a; \theta_b)$ and the radial coordinates $(r_a; r_b)$ in according with giving a directed network layer. Then, we use mutual information to describe intra-layer geometric correlations. Formally, the mutual information about two random various X, Y is obtained by [27].

$$I(X;Y) = \int_Y \int_X p(x, y) ln\left(\frac{p(x, y)}{p(x)p(y)}\right) dxdy, \tag{3}$$

where $p(x, y)$ is the joint probability density function of X, Y, and $p(x)$, $p(y)$ are marginal PDF of X and Y. In this paper, the intra-layer angular correlation of each layer is quantified by the normalized mutual information $NMI_\theta = I(\theta_a; \theta_b)/max\{I(\theta_a; \theta_a), I(\theta_b; \theta_b)\}$. Similarly, the intra-layer radial correlation is defined as $NMI_r = I(r_a; r_b)/max\{I(r_a; r_a), I(r_b; r_b)\}$. The higher the NMI ($NMI \in [0, 1]$), the stronger are the intra-layer geometric correlations.

2.4 Artificial Geometric Model

We simulate targeted attacks on artificial networks to investigate the relationship between the robustness and intra-layer angular correlations. The geometric multiplex model (GMM, Ref. [19]) is applied to generate the artificial undirected interdependent networks with across-layer geometric correlations. Inspired by it, we use this framework to develop a single-layer directed network with an intra-layer geometric correlation. The difference between the GMM and our work is that we aim to obtain the out-direction and the in-direction coordinates in a specific correlation. In **Figure 2**, each directed layer is generated according to the following steps:

Step 1. Determine the initial parameters: the network size N, the exponent β of the connection probability, the power-law exponent of out-degree γ_a, the power-law exponent of in-degree γ_b, the average degree $\bar{k}$, the intra-layer radial correlation $\nu \in [0, 1]$, and the intra-layer angular correlation $g \in [0, 1]$.

Step 2. Determine the hyperbolic coordinates with a certain correlation in each layer of interdependent directed networks.

First of all, each node is assigned in-direction hidden variables κ_b, θ_b in the set b, as sampled from $\rho(\kappa_b) = (\gamma_b - 1)\kappa_{b,min}^{(\gamma_b-1)}\kappa_b^{-\gamma_b}$ and uniform PDF, respectively.

Secondly, the out-direction angular coordinates are chosen from $\theta_a = mod[\theta_b + 2\pi l_i/N, 2\pi]$, where l_i is an arc length of radius R in a hyperbolic disc, which is satisfied by zero-mean truncated Gaussian PDF, defined as $f_\sigma = \frac{1/\sigma\phi(l/\sigma)}{\Phi(N/2\sigma)-\Phi(-N/2\sigma)}$, $\sigma = \sigma_0(1/g - 1)$, $\sigma_0 = min[100, N/4\pi]$. $\phi(x)$ is normal distribution. $\Phi(x)$ is the PDF of $\phi(x)$.

Thirdly, each node of out-direction radial coordinates r_a is assigned. Notice that r_a is taken the place of the hidden variables κ_a to implement the algorithm easily. Specifically, the κ_a is derived from the copulas function $C_\eta(F(\kappa_a), F(\kappa_b)) = e^{-[-ln(F(\kappa_b))^\eta + (-ln(F\kappa_a))^\eta]^{1/\eta}}$, where $F(\kappa_a) = 1 - \kappa_a^{(1-\gamma_a)}\kappa_{a,min}^{(\gamma_a-1)}$, $F(\kappa_b) = 1 - \kappa_b^{(1-\gamma_b)}\kappa_{b,min}^{(\gamma_b-1)}$, $\eta = 1/(1 - \nu)$, the minimum of hidden variable $\kappa_{a,min} = \bar{k}(\gamma_a - 1)/(\gamma_a - 2)$ and $\kappa_{b,min} = \bar{k}(\gamma_b - 1)/(\gamma_b - 2)$. We then transform hidden variables to radial coordinates $r_a = R - 2ln(\kappa_a/\kappa_{a,min})$ and $r_b = R - 2ln(\kappa_b/\kappa_{b,min})$.

In particular, when $g = 1$ and $\nu = 1$, the coordinates of each node is identical in the two directions (that is, $\theta_a = \theta_b$ and $\kappa_a = \kappa_b$, respectively), and a generated network degenerates into a undirected network. To overcome this problem, we regard $\nu = 0.99$ and $g = 0.99$ as the full correlations (i.e., $\nu = 1$ and $g = 1$) in this paper and make sure to generate a directed network.

Step 3. Determine the artificial networks. Links are created by the connection probability, i.e., each node pair i, j is connected by probabilities $f(\chi_{ij}) = (1 + \chi^\beta)^{-1}$, $\chi_{ij} = \frac{\Delta\theta N\bar{k}}{\beta sin(\pi/\beta)\kappa_{ia}\kappa_{jb}}$ and $\Delta\theta = |\pi - |\pi - |\theta_{ia} - \theta_{jb}||$. To do so, a layer of the artificial network has been constructed. The steps 1–3 are repeated to generate another layer.

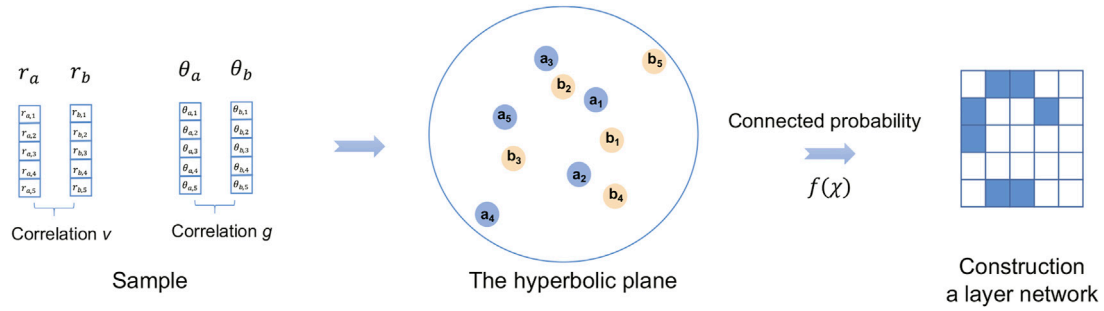


FIGURE 2 | The flow diagram of construction teach layer of artificial interdependent networks. Yellow nodes and blue nodes are represented in-direction nodes and out-direction nodes, respectively.

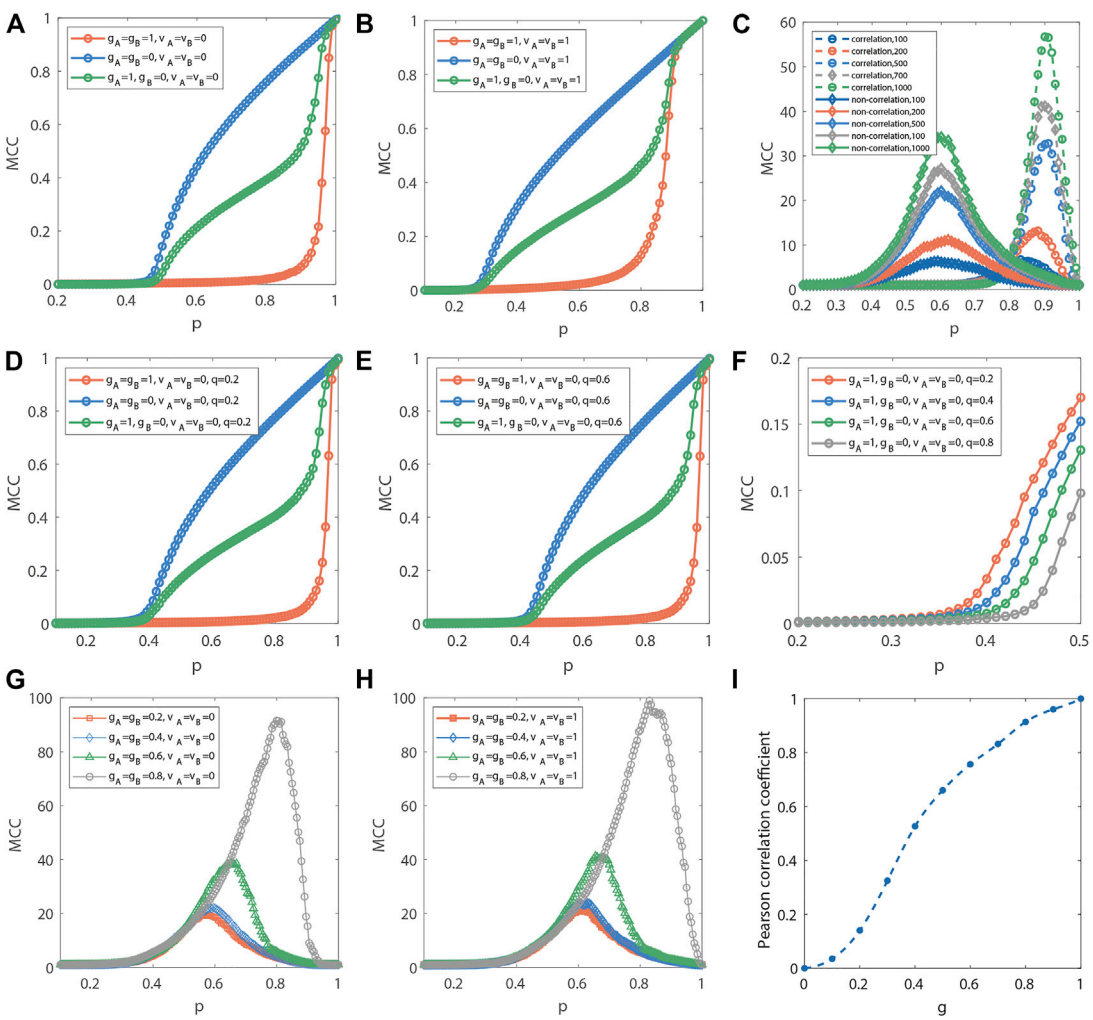


FIGURE 3 | Targeted attack in artificial networks. **(A,B)** Targeted attacks on different kinds of synthetic networks with N = 5,000. **(C)** The size of the 2nd-MCC as a function of p for different sizes N. we set $g_A = g_A = 1$, $r_A = r_A = 0$ in the correlation case and $g_A = g_A = 0$, $r_A = r_A = 0$ in the non-correlation case. **(D–F)** Targeted attacks on three kinds of synthetic networks with coupling strengths q. **(G,H)** Simulate targeted attack with different intra-layer angular correlations, and $N = 500$. The results are averages over 100 realizations. **(I)** illustrates the relationship between parameter g and Pearson correlation coefficient in the artificial model.

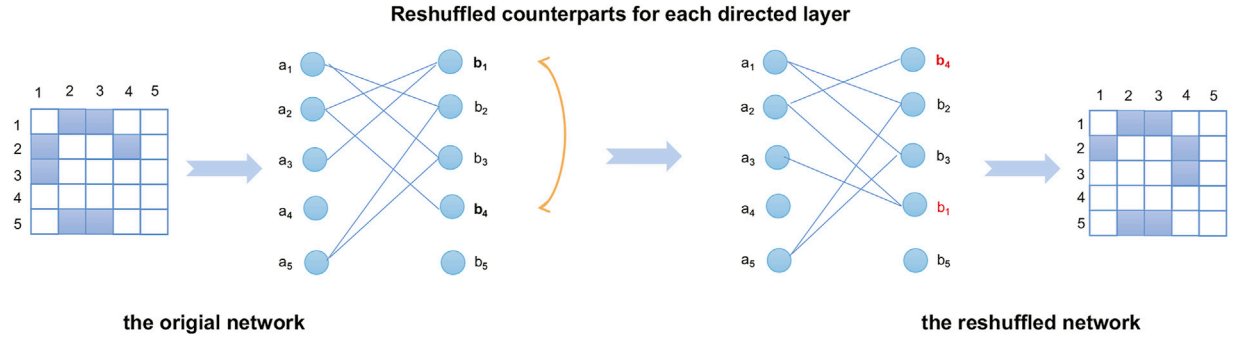


FIGURE 4 | Illustration of the reshuffled counterpart of original networks. In the example, we exchanged the ids of nodes b_1 and b_4, thereby destroying the intra-layer topological similarity.

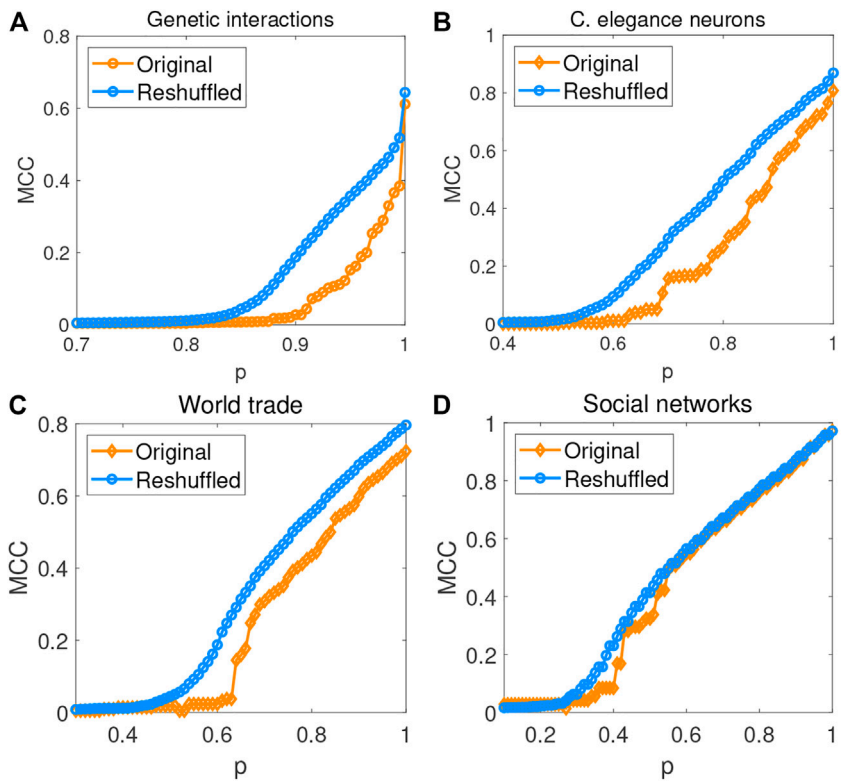


FIGURE 5 | The relative size of the MCC against the remaining fraction p of nodes remaining in the system for real interdependent directed networks, including genetic interactions networks **(A)**, C.elegance neurons networks **(B)**, world trade networks **(C)**, and social networks **(D)**. The orange line and the blue line represent the results of real-world networks (Original) and their reshuffled counterparts (Reshuffled), respectively.

3 RESULTS

3.1 The Influence of Intra-layer Angular Correlations on Robustness in Artificial Networks

In this section, all artificial networks are double-layer directed networks, where a pair of nodes across layers are interdependent. The artificial geometric model is used to generate each layer which is a heterogeneous directed network with the power-law exponent of out-degree $\gamma_a = 2.6$, the power-law exponent of in-degree $\gamma_b = 2.6$, average node degree $\bar{k} = 6$, and the parameter $\beta = 3.5$. The intra-layer angular correlation and the intra-layer radial correlation are denoted by the symbols (g_A, ν_A) in layer A and (g_B, ν_B) in layer B.

By doing this, three kinds of artificial networks have been generated to simulate targeted attacks, as shown in **Figures 3A,B**.

TABLE 1 | The basic properties of empirical directed networks. $NMI_{\theta,ori}$ and $NMI_{\theta,re}$ present the strength of the intra-layer angular correlation in original networks and reshuffled networks, respectively.

Data set	N	Link	$NMI_{\theta,ori}$	$NMI_{\theta,re}$
Social networks, *layerA* (*Advice*)	71	892	0.859	0.846
Social networks, *layerB* (*Co. – work*)	71	1,104	0.865	0.813
World trade, *layerA* (*Creamfresh*)	214	962	0.808	0.704
World trade, *layerB* (*Cheese*)	214	1,195	0.838	0.754
C.elegance neurons, *layerA* (*ElectrJ*)	281	1,032	0.886	0.874
C.elegance neurons, *layerB* (*PolySyn*)	281	950	0.831	0.725
Genetic interactions, *layerA* (*direct*)	1,449	2,499	0.718	0.629
Genetic interactions, *layerB* (*physical*)	1,449	2,205	0.640	0.539

Results reveal two geometric contributions to the robustness. One, the value of p_c in the orange line is larger than others, which shows that intra-layer angular correlations increase the vulnerability of interdependent directed networks. Notice that our results are in contrast to the situation on across-layer correlations between interdependent networks [20], which reveals that intra-layer angular correlations are hidden factors to understand complex systems. Two, such vulnerability will be exacerbated by the increase in the number of layers. Additionally, we also provide the behavior of cascading failures for the 2nd-MCC in different size systems. The largest 2nd-MCC achieves its extremum near the critical point, which is a way to estimate and compare p_c. **Figure 3C** illustrates the extreme value point p_c for interdependent directed networks with full angular correlations is always significantly higher than the case of the non-angular correlations. Multi-subsystem interaction and its hidden geometric structure thus should be considered designing network systems more robust. Additional, we analyze the fraction of coupling strength $q \in [0, 1]$, where $q = 0$ represents that network systems become two single and independent networks, and $q = 1$ represents the mapping relationship of nodes between two layers is one to one. **Figures 3D–F** illustrates that the results of **Figure 3A** can expand to general cases (the inter-layer coupling of arbitrary proportions). **Figure 3F** shows their percolation behaviors with the fraction of remaining nodes p changing from 0 to 1 under intra-layer angular correlations and different coupling strengths q. The results show that decreasing coupling strength can mitigate the vulnerability of interdependent directed networks with the intra-layer angular correlation against targeted attacks.

To study this issue further, we examine the impact of different angular correlations on robustness by several variations of artificial networks, as shown in **Figures 3G,H**. As intra-layer angular correlations decrease, the vulnerability of directed systems is mitigated, irrespective of the effect of intra-layer radial correlations. This means that, although the contribution of in-out degree correlations is positive to robustness for interdependent directed networks, intra-layer angular correlations play an essential factor in undermining the robustness. Thus, intra-layer angular correlations have an early-warming function when interdependent directed networks face a sudden extreme attack. In addition, we also found that such an increasing trend is not apparent in low-correlation situations. To analyze the cause, we checked the relationship between parameter g and the Pearson correlation between intra-layer angular coordinates. **Figure 3I** suggests that the nonlinear relationship induces the phenomenon mentioned above.

3.2 Linking Intra-layer Angular Correlations to Robustness in Real Interdependent Networks

The influence of intra-layer angular correlations on the robustness in real-world interdependent networks is simulated in this subsection. Empirical networks are all derived from open databases and describe in detail, as followed. 1) C. elegans neural dataset describes the neural interconnection *via* chemical synapses and gap junctions, which can be obtained from the Wormatlas database [28]. The nodes are neurons, and each layer corresponds to a different type of synaptic connection. 2) International trade dataset considers different types of trade relationships among countries, obtained from Ref. [29]. The worldwide food import/export network is an economic network in which layers represent products, nodes are countries, and edges at each layer represent import/export relationships of a specific food product among countries. Each layer is directed and weighted networks with 214 nodes. 3) Arabidopsis interdependent Genetic networks are obtained from the Biological General Repository for Interaction Datasets (BioGRID, thebiogrid.org), a public database that archives and disseminates genetic and protein interaction data from humans and model organisms [30, 31]. Each layer is directed and unweighted networks with 1,449 nodes after removing the isolated nodes. 4) Social networks consist of 3 kinds of (Co-work, Friendship, and Advice) between partners and associates of a corporate law partnership [32, 33]. Each layer is directed and unweighted networks.

Secondly, we construct reshuffled counterparts (so-called reshuffled networks) from real-world networks (so-called original networks). The reshuffled counterpart is a variant of the original network to alter intra-layer geometric correlations. Specifically, each layer (a directed network) is transformed into a bipartite structure, as shown in **Figure 4**, and randomly reshuffled nodes' ID of the set b in a way. Notably, interdependent nodes are also reshuffled in the same way in other layers if nodes' ID is reshuffled at a layer. Node b_1 and node b_4 are also reshuffled in layer B, when node b_1 and node b_4 are reshuffled in layer A, To this end, the reshuffled counterparts are destroyed the intra-layer geometric correlation and preserved across-layers geometric correlations.

Then, each layer for these networks can be embedded into a hyperbolic space, where each layer is represented by a group of angular coordinates (θ_a, θ_b) and a group of radial coordinates (r_a, r_b). To validate the influence of intra-layer geometric correlations on this real-world multiplex network, we implement targeted attacks on the original networks and reshuffled networks for empirical networks, respectively. **Figure 5** displays that the p_c of original networks is smaller than their reshuffled counterparts under targeted attacks. We also observe that the $NMI_{\theta,ori}$ is always larger than the $NMI_{\theta,re}$ for different real-world networks, as shown in **Table 1**. Linking those results, we find that the larger the value p_c, the stronger intra-layer angular correlations. It is the reason why interdependent directed

networks are more robust after the reshuffle. Results also suggest our arguments and highlight the importance of intra-layer angular correlations.

4 CONCLUSION

The hidden geometric structures of real-world networks provide a new perspective in revealing a relationship between topology and dynamical processes. Here, we examine the importance of intra-layer geometric correlations in understanding the robustness of interdependent directed networks from the perspective of hyperbolic embedding. For one thing, simulations are performed targeted attacks on artificial networks with diverse geometric correlations. Our main finding is that strong intra-layer angular correlations can quickly shift the sizes of the mutually connected components to fragmentation. The robustness will decrease as the increase in intra-layer angular correlations, even if in the case of in-out degree correlations. Couple strength q impacts the robustness: robustness of interdependent directed networks enhances as decrease of q. For another, we have studied two-layered empirical directed networks, validating that intra-layer geometric correlations also induce the vulnerability of real-world systems. Our results may help design a more robust network system and plan efficient protection strategies. However, it is also the beginning of clarifying the relationship between geometric structures and the dynamical process in interdependent directed networks. There are also some limitations in this work. For instance, the contribution of geometric correlations and coupling patterns across layers in the aspect of robustness has not yet been discussed. Exploring the failure mechanism of one-to-one correspondence nodes between layers may also offer new insights into studying the robustness of multilayer networks.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. These data can be found in **Section 3.2**.

AUTHOR CONTRIBUTIONS

ZNW performed the analysis, validated the analysis, and drafted the manuscript. ZRD and YF designed the research and reviewed the manuscript. All authors have read and approved the content of the manuscript.

FUNDING

This work was supported by the National Natural Science Foundation of China (Grant Nos. 71731002 and 61573065).

REFERENCES

1. Kivelä M, Arenas A, Barthelemy M, Gleeson JP, Moreno Y, and Porter MA. Multilayer Networks. *J complex networks* (2014) 2:203–71. doi:10.1093/comnet/cnu016
2. Boccaletti S, Bianconi G, Criado R, del Genio CI, Gómez-Gardeñes J, Romance M, et al. The Structure and Dynamics of Multilayer Networks. *Phys Rep* (2014) 544:1–122. doi:10.1016/j.physrep.2014.07.001
3. Wu Z, Di Z, and Fan Y. The Structure and Function of Multilayer Networks: Progress and Prospects. *J Univ Electron Sci Technol China* (2021) 50:106–20. doi:10.12178/1001-0548.2020068
4. Gómez S, Díaz-Guilera A, Gómez-Gardeñes J, Pérez-Vicente CJ, Moreno Y, and Arenas A. Diffusion Dynamics on Multiplex Networks. *Phys Rev Lett* (2013) 110:028701. doi:10.1103/PhysRevLett.110.028701
5. De Domenico M, Granell C, Porter MA, and Arenas A. The Physics of Spreading Processes in Multilayer Networks. *Nat Phys* (2016) 12:901–6. doi:10.1038/nphys3865
6. Wang W, Liu QH, Liang J, Hu Y, and Zhou T. Coevolution Spreading in Complex Networks. *Phys Rep* (2019) 820:1–51. doi:10.1016/j.physrep.2019.07.001
7. Buldyrev SV, Parshani R, Paul G, Stanley HE, and Havlin S. Catastrophic cascade of Failures in Interdependent Networks. *Nature* (2010) 464:1025–8. doi:10.1038/nature08932
8. Gao J, Buldyrev SV, Stanley HE, Xu X, and Havlin S. Percolation of a General Network of Networks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2013) 88:062816. doi:10.1103/PhysRevE.88.062816
9. Yuan X, Hu Y, Stanley HE, and Havlin S. Eradicating Catastrophic Collapse in Interdependent Networks via Reinforced Nodes. *Proc Natl Acad Sci USA* (2017) 114:3311–5. doi:10.1073/pnas.1621369114
10. Duan D, Lv C, Si S, Wang Z, Li D, Gao J, et al. Universal Behavior of Cascading Failures in Interdependent Networks. *Proc Natl Acad Sci U S A* (2019) 116:22452–7. doi:10.1073/pnas.1904421116
11. Reis SDS, Hu Y, Babino A, Andrade Jr JS, Canals S, Sigman M, et al. Avoiding Catastrophic Failure in Correlated Networks of Networks. *Nat Phys* (2014) 10:762–7. doi:10.1038/nphys3081
12. Parshani R, Buldyrev SV, and Havlin S. Interdependent Networks: Reducing the Coupling Strength Leads to a Change from a First to Second Order Percolation Transition. *Phys Rev Lett* (2010) 105:048701. doi:10.1103/PhysRevLett.105.048701
13. Sun J, Zhang R, Feng L, Monterola C, Ma X, Rozenblat C, et al. Extreme Risk Induced by Communities in Interdependent Networks. *Commun Phys* (2019) 2:1–7. doi:10.1038/s42005-019-0144-6
14. Shekhtman LM, Shai S, and Havlin S. Resilience of Networks Formed of Interdependent Modular Networks. *New J Phys* (2015) 17:123007. doi:10.1088/1367-2630/17/12/123007
15. Li M, Lü L, Deng Y, Hu M-B, Wang H, Medo M, et al. History-Dependent Percolation on Multiplex Networks. *Natl Sci Rev* (2020) 7:1296–305. doi:10.1093/nsr/nwaa029
16. Sun S, Wu Y, Ma Y, Wang L, Gao Z, and Xia C. Impact of Degree Heterogeneity on Attack Vulnerability of Interdependent Networks. *Sci Rep* (2016) 6:32983–9. doi:10.1038/srep32983
17. Kim JY, and Goh KI. Coevolution and Correlated Multiplexity in Multiplex Networks. *Phys Rev Lett* (2013) 111:058702. doi:10.1103/PhysRevLett.111.058702
18. Min B, Yi SD, Lee KM, and Goh KI. Network Robustness of Multiplex Networks with Interlayer Degree Correlations. *Phys Rev E Stat Nonlin Soft Matter Phys* (2014) 89:042811. doi:10.1103/PhysRevE.89.042811
19. Kleineberg K-K, Boguñá M, Ángeles Serrano M, and Papadopoulos F. Hidden Geometric Correlations in Real Multiplex Networks. *Nat Phys* (2016) 12:1076–81. doi:10.1038/nphys3812
20. Kleineberg KK, Buzna L, Papadopoulos F, Boguñá M, and Serrano MÁ. Geometric Correlations Mitigate the Extreme Vulnerability of Multiplex Networks against Targeted Attacks. *Phys Rev Lett* (2017) 118:218301. doi:10.1103/PhysRevLett.118.218301

21. Fan D, Jiang G-P, Song Y-R, and Zhang X. Influence of Geometric Correlations on Epidemic Spreading in Multiplex Networks. *Physica A: Stat Mech its Appl* (2019) 533:122028. doi:10.1016/j.physa.2019.122028
22. Liu X, Stanley HE, and Gao J. Breakdown of Interdependent Directed Networks. *Proc Natl Acad Sci USA* (2016) 113:1138–43. doi:10.1073/pnas.1523412113
23. Liu RR, Jia CX, and Lai YC. Asymmetry in Interdependence Makes a Multilayer System More Robust against Cascading Failures. *Phys Rev E* (2019) 100:052306. doi:10.1103/PhysRevE.100.052306
24. Wu Z, Di Z, and Fan Y. An Asymmetric Popularity-Similarity Optimization Method for Embedding Directed Networks into Hyperbolic Space. *Complexity* (2020) 2020(5):1–16. doi:10.1155/2020/8372928
25. Newman M, and Barkema G. *Monte Carlo Methods in Statistical Physics*. New York, USA: Clarendon Press (1999).
26. Boguñá M, Papadopoulos F, and Krioukov D. Sustaining the Internet with Hyperbolic Mapping. *Nat Commun* (2010) 1:62. doi:10.1038/ncomms1063
27. Kraskov A, Stögbauer H, and Grassberger P. Estimating Mutual Information. *Phys Rev E Stat Nonlin Soft Matter Phys* (2004) 69:066138. doi:10.1103/PhysRevE.69.066138
28. Varshney LR, Chen BL, Paniagua E, Hall DH, and Chklovskii DB. Structural Properties of the caenorhabditis Elegans Neuronal Network. *Plos Comput Biol* (2011) 7:e1001066. doi:10.1371/journal.pcbi.1001066
29. De Domenico M, Nicosia V, Arenas A, and Latora V. Structural Reducibility of Multilayer Networks. *Nat Commun* (2015) 6:6864. doi:10.1038/ncomms7864
30. Stark C, Breitkreutz BJ, Reguly T, Boucher L, Breitkreutz A, and Tyers M. Biogrid: A General Repository for Interaction Datasets. *Nucleic Acids Res* (2006) 34:D535–D539. doi:10.1093/nar/gkj109
31. De Domenico M, Porter MA, and Arenas A. Muxviz: A Tool for Multilayer Analysis and Visualization of Networks. *J Complex Networks* (2015) 3:159–76. doi:10.1093/comnet/cnu038
32. Lazega E. *The Collegial Phenomenon: The Social Mechanisms of Cooperation Among Peers in a Corporate Law Partnership*. Oxford: Oxford University Press (2001).
33. Snijders TAB, Pattison PE, Robins GL, and Handcock MS. New Specifications for Exponential Random Graph Models. *Sociological Methodol* (2006) 36: 99–153. doi:10.1111/j.1467-9531.2006.00176.x

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 18 October 2021
doi: 10.3389/fphy.2021.731941

Resilience of Nematode Connectomes Based on Network Dimension-reduced Method

Duan Dongli[1]*, *Wu Xixi*[1] and *Si Shubin*[2]

[1]School of Information and Control Engineering, Xi'an University of Architecture and Technology, Xi'an, China, [2]School of Mechanical Engineering, Northwestern Polytechnical University, Xi'an, China

The whole map of nematode connectomes provides important structural data for exploring the behavioral mechanism of nematodes, but to further reveal the functional importance and resilience pattern of nematode neurons, it is necessary to effectively couple the regulatory relationship between neurons and their topology. Here, with a typical signal excitation function we propose a model to capture the interacting relationship between the neurons, because a differential equation depicts the activity of a neuron, *n* neurons mean we need high-D differential equations to capture the neural network. With mean-field theory, we decouple this N-dimension question into a one-dimension problem mathematically. In our framework, we emphatically analyze the characteristics, similarities and differences of the structure and dynamical behaviors of the neuronal system for *Caenorhabditis elegans* and *Pristionchus pacificus*. The comparing results of simulating method and theoretical approach show that the most important homologous neurons between *C.elegans* and *P.pacificus* are I2 and NSM, which may lead to their different behavior characteristics of predation and prey. At the same time, we expect that the x_{eff} index can be used to reveal the importance of neurons for the functional evolution and degeneration of neural networks from a dynamic perspective. In the hermaphroditic and male *C.elegans*, we test the control level of the intermediate neuron groups over the output neuron groups and the single neuron. These results suggest that our theoretical approach can be used to reveal the effects of bio-connectivity groups, potentially enabling us to explore the interaction relationship of neural networks in humans and animals.

Keywords: resilience, mean-field theory, network dynamics, nematodes connectomes, neural networks

OPEN ACCESS

Edited by:
Haroldo V. Ribeiro,
State University of Maringá, Brazil

Reviewed by:
Bradly J Alicea,
Orthogonal Research and Education Laboratory, United States
Matjaž Perc,
University of Maribor, Slovenia

***Correspondence:**
Duan Dongli
mineduan@163.com

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *28 June 2021*
Accepted: *20 September 2021*
Published: *18 October 2021*

Citation:
Dongli D, Xixi W and Shubin S (2021) Resilience of Nematode Connectomes Based on Network Dimension-reduced Method. Front. Phys. 9:731941. doi: 10.3389/fphy.2021.731941

1 INTRODUCTION

Due to special physiological structure and easy modeling, nematode has become the primary model to reveal the neurons structure and functional mechanism for humans and animals [1, 2]. After four decades of exploration, nematodes are the first organisms, for which the wiring diagram of their entire nervous system has been mapped at the cellular level [3, 4]. Even Witvliet et al reconstructed full brain of eight isogenic *Caenorhabditis elegans* individuals across postnatal stages to investigate how it changes with age [5]. This contributes to a more detailed and accurate understanding and exploration of human and animal behavior at the neuronal level, as well as an analysis of the functional importance of individual neurons at the systemic level. Therefore, we coupled the structural information of the neuronal map of the nematode and the functional relationship

between the neurons, predicted the functional involvement of specific neurons or synapses in defined behavioral responses [6, 7].

Resilience is system's ability to retain its basic functionality while errors, failures and environmental changes occur, which universally presents in most dynamical systems [8]. Thanks to the rapid development of network theory, the description of the nonlinear dynamics that governs the interactions between the neurons have been extracted. According to external disturbance for neuron systems, deleting interneurons or synapses may disconnect the networks, or make a great impact on the individual behavior [9]. The methods to explore the nematode's resilience mainly can be divided into two categories. *1*) Biological experiments: such as the gene labeling and the neuron ablation. They can track some specific synapses or their function in detail. The labeling approach can capture the directionality of synaptic connections, and its quantitative analysis of synapse patterns display excellent concordance with electronic micrograph reconstructions [10, 11]. However, this approach takes a lot of energy and is not universal. *2*) Theoretical experiments: using different mathematical methods and engineering mechanisms, which can abstractly study the function of outstanding nodes in nematodes [12–16]. For example, according to the theory of symmetry group, they found that the symmetry of the neural network has directly biological significance, and its correctness can be strictly proved by using the mathematical form of symmetry group. This form makes it possible to understand the importance of the structure-function relationship [17]. In addition, Yan also applied network control principles to the connectomes, which reveals both neurons with known importance and neurons which was previously unknown [18]. Within a network control principle, they add input signal to control the output of neurons by a linear framework. The results remain reliable with a small amount of disturbance to the reference connectors, but large disturbances are likely to cause distortion.

Here we construct a framework to explore the resilience of nematode connectomes: we use the signal excitation model to describe and solve quantitatively structure-function relationship of the nematode, which combines the biological behavior with dynamic behavior. The application of signal excitation mode is key to revealing how different behaviors, which contributes to understand the mapping from network structure to function [19]. Since the network contains a large number of neurons, each activity of synapse node or neuron node can be seen as a solution of the high-D differential equations. However, calculating the stable state of the neural system could be difficult or almost impossible, especially when the system is large-scale. With a network dimension-reduction method, we can derive an effective one-dimensional dynamic model which captures the system function of the neural networks. Finally, we use a weighted average activity x_{eff} to measure the neural performance of the whole nematodes. Meanwhile, we introduce a weighted average connectivity β_{eff} to express the structural strength of the nematode neuron system.

With the application of our framework into the neuron networks of *P.pacificus* and *C.elegans*, the differences between the predator and prey behaviors of these two nematodes can be clearly quantified at the neural network level, and the key neurons leading to the differences in nematode behaviors can be easily identified as well. Similarly, for hermaphroditic and male *C.elegans*, we apply our approach to discuss the core control of the intermediate neuron groups to output neuron groups. Core control means that the interneurons have great influence over the output neurons or all the neurons after neuronal perturbation.

Actually, our approach is a general mathematical framework, which couples the complex structure of the system with the nonlinear activation function, and enriches the research methods for exploring the functional behaviors of nematode. We can reveal the underlying principle of the neural network in this way. In the future, our theoretical methods can be applied to more specific linkage groups, to do targeted quantitative research [20].

2 NEURAL MODEL AND NETWORK DIMENSION-REDUCED METHOD

2.1 Neural Dynamics Model

There are nonlinear regulation relationships between each synapse in neural networks. Taking hyperbolic tangent excitation function as an example in this paper, we give a neural network decoupling method with a general network structure. For the stimulation relationships between the trillions of neuron synapses in human brain or animals, it would enable the individuals show a much more complex nonlinear phenomenon of affine transformation. The activation function can be used to describe the coupling mechanism among synapses as

$$\frac{dx_i}{dt} = I - \frac{x_i}{R} + \frac{J}{2}\sum_{j=1}^{N} A_{ij}\left(1 + \tanh\left(n\left(x_j - \alpha\right)\right)\right), \tag{1}$$

Where, x_i describes the activity of the neuron i, I is the basal activity of the neurons, R is the inverse of the death rate, α is the firing threshold, and J is the maximal interaction strength between pair of neurons. The adjacency matrix A depicts the topology of the neuron networks. The coefficient n governs the steepness of the sigmoid function, analogously to the *Hill* coefficient n in gene regulatory networks [18]. Actually, the **Eq. 1** is made up of two parts: $I - \frac{x_i}{R}$ describes the growth rate of the neuron itself, $\frac{J}{2}\sum_{j=1}^{N} A_{ij}\left(1 + tanh\left(n\left(x_j - \alpha\right)\right)\right)$ describes the positive excitation effect of its neighbor neurons on neuron i.

2.2 Network Dimension-Reduced Method

When the system of **Eq. 1** tends to a relatively stable state, which means that the activities of the N individuals in the network are constant values, so the N-dimensional nonlinear rate equations all equal to 0. However, calculating the stable state of the system requires to solve the N-dimensional nonlinear rate equations numerically or analytically, which could be very difficult, or almost impossible especially when the system is large-scale. We present a new dimensionality reduction to explore the interactive relationship between neuronal connectomes for

nematodes with mean-field approximation. This approximation is exact in the limit where the node activities are uniformly distributed.

2.2.1 Theoretical Framework for Network Resilience

Once we get the value of x_i for the neuron i from the solutions of **Eq. 1**, we can quantify the performance and the connectivity strength of the neural networks with a weighted average metrics on the network topology following the way in [21]. Defining an operator for the degree sequence of A as

$$\Gamma(y) = \frac{1^\top A y}{1^\top A 1} = \langle y_{nn} \rangle = \frac{\langle s_j^{out} y_j \rangle}{\langle s_j^{out} \rangle}. \tag{2}$$

Here, y_i is a variable of neuron i, and y is the weighted average of all the neurons. s_j^{out} is the outdegree of neuron j. In contrast, s_i^{in} represents the indegree of neuron i. This operator is used to calculate the weighted average y over all nearest neighbor nodes of network A.

In order to simplify the N-dimension of **Eq. 1** and approximate it to 1D formalism, we use a mean field hypothesis. Here we define $I - \frac{x_i}{R}$ as $F(x_i)$, define $(1 + tanh(n(x_j - \alpha))$ as $G(x_i, x_j)$. Using $\Gamma(G(x_i, \mathrm{x})) \approx G(x_i, \Gamma(\mathrm{x}))$ approximate **Eq. 1**, we get

$$\frac{dx_i}{dt} = I - \frac{x_i}{R} + s_i^{\mathrm{in}} \frac{J}{2}(1 + \tanh(n(\Gamma(\mathrm{x}) - \alpha))). \tag{3}$$

For the states of all nodes in the system, **Eq. 3** can be rewritten by the Hadamard product as

$$\frac{d\mathrm{x}}{dt} = I - \frac{\mathrm{x}}{R} + s^{in} \circ \frac{J}{2}(1 + \tanh(n(\Gamma(\mathrm{x}) - \alpha))). \tag{4}$$

Where we used the Hadamard product $\circ$, namely $\mathrm{a} \circ \mathrm{b} = (\mathrm{a}_1\mathrm{b}_1, \ldots, \mathrm{a}_N\mathrm{b}_N)^{\mathrm{T}}$. **Eq. 4** is an equation composed of N dimensions. In order to reduce the dimensionality of this set of equations, we apply $\Gamma(\mathrm{x}) = \frac{1^T A \mathrm{x}}{1^T A 1}$ to both sides of **Eq. 4**, namely

$$\frac{\mathrm{d}\Gamma(\mathrm{x})}{dt} = \Gamma\left(I - \frac{\mathrm{x}}{R} + s^{in} \circ \frac{J}{2}(1 + \tanh(n(\Gamma(\mathrm{x}) - \alpha)))\right). \tag{5}$$

Using $\Gamma(F(\mathrm{x})) \approx F(\Gamma(\mathrm{x}))$ and $\Gamma(G(\mathrm{x}, \Gamma(\mathrm{x}))) \approx G(\Gamma(\mathrm{x}), \Gamma(\mathrm{x}))$, we get the equation

$$\frac{\mathrm{d}\Gamma(\mathrm{x})}{dt} = I - \frac{\Gamma(\mathrm{x})}{R} + \Gamma(s^{in}) \frac{J}{2}(1 + \tanh(n(\Gamma(\mathrm{x}) - \alpha))). \tag{6}$$

In the process of dimension reduction, we introduce two variables to describe the state of the system, where x_{eff} measures the neural performance of the whole nematodes, β_{eff} expresses the structural strength of the nematode neuron system,

$$x_{\mathrm{eff}} = \Gamma(\mathrm{x}) = \frac{1^T A \mathrm{x}}{1^T A 1}, \tag{7}$$

$$\beta_{\mathrm{eff}} = \Gamma(s^{\mathrm{in}}) = \frac{1^T A s^{\mathrm{in}}}{1^T A 1} = \frac{\langle s^{\mathrm{out}} s^{\mathrm{in}} \rangle}{\langle s \rangle}. \tag{8}$$

Lastly, we have successfully decouple this N-dimension question into a one-dimension problem mathematically. Bring **Eqs 7**, **8** into **Eq. 6**, one gets

$$\frac{dx_{\mathrm{eff}}}{dt} = I - \frac{x_{\mathrm{eff}}}{R} + \frac{J}{2}\beta_{\mathrm{eff}}(1 + \tanh(n(x_{\mathrm{eff}} - \alpha))). \tag{9}$$

Subsequently, when the system comes to a stable state, it is obvious that $\frac{dx_{\mathrm{eff}}}{dt} = 0$. Hence, we can further get that

$$\beta_{\mathrm{eff}}(x_{\mathrm{eff}}) = \frac{2}{J}\left(\frac{x_{\mathrm{eff}}}{R} - I\right)\frac{1}{1 + \tanh(n(x_{\mathrm{eff}} - \alpha))}. \tag{10}$$

Equation 10 describes the theoretical relationship between the topology of the neuron networks and its dynamical performance. Actually, by **Eq. 10** we have decoupled the complex system of **Eq. 1** into a 1D problem.

2.2.2 Simulation Method

From **Eq. 10**, we can obtain the theoretical curves of x_{eff} for β_{eff}. To verify the correctness of our dimension-reduced method for the system resilience of x_{eff}, we use the ODE45 function to solve the neural dynamics of **Eq. 1**, which can ensure we get the numerical results of x_i. Then, with the steady state vector **x** and **Eq. 2**, which can separate the system from the topology parameter β_{eff} and the behavior parameter x_{eff}. The steps to simulate the neural dynamics are following

1. use ODE45 function to solve **Eq. 1**. We can obtain the stable vector **x**. In our study we set $I = n = 2$, $R = \alpha = J = 1$. The setting of this parameter we refer to [16]. Assuming the network has N neurons, the solution of the steady state vector is $\mathbf{x} = [x_1, x_2, \ldots, x_N]$. It is easy to know that in the steady state vector, the value of column i represents the steady state activity x_i of neuron i.

2. compute the x_{eff} and β_{eff} from **Eq. 9**. For the vector **x** obtained in step 1 and the network indegree sequence s^{in}, we can get the system topology parameter β_{eff} and the behavior parameter x_{eff} with the operator $\Gamma(y)$.

3. compare the simulation results with the theoretical solutions. From the theoretical curve of **Eq. 10**, we test whether the simulation values of β_{eff} and x_{eff} fall on the theoretical curves. In our experiments, the simulation points agree well with the theoretical curve, which shows the feasibility of our approach.

2.3 Datasets for Neural Networks

In this study, we used two data sets: pharyngeal nervous systems of *C.elegans* and *P.pacifica* [22], all neuronal connections of hermaphrodite and male *C.elegans* [3]. The groundbreaking work of Cook and Bumbarger et al. provides a wealth data of neural networks, which can help explore the wiring problem from the perspective of structure. We want to couple the information of structure and dynamical function, so as to probe into the complex wiring problem of nematode from the network function and system resilience.

The connection matrix for pharyngeal nervous systems of *C.elegans* and *P.pacifica* was derived from the data set used by Bumbarger in his earlier work [22]. The matrix contains neuron connections and weights. The data and its experiment are used for homology comparison of two nematode in our study.

In fact, because of the complex wiring of the nematodes, their neurons have a precise functional grouping: input neuron, intermediate neuron, output neuron. So, for the dataset of

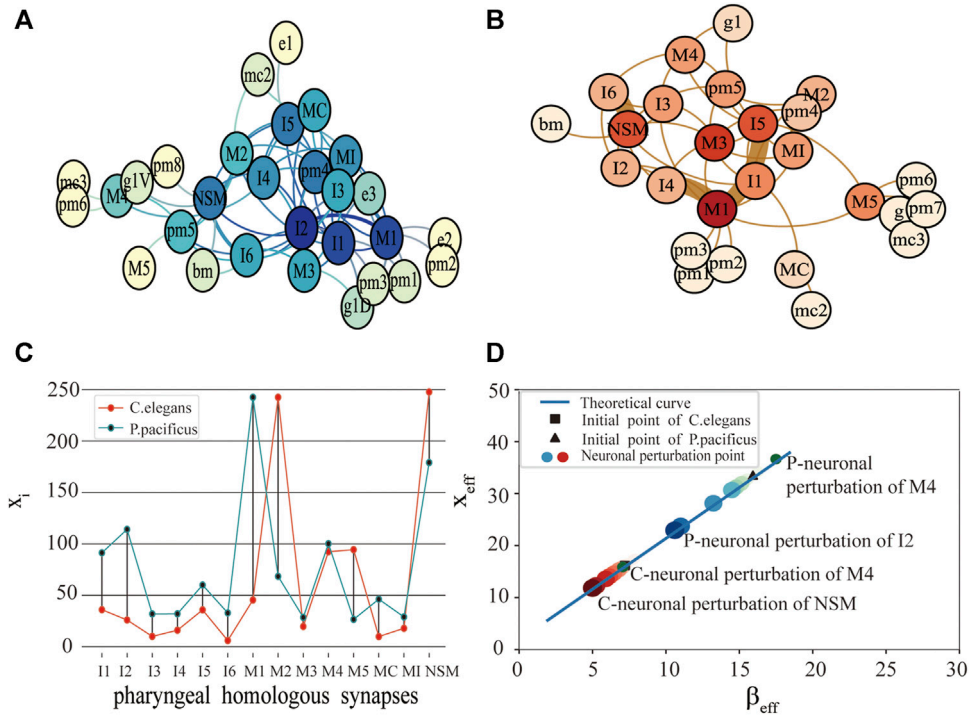


FIGURE 1 | Comparison of function and structure of synaptic connectivity in *C.elegans* and *P.pacificus*. **(A)** Neuron network for *P.pacificus*. **(B)** Neuron network for *C.elegans*. **(C)** Activity of 14 homologous synapses between *C.elegans* and *P.pacificus*. **(D)** System performance of *C.elegans* and *P.pacificus* while the neurons are disturbed. The red circles represent the system resilience of *C.elegans* while the homologous synapses are disturbed. The blue circles represent the system resilience of *P.pacificus*. The darker the color, the greater the effect of the neuronal perturbation.

hermaphrodite and male *C.elegans*, instead of focusing on the function of a single node in the nematode network, we focus on the influence of the intermediate neurons on the output neurons.

Connectome adjacency matrices of hermaphrodite and male *C.elegans* are gap junction, which were provided by Steven J. Cook [3]. Notably, they presented the complete wiring diagram of an animal nervous system for the first time in 2019, including adult *C.elegans* of both sexes. It is an important milestone in the field of neuron science. The data corresponding to one connectome has the following information: the node, the weight, neuron names in each group. e.g., InterNeurons contains all the neurons that belong to the "InterNeurons" group, neuron names in each subgroup, e.g., InterNeurons_1 contains all the neurons that belong to the "InterNeurons_1" subgroup of the "InterNeurons" group.

3 RESULTS

3.1 Resilience of *C.elegans* and *P.pacificus*

P.pacificus (**Figure 1A**) and *C.elegans* (**Figure 1B**) have highly similar synaptic structures, but quite different functions in the pharynx [23], we mainly explore the different connective structure and function in pharyngeal neurons.

We measured the functional differences of the connective structure for *C.elegans* and *P.pacificus* with x_i. As shown in **Figure 1C**, by exploring the impact of the 14 pharyngeal homologous neurons, we found that the values of M1 for *P.pacificus* and *C.elegans* show the greatest difference, which means that M1 is the most functionally different synapse between the two nematodes. M1 is a motor neuron, and their structure centralities of M1 in *C.elegans* and *P.pacificus* are quite similar [22]. Our framework can help identify the potential critical neurons, which may be inconsistent with the traditional structural comparison.

Then, with the framework we explored the differences of the predation behavior for the two nematodes through the system resilience index x_{eff}. As shown in **Figure 1D**, first of all, the activities of *C.elegans* and *P.pacificus* were in good agreement with our predicted theoretical curves. Secondly, we were awared that the x_{eff} of the *P.pacificus* simulation point is much higher than *C.elegans*. That is to say, the total activity of the *P.pacificus* is much higher than *C.elegans*. Nematode feeding strategies differ greatly [24, 25]. *P.pacificus* have a necromenic association with scarab beetles [22]. Their dauer larvae rest on the insect and resume development after the beetle's death to feed on microbes on the decaying carcass. *P.pacificus* can be easily cultured on bacteria [26], however, which is also predatory on other nematodes. In fact, the difference of predation strategy leads to the difference of neuron function. For example, differential but coordinated regulation of pm1 and pm3 in *P.pacificus* represents motor output that is specific to predatory feeding and does not exist in *C.elegans* [27, 28]. Actually, the key characteristic of *P.pacificus* is that it takes predation behavior actively for a long

time [29, 30], while the *C.elegans*, which is preyed on, just eats the food around it. Thus, from the neural level, we can conclude that the system resilience index x_{eff} could be used to reveal the essential differences of the predation behavior for the two nematodes that *C.elegans* are prey, and *P.pacificus* is more likely to be predators [31].

Thirdly, we tested 14 pharyngeal neurons, which showed that NSM and I2 are the neuron with the greatest reduction compared with the original simulation point in **Figure 1D**. It meant that NSM and I2 are the two most important homologous neurons. I2 is an interneuron, which play the role of coordinating corpus and tooth contractions during predation. I2 are more highly connected in *P.pacificus* and may function as network hubs. Although there are no more detailed studies showing the important function of NSM neurons, the high impact of which on the system resilience in our results is sufficient for further attention of biological experiments. Compared with Bumbarger's earlier biological experiments [22], the difference is that they concluded that I1 and I2 are the most important candidate neurons from the view of the system structure, but we found NSM and I2 are the two most important homologous neurons while considering the synaptic structural and functional characteristics simultaneously.

In addition, a phenomenon occurs in our experiment from **Figure 1D**, after neuronal perturbation (node deleting) of a few homozygous neurons, the x_{eff} of *P.pacificus* decreased, but x_{eff} of *C.elegans* increased. M4 is one of these special neurons. With its necromenic beetle association, *P.pacificus* has an intermediate position between the microbivorous *C.elegans* and true parasites [32, 33]. In other words, *C.elegans* are prey and *P.pacificus* is more likely to be predators. As one of the important feeding neurons in the pharynx, M4 is closely related to predation strategy. So we made a bold guess that M4 may degenerate in *P.pacificus*, but evolve in *C.elegans*. More details in the Discussion.

3.2 Quantitative Analysis of Control Model in Hermaphrodite and Male *C.elegans*

From the point of dynamics, the three-layer classification of neurons provides a good basis for the discussion of control. Here we *see* sensory neurons as input neurons, muscle neurons as output neurons, and other categories as intermediate neurons. We explore the control of the intermediate neurons over the output neurons.

At the beginning, we want to find a class of intermediate neurons that have core control over input neurons. Then, we can further get which of the intermediate neurons has the highest level of control. The control level is described by x_i. The interneurons ultimately serve all the neurons in the system, so we also explore the control of the intermediate neurons over all the neurons. In our experiment, aiming at a group of output neurons or all neurons, if a group of interneurons are removed, we should firstly calculate the x_i, the one changes greatest, indicating that the interneurons have core control level over the output neurons or all the neurons.

Originally, We found the intermediate neurons group with the greatest control over the output neuron group. For hermaphrodite *C.elegans*, there are two types of output neurons: SexSpecificCells-Muscle and BodyWallMuscles. As shown in **Figure 2A**, after perturbation of the OtherEndOrgan intermediate neurons, the x_i of the SexSpecificCells-Muscle have dropped mostly, this is to say, the OtherEndOrgan intermediate neurons have the maximum control level over the SexSpecificCells-muscle output neurons. By contrast, after perturbing of the intermediate neurons, the x_i of the BodyWallMuscles changes barely, which means that the intermediate neurons have no control over the BodyWallMuscles output neurons. Male *C.elegans* also has two output neurons: SexSpecificCells-BodyWallMuscles and SexSpecificCells-Muscle. As shown in **Figure 2C**, when perturbing the Sex-OtherOrgan intermediate neurons, the x_i of the SexSpecificCells-BodyWallMuscles and the SexSpecificCells-Muscle both decease sharply, so the sex-OtherOrgan intermediate neurons have the maximum control over the SexSpecificCells-BodyWallMuscles output neurons, and also have the maximum control over the SexSpecificCells-Muscle output neurons. The final result is shown in a three-layer model, as shown in **Figures 2B–D**.

As shown in **Figure 2A**, in hermaphrodite *C.elegans*, no matter removing which group of interneurons, the line at the bottom of the **Figure 2A** is always stable, which means that the x_i of the BodyWallMuscles is steady. When removing the OtherEndOrgan intermediate neurons, what stands out in our results is the x_i of whole neurons (green line) decreases mostly. However, in **Figure 2C**, for the sexOtherorgan intermediate neurons in male *C.elegans*, all line corresponding to the sexOtherorgan drop sharply, which both have great effect on the neural network and the output neurons. As a result, we conclude that although these intermediate neurons have no direct control over the output neurons, they still play an important role in the overall functional mechanism of *C.elegans*. Hence, even though there is no decrease in the activity of the output neurons after the ablation experiment, the average activity of all neurons decreases significantly. In other words, the control mechanism over the output neurons and the whole neurons are not congruent.

Ultimately, we try to identify the intermediate neurons group with the greatest control level. We measure the neuron disturbance by degree in the intermediate group with core control, and calculate the effect of neuron control by the change of the mean value of x_i. In **Figure 3**, the neurons in Y-coordinate are arranged in degrees. As can be seen from the **Figure 3A**, in the case of male *C.elegans*' sexOtherorgan intermediate group of neurons, the value decreases mostly after the removal of CEPshVR neurons. So CEPshVR has the maximum control over the SBmuscle output neurons group. As shown in **Figure 3C**, the value in male *C.elegans*' sexOtherorgan intermediate neurons decreases sharply with the disturbance of Int neurons. Consequently, the Int neurons have the maximum control over the Smuscle output neurons group. Similarly, as shown in **Figure 4A**, in the case of hermaphrodite *C.elegans*' OtherEndOrgan intermediate neurons, the HSNR neurons have the maximum control over the sexspecificcells-muscle output neurons group. Briefly, for most of the interneuron groups, the

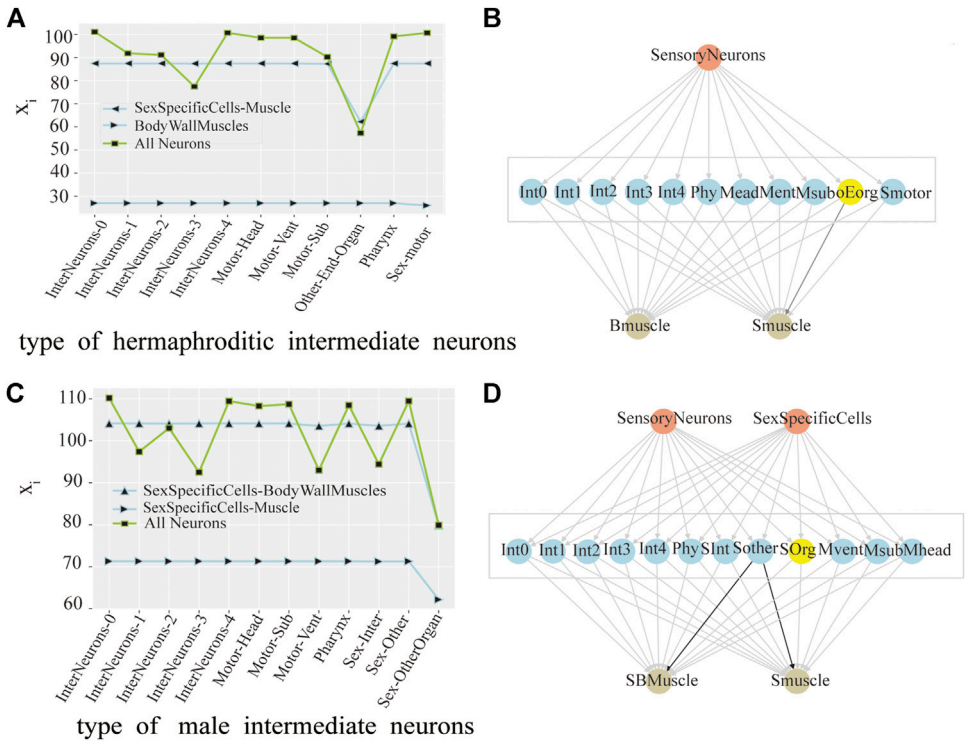


FIGURE 2 | Control analysis of neuron group in hermaphrodite and male *C.elegans*. **(A)** Line chart of the change of the average activity by neuronal perturbation of the each interneurons group in hermaphroditic *C.elegans*. (pink as the input neuron, blue as the intermediate neuron, and yellow as the output neuron, same as below). **(B)** Model of the interneurons group with core control in hermaphroditic *C.elegans*. The groups of interneurons with maximum control were marked with yellow color, same as below. **(C)** Line chart of the change of the average activity by neuronal perturbation of the each interneurons group in male *C.elegans*. **(D)** Model of the interneurons group with core control in male *C.elegans*.

higher the degree, the bigger circle in **Figures 3**, **4**, the greater the controlling impact. To illustrate more clearly, we mark in **Figures 3B,D**, **4B**, The gray area in the middle displays the specific neurons of the interneuron group, where the neurons of the core control level are marked in yellow.

4 DISCUSSION

In our framework, the coupling method of network structure and dynamical interactions enables us to establish a dynamical model of neuron networks to explore the system performance. To quantitatively solve the high-dimension rate equations, we provide a way in which multi-dimensional features between neurons can be reduced into one-dimension equation. Our approach can help the realization of the mapping from structure to function, and the quantitative measurement from function to control for neuron systems.

Excepting this, we noticed that x_{eff} of the *P.pacificus* simulation point is much higher than *C.elegans*. With its necromenic beetle association, *P.pacificus* has an intermediate position between the microbivorous *C.elegans* and true parasites [34, 35]. The omnivorous feeder *P.pacificus* should have the most complex metabolic pathways for nutrition and protection against defense and prey, comparing with the microbivorous *C.elegans* [36, 37]. So we infer that the essence of this phenomenon is the distinction of predation behavior caused the difference of synaptic connection, which changes the structure of nematode network.

Furthermore, we hope that our research could be used to illustrate evolution and degeneration of neuron: M4 most likely degenerates in *C.elegans*, evolve in *P.pacificus*. Combining the differences in the two nematode predation strategies, and the functions of M4, our evidence is as follows: M4 are known to be one of the major excitatory neurons in *C.elegans*, which is required for posterior isthmus peristalsis [38–40], it meant that M4 plays a crucial role in the act of eating or swallowing in *C.elegans*. However, the ablation experiments made by Edelman and Garry have shown that MC are the only neurons required for rapid eating in *P.pacificus*. But the ablation of other cholinergic pharyngeal neurons, such as M2S and M4, only slightly reduced feeding rates [41, 42]. In addition, Trojanowski's previous results demonstrate that this robust and evolutionarily adaptable network is highly degenerate at both the neural and genetic levels, the same behavior can be stimulated by multiple neurons and different types of receptors [41]. Avery and Horvitz even found out, in the *C.elegans* gene ced-3 Mutant, probably MSpaaaaap (the sister of M4), can sometimes take over M4's function. Using a laser microbeam to kill cells, they found that one of the extra cells in ted-3 worms,

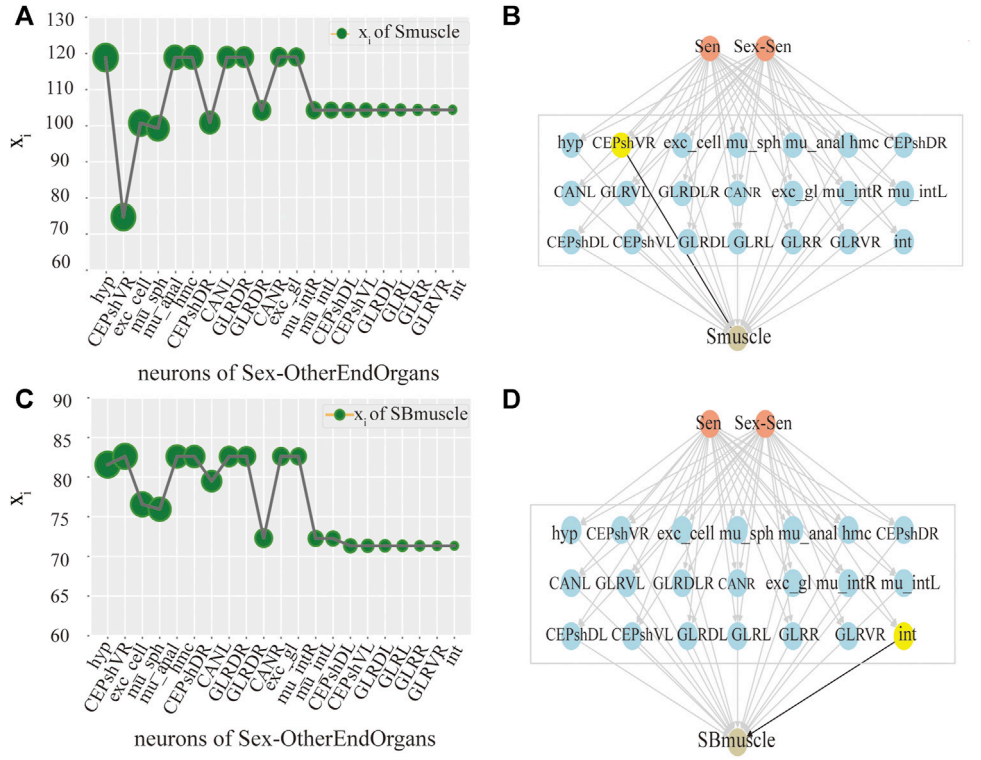


FIGURE 3 | Control analysis of single neuron in male *C.elegans*. **(A)** Activity line chart of SBmuscle, after neuronal perturbation of the Sexotherorgan intermediate neuronal group in the male *C.elegans* by degree. Degree refers to the degree of the node in this nematode network, we calculated degree and sorted them. The order is shown in figure: The size of the green circle represents the size of degree, same as below. **(B)** Control model of SBmuscle by the Interneuron group of Sexotherorgan. The neurons with maximum control are shown in yellow color, same as below. **(C)** Activity line chart of Smuscle, after neuronal perturbation of the Sexotherorgan intermediate neuronal group in the male *C.elegans* by degree. **(D)** Control model of Smuscle by the Interneuron group of Sexotherorgan. (SensoryNeurons:Sen; SexSpecificCells-SensoryNeuron:Sex-Sen; SexSpecificCells -InterNeurons:Sex-Inter; SexSpecificCells -OtherEndorgans: Sex- OtherEndOrgans. Same as the others).

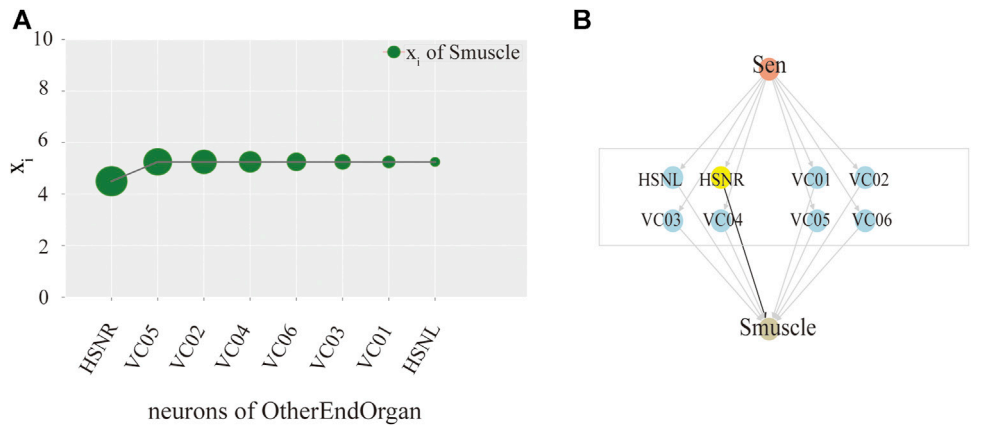


FIGURE 4 | Model exploration of single neuron hermaphroditism in *C.elegans*.**(A)** Activity line chart of SexSpecficalCells-muscle, after neuronal perturbation of the SexSpecficalCells-motor intermediate neuronal group in the hermaphroditism *C.elegans* by degree. **(B)** Control model of SexSpecficalCells-muscle by the Interneuron group of SexSpecficalCells-motor.

tentatively identified as MSpaaaaap, could become a functioning M4 neuron about half of the time, although it rarely or never fully replaced M4 [38]. Given the above, we can not be absolutely sure that M4 most likely degenerates in *C.elegans*, evolve in *P.pacificus*, but we hope our theoretical framework can help explore the function of neurons in the evolution and degeneration process.

To illustrate the power of our framework, we analyzed the control model of hermaphroditic and male *C.elegans*. Based on the data of Cook et al [3], our experiment abstracted the neuron connection group from the real network to the theory level by a nonlinear dynamical model, and obtained a measurable control index of the intermediate neurons to the output neurons. The control between different functional groups need to take into account both structural and functional characteristics. It means that our framework may help design more targeted and accurate biological ablation experiments. To understand vividly, we mapped the control model of the three-layer neurons, which is accurate to the individual neurons [43, 44].

In sum, our theoretical research perfects the exploration of the functional structure of nematodes, and breaks the limitation of analyzing the function and control ability from the structure. Comparing with the linear control model to predict motor neuron controllability, Yan et al. use network control principles, we emphasize the growth rate of the node itself and the influence of its neighbors on the node [18, 45] Importantly, this is a more efficient way to quickly target groups of neurons, even individual neurons or synapses that have core controlling power. In this view, our theoretical approach contributes to exploring the importance and the evolution mechanism of the individual neurons, and proves how to calculate the control level with the dynamics. These observations are not limited to nematode, but are also applicable to connectome model organism with complete data and clear background. However, the real interactions of nematode connection network are much more complicated than our dynamical model [46, 47]. We use this model for theoretical exploration, there may be some difference between our parameter setting and the real system. We need to refer to more biological experiments for further parameter setting and to use more complex dynamical equations or generative models to capture the interactions in our next work.

DATA AVAILABILITY STATEMENT

The datasets presented in this study can be found in online repositories. The names of the repository/repositories and accession number(s) can be found below: https://doi.org/10.1016/j.cell.2012.12.013 and https://doi.org//10.1038/s41586-019-1352-7.

AUTHOR CONTRIBUTIONS

DD and WX performed the analysis. WX validated the analysis and drafted the manuscript. DD and SS reviewed the manuscript. WX designed this study. All authors have read and approved the content of the manuscript.

FUNDING

This work was supported by the National Natural Science Foundation of China (projects no. 72071153, the Natural Science Foundation of Shaanxi Province (project n.2020JM-486), the China Postdoctoral Science Foundation (project n.2017M613336).

REFERENCES

1. Dirven L, Petersen M, Petersen MA, Aaronson NK, Chie W-C, Conroy T, et al. Development and Psychometric Evaluation of an Item Bank for Computerized Adaptive Testing of the Eortc Insomnia Dimension in Cancer Patients (Eortc Cat-Sl). *Appl Res Qual Life* (2019) 16:827–44. doi:10.1007/s11482-019-09799-w
2. Bargmann CI. Genetic and Cellular Analysis of Behavior in C. Elegans. *Annu Rev Neurosci* (1993) 16:47–71. doi:10.1146/annurev.ne.16.030193.000403
3. Cook SJ, Jarrell TA, Brittin CA, Wang Y, Bloniarz AE, Yakovlev MA, et al. Whole-animal Connectomes of Both *Caenorhabditis elegans* Sexes. *Nature* (2019) 571:63–71. doi:10.1038/s41586-019-1352-7
4. Sarma GP, Lee CW, Portegys T, Ghayoomie V, Jacobs T, Alicea B, et al. Openworm: Overview and Recent Advances in Integrative Biological Simulation of *Caenorhabditis elegans*. *Philos Trans R Soc Lond B Biol Sci* (2018) 373(1758):20170382. doi:10.1098/rstb.2017.0382
5. Witvliet D, Mulcahy B, Mitchell JK, Meirovitch Y, Berger DR, Wu Y, et al. Connectomes Across Development Reveal Principles of Brain Maturation. *Nature* (2021) 596:257–61. doi:10.1038/s41586-021-03778-8
6. Morita S, Oshio K-i., Osana Y, Funabashi Y, Oka K, and Kawamura K. Geometrical Structure of the Neuronal Network of *Caenorhabditis elegans*. *Physica A: Stat Mech its Appl* (2001) 298:553–61. doi:10.1016/s0378-4371(01)00266-7
7. Alicea B. Raising the Connectome: The Emergence of Neuronal Activity and Behavior in *Caenorhabditis elegans*. *Front Cel Neurosci* (2020) 14(524791):524791. doi:10.3389/fncel.2020.524791
8. Duan D, Lv C, Si S, Wang Z, Li D, Gao J, et al. Universal Behavior of Cascading Failures in Interdependent Networks. *Proc Natl Acad Sci USA* (2019) 116:22452–7. doi:10.1073/pnas.1904421116
9. Chen BL, Hall DH, and Chklovskii DB. Wiring Optimization Can Relate Neuronal Structure and Function. *Proc Natl Acad Sci* (2006) 103(12):4723–8. doi:10.1073/pnas.0506806103
10. Lav R, Varshney LB, Chen EP, Hall DH, and Chklovskii DB. Structural Properties of the *Caenorhabditis elegans* Neuronal Network. *PLoS Comput Biol* (2011) 7(2):e1001066. doi:10.1371/journal.pcbi.1001066
11. Chalfie M, Sulston J, White J, Southgate E, Thomson J, and Brenner S. The Neural Circuit for Touch Sensitivity in *Caenorhabditis elegans*. *J Neurosci* (1985) 5(4):956–64. doi:10.1523/jneurosci.05-04-00956.1985
12. Costa AC, Ahamed T, and Stephens GJ. Adaptive, Locally Linear Models of Complex Dynamics. *Proc Natl Acad Sci U S A* (2019) 116(5):1501–10. doi:10.1073/pnas.1813476116
13. Baltzley MJ, Gaudry Q, and Kristan WB. Species-specific Behavioral Patterns Correlate with Differences in Synaptic Connections Between Homologous Mechanosensory Neurons. *J Comp Physiol A* (2010) 196(3):181–97. doi:10.1007/s00359-010-0503-y
14. Liu Y, Sanhedrai H, Dong GG, Shekhtman LM, Wang F, Buldyrev SV, et al. Efficient Network Immunization Under Limited Knowledge. *Natl Sci Rev* (2020) doi:10.1093/nsr/nwaa229
15. Dong G, Wang F, Shekhtman L, Danziger M, Fan J, Du R, et al. Optimal Resilience of Modular Interacting Networks. *Proc Natl Acad Sci* 118(22):e1922831118. doi:10.1073/pnas.1922831118
16. Morone F, Del Ferraro G, and Makse HA. The K-Core as a Predictor of Structural Collapse in Mutualistic Ecosystems. *Nat Phys* (2018) 15:95–102. doi:10.1038/s41567-018-0304-8
17. Morone F, and Makse HA. Symmetry Group Factorization Reveals the Structure-Function Relation in the Neural Connectome of *Caenorhabditis elegans*. *Nat Commun* (2019) 10(1):4961. doi:10.1038/s41467-019-12675-8
18. Yan G, Vértes PE, Towlson EK, Chew YL, Walker DS, Schafer WR, et al. Network Control Principles Predict Neuron Function in the *Caenorhabditis*

elegans Connectome. *Nature* (2017) 550(7677):519–23. doi:10.1038/nature24056
19. Blaxter ML, De Ley P, Garey JR, Liu LX, Scheldeman P, Vierstraete A, et al. A Molecular Evolutionary Framework for the Phylum Nematoda. *Nature* (1998) 392:71–5. doi:10.1038/32160
20. Duan D-L, Tao C, Wu X-X, Wu C, Shu-bin S, and Gen-qing B. Identification of Unstable Individuals in Dynamic Networks. *Chin Phys B* (2021) 30(9):090501. doi:10.1088/1674-1056/abe92f
21. Gao J, Barzel B, and Al B. Universal Resilience Patterns in Complex Networks. *Nature* (2016) 530(7590):307–12. doi:10.1038/nature16948
22. Bumbarger DJ, Riebesell M, Rödelsperger C, Sommer RJ, and Sommer RJ. System-wide Rewiring Underlies Behavioral Differences in Predatory and Bacterial-Feeding Nematodes. *Cell* (2013) 152(1):109–19. doi:10.1016/j.cell.2012.12.013
23. Franks CJ, Holden-Dye L, Bull K, Luedtke S, and Walker RJ. Anatomy, Physiology and Pharmacology of *Caenorhabditis elegans* Pharynx: A Model to Define Gene Function in a Simple Neural System. *Invert Neurosci* (2006) 6(3):105–22. doi:10.1007/s10158-006-0023-1
24. Mörck C, Axäng C, and Pilon M. A Genetic Analysis of Axon Guidance in the C Elegans Pharynx. *Dev Biol* (1200) 260:158–75. doi:10.1016/s0012-1606(03)00238-0
25. Pilon M. Developmental Genetics of the Caenorhabditis Elegans pharynx. *Wires Dev Biol* (2014) 3:263–80. doi:10.1002/wdev.139
26. Gruninger TR, Gualberto DG, LeBoeuf B, and Garcia L. Integration of Male Mating and Feeding Behaviors in *Caenorhabditis elegans*. *J Neurosci* (2006) 26:169–79. doi:10.1523/jneurosci.3364-05.2006
27. Avery L, and You YJ. *C. elegans* Feeding. *WormBook* (2012) 1–23:1–23. doi:10.1895/wormbook.1.150.1
28. Avery L, and Horvitzt HR. Pharyngeal Pumping Continues After Laser Killing of the Pharyngeal Nervous System of *C. elegans*. *Neuron* (1989) 3:473–85. doi:10.1016/0896-6273(89)90206-7
29. Pervezand Rashid. Attraction of Allodorylaimus americanus (Nematoda: Dorylaimida) towards different prey nematodes and factors influencing this attraction. *Archives of Phytopathology and Plant Protection* 42:344–351. doi:10.1080/03235400601070421 (2009).
30. Lichtman JW, Livet J, and Sanes JR. A Technicolour Approach to the Connectome. *Nat Rev Neurosci* (2008) 9(6):417–22. doi:10.1038/nrn2391
31. Haspel G, O'Donovan MJ, and Hart AC. Motoneurons Dedicated to Either Forward or Backward Locomotion in the Nematode *Caenorhabditis elegans*. *J Neurosci* (2010) 30(33):11151–6. doi:10.1523/jneurosci.2244-10.2010
32. Albertson D, and Thomson JN. The Pharynx of *Caenorhabditis elegans*. *Phil Trans R Soc Lond B* (1976) 275:299–325. doi:10.1098/rstb.1976.0085
33. Sherman D, and Harel D. *Deciphering the Underlying Mechanisms of the Pharyngeal Motions in* Caenorhabditis elegans. Ithaca, NewYork: Neurons and Cognition (2019).
34. Mapes CJ. Structure and Function in the Nematode Pharynx. *Parasitology* (1965) 55:583–94. doi:10.1017/s0031182000069286
35. Mayer WE, Herrmann M, and Sommer RJ. Phylogeny of the Nematode Genus Pristionchus and Implications for Biodiversity, Biogeography and the Evolution of Hermaphroditism. *BMC Evol Biol* (2007) 7:104. doi:10.1186/1471-2148-7-104
36. Dieterich C, Clifton SW, Schuster LN, Chinwalla A, Delehaunty K, Dinkelacker I, et al. The *Pristionchus Pacificus* Genome Provides a Unique Perspective on Nematode Lifestyle and Parasitism. *Nat Genet* (2008) 40:1193–8. doi:10.1038/ng.227
37. Stern S, Kirst C, and Bargmann CI. Neuromodulatory Control of Long-Term Behavioral Patterns and Individuality across Development. *Cell* (2017) 171:1649–62. doi:10.1016/j.cell.2017.10.041
38. Avery L, and Horvitz HR. A Cell that Dies During Wild-type *C. elegans* Development Can Function as a Neuron in a Ced-3 Mutant. *Cell* (1987) 51(6):1071–8. doi:10.1016/0092-8674(87)90593-9
39. Avery L, and Horvitzt HR. Pharyngeal Pumping Continues After Laser Killing of the Pharyngeal Nervous System of *C. elegans*. *Neuron* (1989) 3(4):473–85. doi:10.1016/0896-6273(89)90206-7
40. Wicks S, and Rankin C. Integration of Mechanosensory Stimuli in *Caenorhabditis elegans*. *J Neurosci* (1995) 15(3):2434–44. doi:10.1523/jneurosci.15-03-02434.1995
41. Trojanowski NF, Padovan-Merhar O, Raizen DM, and Fang-Yen C. Neural and Genetic Degeneracy Underlies *Caenorhabditis elegans* Feeding Behavior. *J Neurophysiol* (2014) 112(4):951–61. doi:10.1152/jn.00150.2014
42. Rudiger B, Colomb J, Pankratz B, Schröck A, and Stocker RF Genetic Dissection of Neural Circuit Anatomy Underlying Feeding Behavior Indrosophila: Distinct Classes Ofhugin-Expressing Neurons. *J Comp Neurol* (2007) 502(5):848–56. doi:10.1002/cne.21342
43. Whalen AJ, Brennan SN, Sauer TD, and Schiff SJ. Observability and Controllability of Nonlinear Networks: The Role of Symmetry. *Phys Rev X* (2015) 5:011005. doi:10.1103/PhysRevX.5.011005
44. Tsalik EL, and Hobert O. Functional Mapping of Neurons that Control Locomotory Behavior in Caenorhabditis Elegans. *J Neurobiol* (2003) 56(2):178–97. doi:10.1002/neu.10245
45. Gao J, Liu YY, D'Souza RM, and Barabási AL. Target Control of Complex Networks. *Nat Commun* (2014) 5:5415. doi:10.1038/ncomms6415
46. Stephens GJ, Johnson-Kerner B, Bialek W, and Ryu WS. Dimensionality and Dynamics in the Behavior of *C. elegans*. *Plos Comput Biol* (2008) 4:e1000028. doi:10.1371/journal.pcbi.1000028
47. Zhen M, Samuel AD, and Samuel T. *C. elegans* Locomotion: Small Circuits, Complex Functions. *Curr Opin Neurobiol* (2015) 33:117–26. doi:10.1016/j.conb.2015.03.009

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

frontiers in Physics

ORIGINAL RESEARCH
published: 25 November 2021
doi: 10.3389/fphy.2021.769420

A Study on Drivers of Water Consumption in China From a Complex Network Perspective

Ruijin Du[1,2], *Xiaoxia Zheng*[3], *Lixin Tian*[1,4]*, *Kaihui Liu*[3], *Lijuan Qian*[3], *Qi Wu*[3] and *Guochang Fang*[5]

[1]Institute of Applied System Analysis, Jiangsu University, Zhenjiang, China, [2]The Physics Department, School of Arts and Sciences, Boston University, Boston, MA, United States, [3]School of Mathematical Sciences, Jiangsu University, Zhenjiang, China, [4]School of Mathematical Sciences, Nanjing Normal University, Nanjing, China, [5]School of Economics, Nanjing University of Finance and Economics, Nanjing, China

Water consumption has been one of the most important topics in the field of environment and economy. Even though the driving factors of water consumption have been well studied, it is still a daunting task to reveal the influence of the status of provinces in the entire supply chain. By combining the multi-regional input-output (*MRIO*) model and complex network theory, an inter-provincial virtual water transfer (*VWT*) network was constructed to analyze the overall structural characteristics of the network model and identify the structural roles of each province. The constructed inter-provincial *VWT* network exhibited the characteristics of a small-world network, that is, virtual water can be easily transferred from one province to another. Moreover, network analysis revealed that provinces with different positions in the *VWT* network played discrepant structural roles. Panel regression analysis was further used to quantify the impact of provincial structural roles on their water consumption. The results showed that water consumption in China largely depended on some structural role characteristics in the *VWT* network. Out-degree and out-strength characterizing the ability of direct exporting virtual water exerted significant positive influences, while in-closeness featuring the indirect virtual water importing rate had a significant negative effect on water usage. This indicated that adjusting the uneven provincial consumption structure, the direct production demand of downstream provinces and the indirect production activities in the supply chain would help reduce water consumption. Therefore, to come true the goal of water conservation in China, it would be necessary to improve the trade structure between direct and indirect exporters and importers in the entire supply chain.

Keywords: water consumption, virtual water transfer, complex network, multi-regional input-output model, panel regression analysis

OPEN ACCESS

Edited by:
Yongxiang Xia,
Hangzhou Dianzi University, China

Reviewed by:
Junhao Peng,
Guangzhou University, China
Lin Chen,
Northwestern Polytechnical University, China
Xiangyun Gao,
China University of Geosciences, China

***Correspondence:**
Lixin Tian
tianlx@ujs.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *02 September 2021*
Accepted: *12 October 2021*
Published: *25 November 2021*

Citation:
Du R, Zheng X, Tian L, Liu K, Qian L, Wu Q and Fang G (2021) A Study on Drivers of Water Consumption in China From a Complex Network Perspective. Front. Phys. 9:769420. doi: 10.3389/fphy.2021.769420

1 INTRODUCTION

The State of Food and Agriculture 2020 report released by Food and Agriculture Organization of the United Nations pointed out that due to factors such as population growth, socio-economic development and the world's shortage of fresh water resources, 3.2 billion people worldwide are facing water shortages, and about 1.2 billion people live in agricultural areas with extreme water shortages [1]. In the past 100 years, global demand for water has increased by 6 times, and will

continue to grow steadily at a rate of about 1% per year in the future [2]. With water resources per capita only a quarter of the world average, China has a serious water shortage, which will be exacerbated by climate change and environmental pollution and ecosystem damage [3, 4]. The scarcity of water resources has become a serious challenge facing the sustainable development of human society.

The concept of virtual water provides new idea for solving the problem of water scarcity. Different from physical water, virtual water contains the amount of water needed to produce goods and services, which provides a more systematical perspective for investigating related issues [5, 6]. It not only has further increased understanding of trade and water management issues, both locally, regionally and globally, but also has provided positive implications to the successful and sustainable development of water resources [7]. Compared with trans-basin water transfer projects, virtual water strategy has the characteristics of easier operation, more convenient and lower cost [8].

In the existing literature, the evaluation, driving factors and economic benefits of virtual water flow have attracted extensive attention from researchers [9, 10]. For research methods, Input-output model has been universally selected to calculate virtual water flow [11, 12]. The input-output table uncovers the relationship between production and consumption in all economies, which provides an approach to track the flow of virtual water in the economic system [13, 14]. Many previous studies focused on the use of input-output (*IO*) analysis to account for virtual water in a country or single region [15, 16]. Given the imbalance of regional production and consumption structure in China, it is essential to reveal the virtual water flow between provinces. Multi-regional input-output (*MRIO*) model can be employed to system atically explain the input-output relationship between different sectors in different regions, so as to trace how the resource and environment influenced by the consumption activities in one region is transferred to a specific production sector in another region through the cross-regional supply chain [4]. *MRIO* model has a comprehensive system boundary to avoid the defects of incomplete supply chain, which has been universally chosen to quantify the virtual water flow between regions [17, 18].

Based on the analysis of *IO* and *MRIO*, researchers have revealed the factors affecting water consumption from different perspectives. Some of these studies focus on the impact of virtual water on water consumption [19–21]. For example, Wang et al. found a significant correlation between virtual water imports and water consumption [22]. In addition, the Logarithmic Mean Divisional Index (*LMDI*) method can decompose all factors without residuals, which is used to quantitatively analyze the driving effect of variables on changes in water consumption [23, 24]. Structural decomposition analysis (*SDA*) combined with input-output analysis is used to reveal the economic reasons for changes in water consumption, including population, *GDP* per capita, water use intensity, technology, and final demand [25, 26]. Liu et al. demonstrated that increasing the export of virtual water in goods and services greatly increases water consumption [26]. These works laid a solid basic to analysis the effect of individual economic activities in regional water consumption and provided valuable implications for reducing regional water consumption.

In China, with the increasingly close inter-provincial trade, the national economy has become an intricate giant system in which each province plays its own unique role and interacts with each other. The water consumption of a province is not only driven by its own development needs, but also affected by other provinces. Although, the economic scale of a province or sector may be relatively small, it may become an important driver of water consumption due to its pivotal position in the national economic system. In other words, the actions to achieve the national water saving goal should not be limited to a certain province, but the national economic system should be regarded as a complete supply chain. Therefore, it is necessary to identify the structural role played by each province and evaluate its impact on water consumption in China.

Emphasizing the system structure and analyzing the system function from the structural perspective is the research idea of complex network theory. Many researchers have found that the function of a network depends on its structure, and the performance of individuals largely depends on their status in the network [27–30]. So far, complex network theory has been universally applied in many scientific fields such as economics [31], finance and trading [32], energy [33–35], climate [36–38]. The existing literature showed that complex network method has significant advantages in identifying the structural roles of nodes in both theoretical and realistic networks.

Different from previous researches on water consumption, this paper designed a novel framework from a complex network perspective. An inter-provincial virtual water transfer (*VWT*) network model was built to analyze the overall structural characteristics of China's supply chain. By combining multi-regional input-output analysis and complex network analysis, the structural role of each province in the network was identified. Finally, a panel regression model was used to quantify the contribution of provincial structural effects on water consumption.

2 DATA AND METHODOLOGY

2.1 Data

The multi-regional input-output (*MRIO*) model has been universally chosen for revealing the virtual water flows between regions [39]. In a *MRIO* framework, regions are linked together by trade. The *MRIO* table used in this study contains 30 provincial-level administrative regions, including 23 provinces, three autonomous regions and four municipalities at the year 2007, 2010, 2012, and 2015. The *MRIO* data is obtained from CEADs database[1], published papers and books [40–42]. The data on water consumption and population at the year 2007, 2010, 2012, and 2015 are taken from China Statistical Yearbook [43–46] and China Urban-Rural Construction Statistical

[1]http://www.ceads.net.n/.

TABLE 1 | Multi-regional input-output table.

Intput / Output		Intermediate use					Final demand					Total output
	—	Region 1	⋯	Region *j*	⋯	Region *N*	Region 1	⋯	Region *j*	⋯	Region *N*	
Intermediate input	Region 1 ⋯ Region *i* ⋯ Region *N*	—	—	x_{ij}	—	—	—	—	f_{ij}	—	—	x_i
Value added						v_j						
Total input						x_j						

x_{ij} *denotes the intermediate input from Region* i *to Region* j, f_{ij} *denotes the final demand of Region* j *derived from Region* i, v_j *and* x_j *respectively represent value added and the total input (output) of Region* j.

Yearbook [47–50]. For the sake of brevity, we use particular codes in figures to abbreviate the name of different provinces, which are shown in **Table A1** in the Appendix.

2.2 Estimation of Inter-Provincial Virtual Water Flows

Multi-regional input-output table provides a useful approach that can be used to reveal the virtual water flows among sectors or regions [42]. As shown in **Table 1**, Chinese economic system consists of N regions. The goods or services imported from Region i to Region j can serve either as intermediate use (denoted by x_{ij}) or final use (denoted by f_{ij}). Thus, the total output in Region i, denoted by x_i, is the sum of intermediate inputs and the final demand, which is shown in **Eq. 1**.

$$x_i = \sum_{j=1}^{N} x_{ij} + \sum_{j=1}^{N} f_{ij}. \tag{1}$$

The direct consumption coefficient a_{ij} reflects the required quantity of imports from Region i per unit output in Region j, which is expressed as:

$$a_{ij} = \frac{x_{ij}}{x_j}. \tag{2}$$

By substituting **Eq. 2** into **Eq. 1**, the matrix expression of the basic form of *MRIO* model is obtained as following:

$$X = AX + F. \tag{3}$$

It follows from **Eq. 3** that

$$X = (I - A)^{-1}F, \tag{4}$$

where I is a N-by-N identity matrix. $(I - A)^{-1}$ is Leontief inverse matrix, which contains both direct and indirect inputs required to meet one unit of final demand in monetary value [51].

In multi-regional input-output analysis of China, the direct water intensity coefficient WI_i of province i is defined as:

$$WI_i = \frac{Y_i}{x_i}, \tag{5}$$

where Y_i and x_i respectively represent the water consumption and total output of province i. By multiplying the direct water intensity coefficient by Leontief inverse matrix, the total virtual water coefficient ε can be expressed as following:

$$\varepsilon = WI\,(I - A)^{-1}. \tag{6}$$

Combined with the total virtual water coefficient matrix and the final demand matrix, the inter-provincial virtual water transfer amount T can be calculated, which is expressed as:

$$T = \varepsilon F. \tag{7}$$

2.3 Inter-Provincial Virtual Water Transfer Network

2.3.1 Network Construction

In this study, the nodes are provinces in China, and the edges are the virtual water transfer relationships between the nodes. The weight of an edge is the amount of virtual water transfer from one province to another. In this way, a directed and weighted inter-provincial virtual water transfer (*VWT*) network is constructed. Centrality is a concept commonly used in complex network analysis to express the degree to which a point is the center of the entire network. In other words, the centrality of nodes reflects their importance in the network. There are many indicators for measuring centrality, including: strength centrality, closeness centrality, betweenness centrality and so on.

2.3.2 The Overall Structural Characteristics

1) Network density

The network density D, is defined as the ratio of the number of edges that actually exist in the network to the number of all possible edges. For a directed network, it can be calculated as follows [36, 52]:

$$D = \frac{E}{N(N-1)}, \tag{8}$$

where E is the number of edges of the network, N is the number of nodes. The network density represents the scale of inter-provincial *VWT* in China. It not only reflects the influence of the entire network on nodes, but also the mutual influence between nodes. The greater the network density, the greater the possibility that the network will affect the nodes, and the closer the relationship between the nodes.

2) Average clustering coefficient

The clustering coefficient quantifies the degree to which the neighboring nodes of a node gather together to form a cluster (complete graph). It can be calculated by the ratio of the number of edges that actually exist between the neighboring nodes of a node and all the possible edges between the neighboring nodes. The average clustering coefficient of a network is defined as the average of the clustering coefficients of all nodes in the network, which can be calculated as follows [53]:

$$C = \frac{1}{N}\sum_{i=1}^{N} c_i, \tag{9}$$

where $c_i = \frac{e_i}{k_i(k_i-1)}$, k_i is the degree of node i, and e_i is the number of actual edges between neighboring nodes of node i. The average clustering coefficient reflects the concentration of inter-provincial *VWT* network. A larger value indicates a closer connection between nodes in the network.

3) Average shortest path length

The distance d_{ij} between nodes i and j is defined as the number of edges on the shortest path connecting i and j. The average shortest path length of a network, L, is the average of the distances between all pairs of nodes in the network. In this paper, it reflects the efficiency of inter-provincial virtual water transfer in China, and can be calculated as [54]:

$$L = \frac{1}{N(N-1)}\sum_{i \neq j} d_{ij}, \tag{10}$$

where N is the number of nodes in the network.

2.3.3 Role Characteristics

1) Degree centrality

The node degree is the number of edges connected to the node, which is the most direct measure of the centrality of the node in network analysis. The greater the degree of a node, the more important the node is in the network. In a directed network, since the edges have directions, the node degree includes in-degree and out-degree. The in-degree of a node is the number of edges with the node as the end point, and the out-degree of the node is the number of edges with the point as the starting point. In this paper, the in-degree D_i^{in} and out-degree D_i^{out} of node i respectively represent the number of import partners and export partners of province i, which can be calculated as follows [52]:

$$D_i^{in} = \sum_{j=1, j\neq i}^{N} A_{ji}, \tag{11}$$

$$D_i^{out} = \sum_{j=1, j\neq i}^{N} A_{ij}, \tag{12}$$

where N is the number of nodes in the inter-provincial *VWT* network, A_{ij} (A_{ji}) is an element in the adjacency matrix of the network. If there is an edge connecting from node i (j) to node j (i), A_{ij} (A_{ji}) = 1, otherwise A_{ij} (A_{ji}) = 0.

2) Strength centrality

One of the centrality measures for a node is its strength. The strength of one node represents the total weight of the edges connected to the node. Since the network is directed, the strength is classified into in-strength and out-strength. In-strength and out-strength respectively reflect the total weight of all incoming and outgoing edges of a node. Here, in-strength S_i^{in} and out-strength S_i^{out} represent the total inflow and outflow of virtual water of province i, respectively. They are calculated as follows [55]:

$$S_i^{in} = \sum_{j=1, j\neq i}^{N} W_{ji}, \tag{13}$$

$$S_i^{out} = \sum_{j=1, j\neq i}^{N} W_{ij}, \tag{14}$$

where N is the number of nodes in the inter-provincial *VWT* network, W_{ij} (W_{ji}) denotes the weight of the edge connecting i (j) to j (i). The net virtual water (*NVW*) inflow of node i is denoted as NVW_i, $NVW_i = S_i^{in} - S_i^{out}$. If $NVW_i > 0$, node i is a *NVW* importer, otherwise it is a *NVW* exporter [10].

3) Closeness centrality

Closeness centrality reflects how easy it is for a node to access other nodes, and is defined by the inverse of the average length of the shortest path connecting one node to all other nodes in the network [52]. In a directed network, in-closeness is used to measure how many steps are required at least if other nodes want to access a given node, reflecting how easy it is for other nodes to access the given node. The higher the in-closeness of one node, the easier it is for other nodes to access it. While out-closeness measures how many steps a given node takes at least to access every other node. The greater the out-closeness of one node, the easier it is for the node to access other nodes. In this paper, in-closeness C_i^{in} and out-closeness C_i^{out} respectively represent the transfer speed of virtual water from the other provinces to one province or from one province to the others. They are calculated as following [56]:

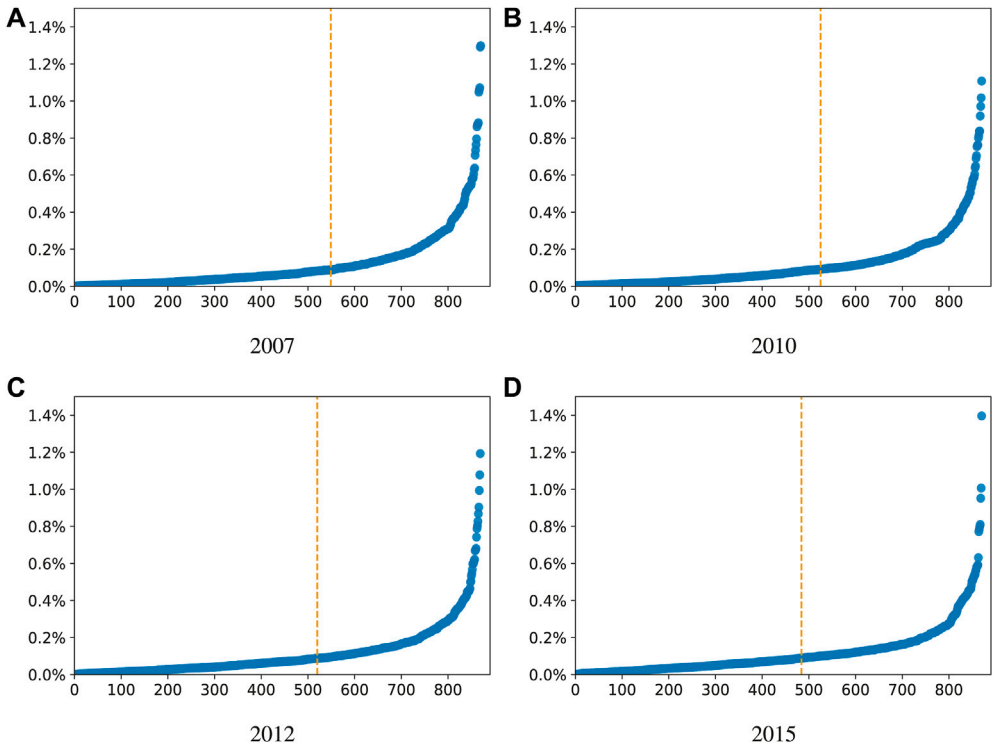


FIGURE 1 | The distribution of the ratio of edge weight to total weights in the initial VWT network, arranged in ascending order from left to right. **(A)** 2007; **(B)** 2010; **(C)** 2012; **(D)** 2015.

$$C_i^{in} = \left[\frac{1}{N-1}\sum_{j=1,j\neq i}^{N} d_{ji}\right]^{-1}, \tag{15}$$

$$C_i^{out} = \left[\frac{1}{N-1}\sum_{j=1,j\neq i}^{N} d_{ij}\right]^{-1}, \tag{16}$$

where N is the number of nodes in the inter-provincial *VWT* network, d_{ij} (d_{ji}) represents the length of the shortest path from node i (j) to node j (i).

2.4 Selection of Panel Regression Model and Variables

In the inter-provincial *VWT* network, the roles of provinces on water consumption are different and change over time. On the one hand, due to regional heterogeneity, different provinces play different roles. On the other hand, the role of provinces in the network evolves dynamically over time. Therefore, the panel regression model can be used to analyze the relationship between the roles of provinces and water consumption in China from the spatial and temporal dimensions:

$$Y_{it} = \alpha + \beta 1_{it} X_{it} + \beta 2_{it} contronl_{it} + \gamma_{it} \quad (i = 1, 2, \ldots, N;\ t = 1, 2, \ldots, T), \tag{17}$$

X_{it}, Y_{it} and $control_{it}$ separately represent the set of core explanatory variables, explained variable and control variables. $\beta 1_{it}$ and $\beta 2_{it}$ are the coefficients of explanatory variables and control variables. γ_{it} is the residual.

1) Explained variable

This paper aims to use panel regression model to evaluate the drivers of water consumption in China. The water consumption of each province is selected as explained variable.

2) Core explanatory variables

Indicators reflecting the structural centrality of the inter-provincial *VWT* network are chosen as core explanatory variables, including: in-degree (D^{in}), out-degree (D^{out}), in-strength (S^{in}), out-strength (S^{out}), in-closeness (C^{in}) and out-closeness (C^{out}).

3) Control variables

Control variables are used to eliminate some important common factors affecting virtual water consumption in the province. The increase in the urbanization rate and the improvement of the water-saving system will drive the reduction of water consumption. The final demand represents the final use or consumption of the social total products by consumers. If a province has a high consumption capacity, this drive the province's water use from production to consumption

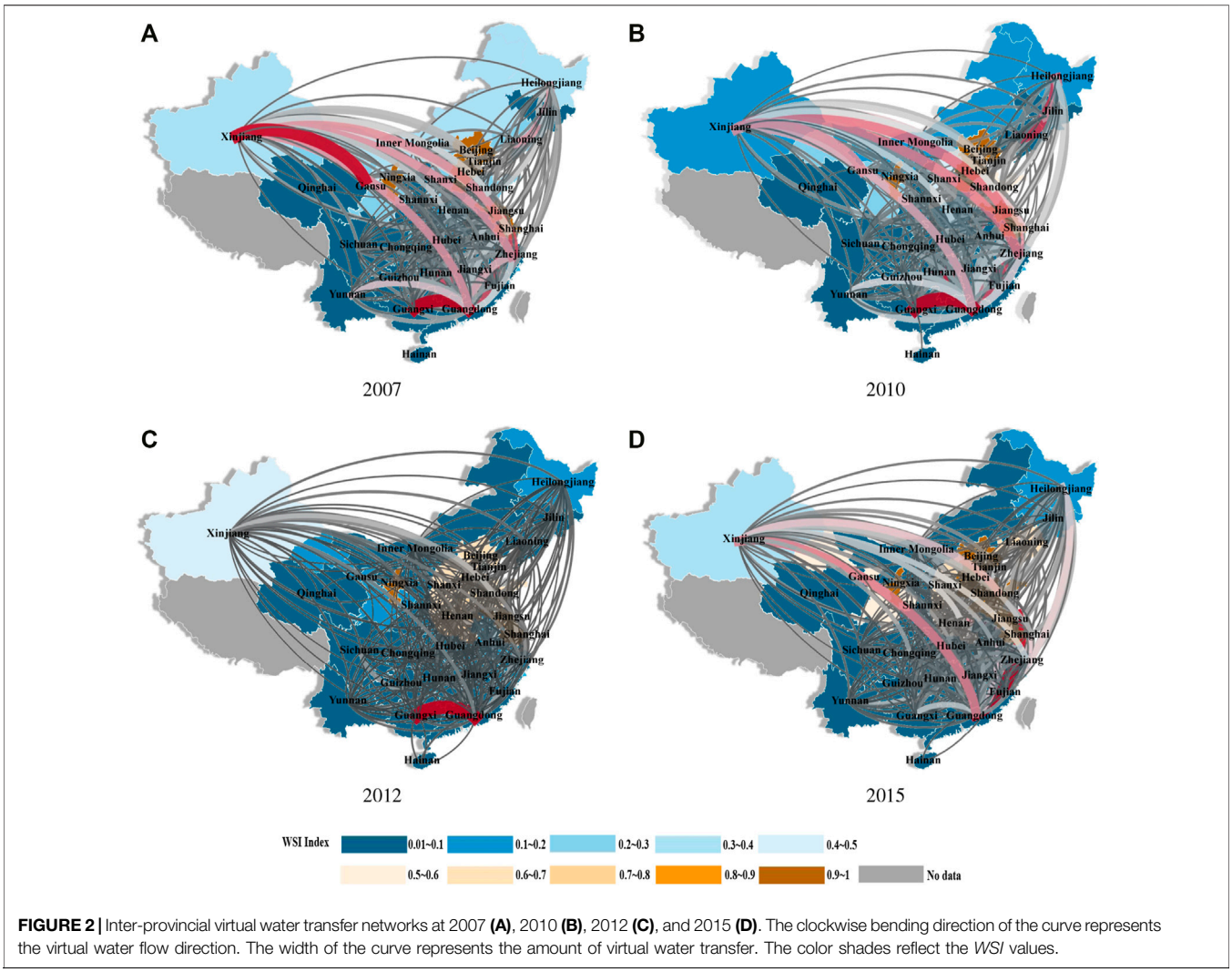


FIGURE 2 | Inter-provincial virtual water transfer networks at 2007 **(A)**, 2010 **(B)**, 2012 **(C)**, and 2015 **(D)**. The clockwise bending direction of the curve represents the virtual water flow direction. The width of the curve represents the amount of virtual water transfer. The color shades reflect the *WSI* values.

TABLE 2 | The overall structural characteristics of inter-provincial *VWT* network.

Year	2007	2010	2012	2015
Network density	0.369	0.397	0.402	0.444
Average shortest path length	1.639	1.673	1.662	1.540
Average clustering coefficient	0.595	0.631	0.660	0.669

to a certain extent. In addition, there are differences in production technology in different provinces. Advanced technology can promote the reduction of water consumption. Water intensity reflects the difference in production technology, and thus can effectively describe the difference in water consumption between different provinces. Therefore, in this paper, urbanization rate (U)[2], final demand (F) and water intensity (WI) are selected as control variables. In order to eliminate potential multicollinearity between variables, each variable in the panel regression model is estimated separately.

[2]The urbanization rate is a measure of urbanization, the urbanization rate of a province is defined as the ratio of the urban population to the total population of the province.

3 RESULTS

3.1 The Overall Structural Characteristics of *VWT* Network

The initial inter-provincial *VWT* network based on *MRIO* table in China is a fully connected network. In complex network theory, it is difficult to reveal the essential characteristics for a fully connected network [36]. To better understand the basic structural characteristics of virtual water transfer flows between provinces, it is essential to set a threshold to eliminate the disturbance of edges with negligible weights. Firstly, the edges in the initial *VWT* network from 2007 to 2015 are sorted by weight. Then, we find that at most 40% of the edges have transferred more than 80% of the total virtual water flow. The remaining more than 60% edges are very weak

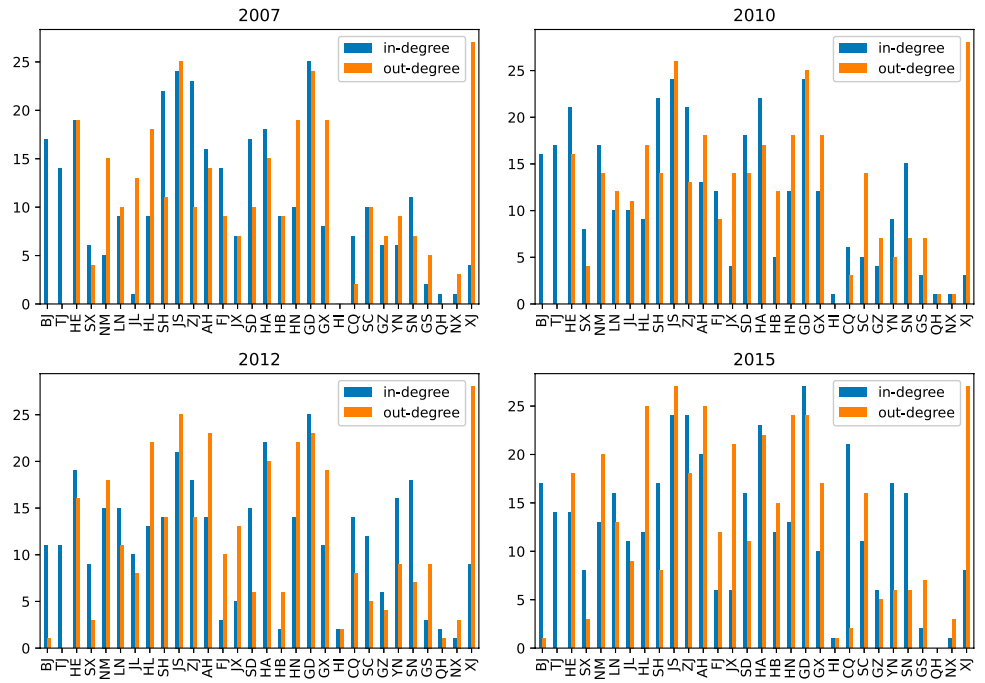


FIGURE 3 | The distribution of in-degree and out-degree of each province in the inter-provincial *VWT* network.

connections, which are relatively trivial for structural analysis. **Figure 1** shows the distribution of the ratio of edge weight to total weights in the initial *VWT* network during the period 2007–2015, arranged in ascending order from left to right. The yellow dashed line represents the critical threshold for filtering out those unimportant edges, which is set to guarantee the total weight of the removed edges accounts for 20%. Thus, only those edges that accounted for 80% of the total volume of the virtual water transfer are retained in the final networks. The inter-provincial *VWT* networks in 2007, 2010, 2012, and 2015 are shown in **Figure 2**. During 2007–2015, virtual water flow played an increasingly important role in water usage of China. The virtual water flow was 233.6, 228.6, 239.2, and 251.6 billion cubic meters for 2007, 2010, 2012, and 2015 respectively. In other words, the virtual water flow has increased by more than 7% in the past few years. **Figure 2A** shows the virtual water in Xinjiang, the largest exporting province at that time, was mainly transferred to the Central region in 2007, then to the South Coast region through the East Coast in 2010 (shown in **Figure 2B**) and 2012 (shown in **Figure 2C**). By 2015, Jiangsu has replaced Xinjiang as the largest exporter, the virtual water in which were mainly transported to the South Coast region (shown in **Figure 2D**).

It can be found from **Table 2** that the network structure has characteristics of evolution with time. From 2007 to 2015, the density of inter-provincial virtual water transfer networks showed an increasing trend, indicating that network connections have become closer. The growing network density reflected the increasing frequency of virtual water transfer between provinces, which was related to the rapid development of inter-provincial trade in China. The average clustering coefficient was roughly around 0.6, implying that the probability of virtual water transfer between neighboring provinces was relatively high. The average shortest path length of the network experienced a slight fluctuation around 1.6, which showed a quite fast transfer speed of virtual water between provinces. The small average shortest path length indicated that the virtual water in one province could flow either directly or indirectly through at most one intermediate province to the destination province. Large average clustering coefficient and small average shortest path length made the inter-provincial virtual water transfer network exhibit the characteristics of a small world network, where most nodes were non-adjacent and could reach every other node in relative small steps [57].

3.2 Structural Roles of Provinces in the *VWT* Network

The structural roles of each province in the inter-provincial *VWT* network were identified with the aid of complex network analysis. It is widely known that the node degree characterizes the position of the node in a network. It can be seen from **Figure 3** that several provinces have sustained high out-degrees over these years, which indicated that those provinces had many exporting partners. The changes in the number of exporting partners differed greatly among those provinces with high out-degrees. The number for exporting partners has shown a slight upward trend for Jiangsu, Anhui, Henan and Hunan provinces, while a slight decline for Guangxi province. The changes in the number of exporting

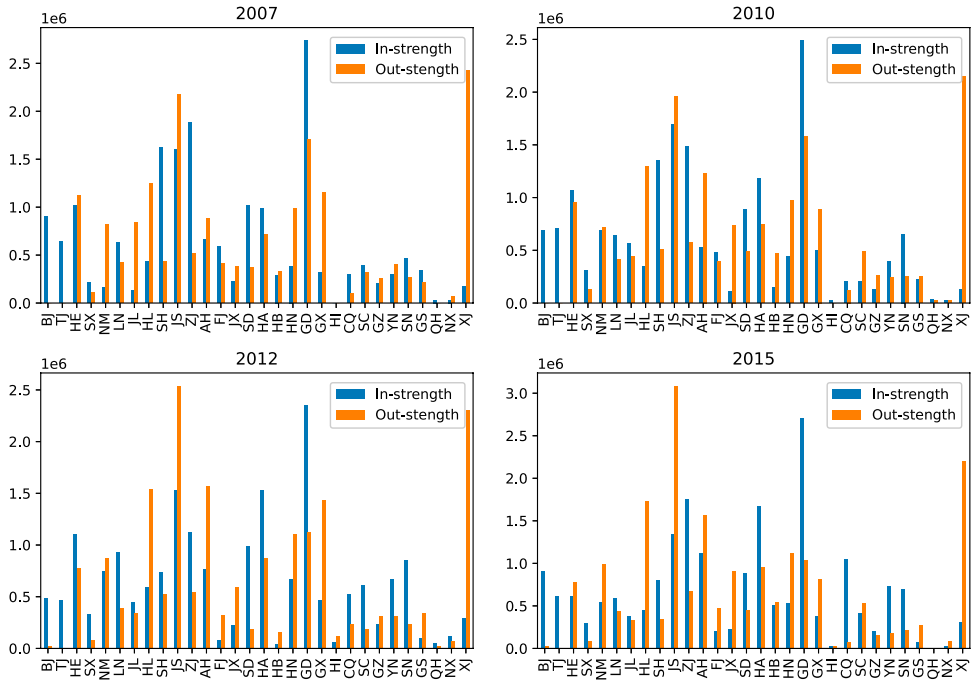


FIGURE 4 | The distribution of in-strength and out-strength of each province in the inter-provincial *VWT* network.

partners differed greatly among these provinces with high out-degrees. The number for exporting partners has shown a slight upward trend for Jiangsu, Anhui, Henan and Hunan provinces, while a slight decline for Guangxi province. Compared with the case of out-degree, provinces with relatively high in-degree have many import partners. Over these years, the number of importing partners has grown slightly for Guangdong, Zhejiang and Henan provinces, while declined slightly for Shanghai. In particular, Jiangsu and Guangdong with both high in-degree and out-degree values had a close virtual water transfer relationship with other provinces, which was consistent with their economic status in the entire supply chain of China.

Another important role character is the node strength. The in-strength and out-strength of each province in the *VWT* network were shown in **Figure 4**. Jiangsu, Xinjiang, Guangdong, Anhui and Heilongjiang with high out-strengths, were the main virtual water suppliers. On the contrary, provinces including Jiangsu, Guangdong, Zhejiang, Henan and Shanghai had high in-strengths and were the main virtual water consumption markets. In addition, water stress index (*WSI*) was employed to evaluate the scarcity of water resources in a region. It is calculated by the ratio of water withdrawn to available water. The range of *WSI* values is between 0.01 and 1. A *WSI* of 0.5 is usually set as a threshold of medium and high water stress [58, 59]. The shade of the color on the map in **Figure 2** represents the *WSI* value of each province. Combined with the results in **Figures 2**, **4**, it can be found that the positions among these provinces are different. In 2007, 2010, 2012, and 2015, Beijing, Shanghai, Tianjin and Jiangsu are provinces with severe water shortage due to extremely high *WSI* values. Beijing, Shanghai and Tianjin are the main *NVW* importers. However, Jiangsu was the main *NVW* exporter, ranking second in net exports. Xinjiang, Heilongjiang, Guangxi, Anhui, Guangdong and Zhejiang were rich in water resources. Especially in Guangxi, Anhui, Guangdong and Zhejiang, *WSI* was lower than 0.1. However, the situation between them was quite different. Xinjiang, Heilongjiang, Guangxi, and Anhui were the main *NVW* exporters during 2007–2015, while Guangdong and Zhejiang were the main *NVW* importers, ranking the top two in terms of net imports.

The closeness of a node accounts for the importance of the node from another perspective. **Figure 5** shows that the values of in-closeness and out-closeness were relatively large, indicating that the virtual water transfer speed was fast. In particular, the out-closeness values of Jiangsu, Guangdong and Xinjiang were all above 0.8, which imply that virtual water in these provinces could flow to other provinces through relative short paths. Moreover, the values of in-closeness and out-closeness both showed a slight upward trend. This trend demonstrated that changes in province would soon spread to other provinces due to closer connections between provinces.

3.3 Impact of Structural Roles of Provinces on Water Consumption in China

The stability of a complex network depends largely on its structure. Therefore, in the inter-provincial *VWT* network, the

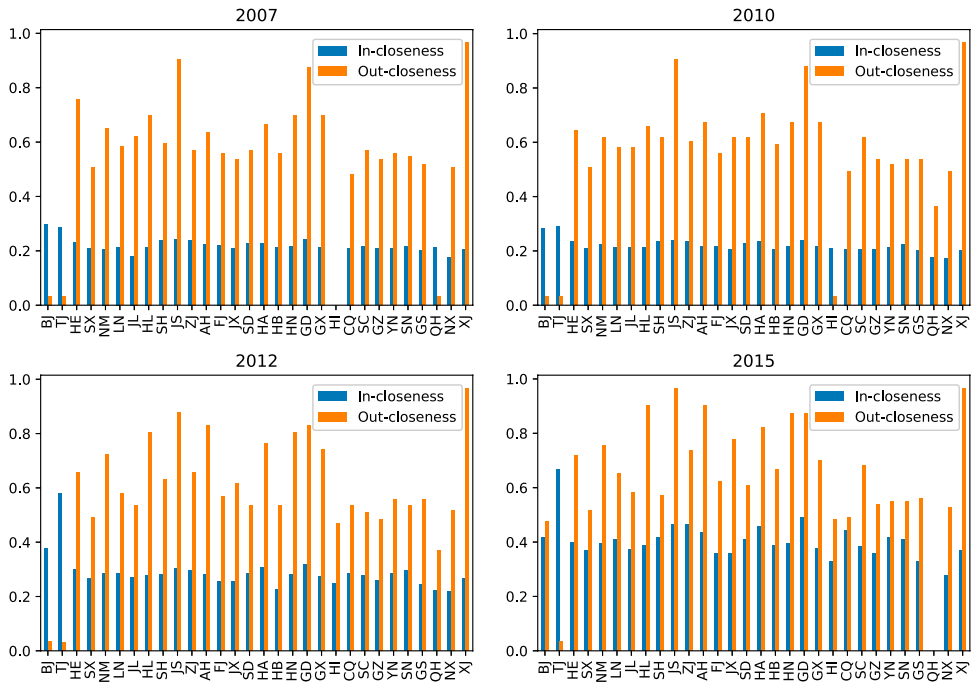


FIGURE 5 | The distribution of in-closeness and out-closeness of each province in the inter-provincial *VWT* network.

TABLE 3 | Descriptive statistics of the variables.

Variables	Obs	Mean	SD	Maximum	Minimum
Core explanatory variables					
D^{in}	120	11.683	7.083	27	0
D^{out}	120	11.683	8.123	28	0
S^{in}	120	635305.9	572132.3	2736180	0
S^{out}	120	635305.9	637195.4	3083848	0
C^{in}	120	0.278	0.096	0.667	0
C^{out}	120	0.585	0.223	0.967	0
Control variables					
U	120	0.530	0.138	0.893	0.282
WI	120	0.007769	0.009	0.068	0.00056
F	120	15314.23	128508.89	61608.54	804.63
Explained variable					
Y	120	1996130	1413768.9	58901376	224856

TABLE 4 | Results of unit root test.

	ADF		PP	
	T-statistic	*p*-value	T-statistic	*p*-value
Core explanatory variables				
D^{in}	−4.12	0.001	−4.13	0.001
D^{out}	−4.37	0.000	−4.29	0.001
S^{in}	−4.27	0.008	−4.38	0.001
S^{out}	−4.13	0.001	−3.83	0.003
C^{in}	−7.04	0.000	−10.36	0.000
C^{out}	−4.30	0.001	−7.44	0.000
Explained variables				
U	−7.81	0.000	−3.33	0.015
WI	−11.86	0.000	−12.02	0.000
F	−11.73	0.000	−14.14	0.000
Explained variable				
Y	−9.01	0.000	−12.44	0.000

TABLE 5 | Results of residual cointegration test.

Method	Statistic	Prob
ADF	−8.636	0.000

structural role of provinces has a significant impact on their water consumption. To test this assumption, panel regression analysis was applied to examine the impact of structural roles of provinces on their water consumption. Here the fixed effects model was selected as the panel regression model through Hausman test. In this paper, water consumption is chosen as the explained variable, D^{in}, D^{out}, S^{in}, S^{out}, C^{in} and C^{out} are the core explanatory variables, and urbanization rate, final demand and water intensity were the control variables.

Table 3 lists the descriptive statistics of the variables considered. Significant differences between some variables can be found from this table. Before substituting into the panel regression model, all variables need to be normalized to eliminate the impact of different dimensions between variables, so that equivalent comparisons can be made between the effects of variables. The results of unit root test and co-integration test showed that all normalized variables were stable, and there was a co-integration relationship between variables, as shown in **Tables 4**, **5**.

TABLE 6 | The correlation of variables.

Variables	Y	D^{in}	D^{out}	S^{in}	S^{out}	C^{in}	C^{out}	U	WI	F
Y	1	—	—	—	—	—	—	—	—	—
D^{in}	0.347***	1	—	—	—	—	—	—	—	—
D^{out}	0.882***	0.439***	1	—	—	—	—	—	—	—
S^{in}	0.407***	0.906***	0.458***	1	—	—	—	—	—	—
S^{out}	0.911***	0.351***	0.894***	0.376***	1	—	—	—	—	—
C^{in}	0.026	0.381***	0.060	0.266***	0.029	1	—	—	—	—
C^{out}	0.791***	0.334***	0.883***	0.369***	0.761***	–0.05	1	—	—	—
U	–0.123	0.395***	–0.129	0.381***	–0.086	0.328***	–0.285***	1	—	—
WI	0.451***	–0.416***	0.342***	–0.357***	0.464***	–0.178**	0.343***	–0.369***	1	—
F	0.529***	0.774***	0.470***	0.824***	0.407***	0.251***	0.388***	0.305***	–0.386***	1

*Level of significance: * is 10%, ** is 5% and *** is 1%.*

TABLE 7 | Results of the panel regressions.

Variable	Model 1		Model 2		Model 3		Model 4	
	Coef	t	Coef	t	Coef	t	Coef	T
U	–0.225**	–2.55	–0.223***	–2.5	–0.266***	–3.01	–0.231**	–2.59
WI	0.256***	3.98	0.257***	2.99	0.247***	2.96	0.260***	3.03
F	0.221***	4.23	0.212***	3.82	0.208***	4.16	0.208***	3.87
D^{in}	—	—	0.007	0.38	—	—	—	—
D^{out}	—	—	—	—	0.049**	2.22	—	—
S^{in}	—	—	—	—	—	—	0.0216	0.72
S^{out}	—	—	—	—	—	—	—	—
C^{in}	—	—	—	—	—	—	—	—
C^{out}	—	—	—	—	—	—	—	—
Const	0.289***	7.26	0.287***	7.14	0.286***	7.37	0.288***	7.23
Hausman test	1195.93***	—	1228.07***	—	529.57***	—	432.11***	—
Variable	**Model 5**		**Model 6**		**Model 7**		**Model 8**	
	Coef	t	Coef	t	Coef	t	Coef	t
U	–0.281***	–3.31	–0.243***	–2.86	–0.250***	–2.81	–0.311***	–3.65
WI	0.229***	2.84	0.344***	3.94	0.270***	3.17	0.327***	3.83
F	0.185***	3.78	0.255***	5.07	0.223***	4.43	0.200***	3.68
D^{in}	—	—	—	—	—	—	0.023	0.69
D^{out}	—	—	—	—	—	—	0.019	0.74
S^{in}	—	—	—	—	—	—	–0.003	–0.08
S^{out}	0.102***	3.48	—	—	—	—	0.082**	2.61
C^{in}	—	—	–0.025***	–2.92	—	—	–0.023***	–2.76
C^{out}	—	—	—	—	0.036	1.62	0.022	0.85
Const	0.296***	7.90	0.282***	7.38	0.272***	6.69	0.273***	7.08
Hausman test	343.81***	—	79.25***	—	373.25***	—	3841.84***	—

*Level of significance: * is 10%, ** is 5% and *** is 1%.*

The correlation between variables was shown in **Table 6**. The results showed that there was a strong correlation between some variables. For instance, the correlation between in-degree and in-strength was 0.906 and the significance level was less than 1%. Thus, this paper constructed six panel regression models to evaluate the influence of the structural characteristics of inter-provincial *VWT* network on water consumption, and the other two models were used to evaluate the influence of control variables and all variables on water consumption. **Table 7** showed the results of the panel regression model. Model 1 measured the impact of control variables on water consumption. The results showed that both water intensity and final demand had a significant positive impacts on water consumption. Specifically, water intensity characterized by technical effects was an important driving force for changes in water consumption [42]. Technological progress and improvement of technical efficiency have led to a reduction in water intensity and greatly reduced water consumption. Final demand was the continuous driving force of economic growth, which in turn would drive water consumption. The level of urbanization had a weak but significantly negative effect on water consumption. The urbanization process accompanied by industrial agglomeration and technological progress has promoted the improvement of water use efficiency and the reduction of water consumption [60]. In addition, the high population density brought about by urbanization made infrastructure sharing inevitable, which also contributed to the reduction of water consumption to a certain extent.

In models 2–7, the effects of the six structural roles (in-degree, out-degree, in-strength, out-strength, in-closeness and out-closeness) of provinces on water consumption in China were evaluated. The results of panel regression analysis showed that out-degree and out-strength had a significant positive effect, while in-closeness had a significant negative effect. In-degree, in-strength and out-closeness had no significant impact on water consumption. The impacts of out-degree indicated that the provinces would consume more water if they had more exporting partners. Similar situation occured when the impact of out-strength was investigated. Provinces exporting more virtual water tended to consume more water. The reason lies in the products with plenty of virtual water embodied in, produced by these provinces are not only to meet the needs of the province, but also to be exported to downstream provinces. This demonstrated that water consumption was mainly affected by direct production demand from downstream provinces. Therefore, by controlling the direct production demand from downstream provinces, water consumption could be significantly reduced. Conversely, the significant negative impact of in-closeness indicated that the transferring speed of the virtual water played a key role in water consumption. One province would consume less water resource if products would be imported from other province in a very short time. Thus, this province was often considered as a direct or indirect downstream market for many provinces in the production chain. In other words, if the production demand of a downstream province would be quickly filled from the upstream provinces, resulting in its less consumption of water resources. The impact of in-closeness indicated that indirect production demand would also significantly drive water consumption. In conclusion, the reduction of water resources should be implemented in both direct and indirect production activities.

4 DISCUSSION AND CONCLUSION

This paper aims to evaluate the impact of structural effects of provinces in China on their water consumption. First, the multi-regional input-output analysis and complex network method were combined to construct the inter-provincial virtual water transfer (*VWT*) network. Then the structural characteristics of provinces in the *VWT* network model were identified. Finally, panel regression analysis was applied to evaluate the contribution of provinces' structural effects to their water consumption.

In the *VWT* network, virtual water establishes different paths through inter-provincial transfer and flows to the final consumer. The analysis of the inter-provincial *VWT* network can help decision makers better understand the current virtual water flow situation, the role of provinces and the flow path. First, the results reveled the overall characteristics of the inter-provincial *VWT* network. The network density has shown an upward trend, reflecting the increasing frequency of virtual water transfers between provinces. The high average clustering coefficient indicated that there were many local clusters in the *VWT* network. In addition, the path of virtual water flowing from one province to another was relatively smooth. The analysis of the average shortest path length showed that virtual water transfer from one province to another only needed to pass through 1.6 provinces, which means that the provinces were quite close to each other in the inter-provincial *VWT* network. The high average clustering coefficient and small average shortest path length showed that the *VWT* network had a small-world nature, which meant that the virtual water in one province would soon be transferred to the other.

Network analysis also showed that provinces have different level of significance and played different roles in the inter-provincial *VWT* network. The results showed that during the period from 2007 to 2015 there was a obvious imbalance between the import and export of the *VWT* network. Guangdong, Zhejiang, Jiangsu, Shanghai and Henan with many importing partners, were provinces with plenty of virtual water inflows. Some provinces, such as Xinjiang, Jiangsu, Guangxi, Anhui and Heilongjiang, not only had many exporting parters, but also a large amount of virtual water outflow. Xinjiang, Heilongjiang, Guangxi and Anhui were the main *NVW* exporters, while Guangdong and Zhejiang with extremely low *WSI* values (<0.1), were the main *NVW* importers. In other words, Guangdong and Zhejiang with abundant water resources have exacerbated water shortages in other provinces by importing virtual water from them. The water scarce situations differ greatly between Beijing, Shanghai, Tianjin and Jiangsu, which had extremely high WSI values. Beijing, Shanghai and Tianjin were the main *NVW* importers, while Jiangsu was the main *NVW* exporter, ranking second in net exports. That is to say, the water scarcity situation in Beijing, Shanghai and Tianjin has been in alleviated through the net import of virtual water, while the large net export of virtual water in Jiangsu has further exacerbated the water shortage situation. In addition, the results showed that changes in other provinces could easily flow into Tianjin with high in-closeness, while virtual water from Jiangsu, Xinjiang and Guangdong with high out-closeness could easily be transferred to other provinces.

Panel regression analysis showed that some structural effects in the inter-provincial *VWT* network significantly determined water consumption related to economic activities in the province. Out-degree and out-strength played a significant positive effect, while in-closeness played a significant negative effect. The relationship between water consumption and the number of trading partners, as well as the virtual water transfer volume, showed that water consumption growed with the increase in the number of export partners and the increase in export volume. Therefore, adjusting the direct production demand and consumption structure of downstream provinces would help reduce water consumption in China. Further investigation on the impact of in-closeness indicated that indirect production activities would significantly affect water consumption. Therefore, the reduction of water consumption in China should be based on the direct and indirect relationship in the production process.

This paper focuses on the contribution of the structural roles of provinces in the *VWT* network to their water consumption. There are some shortcomings in the research. One limitation is that although some important factors are considered as control

variables, there are still some variables that are not included, such as climate change, This is a gap that still exists in the existing knowledge system. Studying the impact of the structural roles of various sectors in the industrial chain on water consumption can provide valuable information for rationally reshaping the industrial structure and reducing water consumption. Another limitation is that this paper considers the impact of structural roles on water consumption at the provincial level, not at the sectoral level. This is a gap that still exists in the existing knowledge system. Studying the impact of the structural roles of various sectors in the industrial chain on water consumption can provide valuable information for rationally reshaping the industrial structure and reducing water consumption. All of these will be improved in future work.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

RD, LT, and LQ designed research; RD, XZ, QW, LT, KL, LQ, and GF performed research; RD, XZ, QW, and GF analyzed data; RD, XZ, KL, LT, and LQ wrote the paper.

FUNDING

This research was financially supported by the National Natural Science Foundation of China (Grant Nos. 71974080, 61973143, 11731014, 11901247, 71774077, 51876081, and 19A297), the Major Program of National Natural Science Foundation of China (Grant No. 71690242), National Key Research and Development Program of China (Grant No. 2020YFA0608601).

ACKNOWLEDGMENTS

KL thanks Foundation for High-Level Entrepreneurial and Innovative Talents of Jiangsu Province, and Research Grants for High-Level Talents of Jiangsu University.

REFERENCES

1. FAO. *The State of Food and Agriculture 2020 Report* (2020). Available from: http://www.fao.org/publications/sofa/en/.
2. USESCO. *The Unite Nations World Water Development Report 2020* (2020). Available from: http://zh.unesco.org/events/.
3. Tao S, Zhang H, Feng Y, Zhu J, Cai Q, Xiong X, et al. Changes in China's Water Resources in the Early 21st century. *Front Ecol Environ* (2020) 18:188–93. doi:10.1002/fee.2164
4. Zhang Y, Chen Y, and Huang M. Water Footprint and Virtual Water Accounting for China Using a Multi-Regional Input-Output Model. *Water* (2019) 11:34. doi:10.3390/w11010034
5. Zhang X, Liu J, Zhao X, Yang H, Deng X, Jiang X, et al. Linking Physical Water Consumption with Virtual Water Consumption: Methodology, Application and Implications. *J Clean Prod* (2019) 228:1206–17. doi:10.1016/j.jclepro.2019.04.297
6. Zhao X, Liu J, Liu Q, Tillotson MR, Guan D, and Hubacek K. Physical and Virtual Water Transfers for Regional Water Stress Alleviation in China. *Proc Natl Acad Sci USA* (2015) 112:1031–5. doi:10.1073/pnas.1404130112
7. *"Virtual Water" Innovator Awarded 2008 Stockholm Water Prize*. 2008. Available from: http://sa.indiaenvironmentportal.org.in/files/Virtual%20water.pdf.
8. Yang H, and Zehnder A. "Virtual Water": An Unfolding Concept in Integrated Water Resources Management. *Water Resour Res* (2007) 43. doi:10.1029/2007WR006048
9. Qian Y, Tian X, Geng Y, Zhong S, Cui X, Zhang X, et al. Driving Factors of Agricultural Virtual Water Trade between China and the Belt and Road Countries. *Environ Sci Technol* (2019) 53:5877–86. doi:10.1021/acs.est.9b00093
10. Wang L, Zou Z, Liang S, and Xu M. Virtual Scarce Water Flows and Economic Benefits of the Belt and Road Initiative. *J Clean Prod* (2020) 253:119936. doi:10.1016/j.jclepro.2019.119936
11. Qasemipour E, Tarahomi F, Pahlow M, Malek Sadati SS, and Abbasi A. Assessment of Virtual Water Flows in iran Using a Multi-Regional Input-Output Analysis. *Sustainability* (2020) 12:7424. doi:10.3390/su12187424
12. Zhang C, and Anadon LD. A Multi-Regional Input-Output Analysis of Domestic Virtual Water Trade and Provincial Water Footprint in China. *Ecol Econ* (2014) 100:159–72. doi:10.1016/j.ecolecon.2014.02.006
13. Zhai M, Huang G, Liu L, Xu X, and Li J. Transfer of Virtual Water Embodied in Food: A New Perspective. *Sci Total Environ* (2019) 659:872–83. doi:10.1016/j.scitotenv.2018.12.433
14. An T, Wang L, Gao X, Han X, Zhao Y, Lin L, et al. Simulation of the Virtual Water Flow Pattern Associated with Interprovincial Grain Trade and its Impact on Water Resources Stress in China. *J Clean Prod* (2021) 288:125670. doi:10.1016/j.jclepro.2020.125670
15. White DJ, Feng K, Sun L, and Hubacek K. A Hydro-Economic MRIO Analysis of the Haihe River Basin's Water Footprint and Water Stress. *Ecol Model* (2015) 318:157–67. doi:10.1016/j.ecolmodel.2015.01.017
16. Wu XJ, Sun J, Liu J, Ding YK, Huang GH, and Li YP. Ecological Network-Based Input-Output Model for Virtual Water Analysis in China. *IOP Conf Ser Earth Environ Sci* (2020) 435:012010. doi:10.1088/1755-1315/435/1/012010
17. Wiedmann T. A Review of Recent Multi-Region Input-Output Models Used for Consumption-Based Emission and Resource Accounting. *Ecol Econ* (2009) 69:211–22. doi:10.1016/j.ecolecon.2009.08.026
18. Qu S, Liang S, Konar M, Zhu Z, Chiu ASF, Jia X, et al. Virtual Water Scarcity Risk to the Global Trade System. *Environ Sci Technol* (2018) 52:673–83. doi:10.1021/acs.est.7b04309
19. Xiong Y, Tian X, Liu S, and Tang Z. New Patterns in China's Water Footprint: Analysis of Spatial and Structural Transitions from a Regional Perspective. *J Clean Prod* (2020) 245:118942. doi:10.1016/j.jclepro.2019.118942
20. Tian Z, Fang D, and Chen B. Three-scale Input-Output Analysis for Energy and Water Consumption in Urban Agglomeration. *J Clean Prod* (2020) 268:122148. doi:10.1016/j.jclepro.2020.122148
21. Wang YB, Wu PT, Zhao XN, and Engel BA. Virtual Water Flows of Grain within China and its Impact on Water Resource and Grain Security in 2010. *Ecol Eng* (2014) 69:255–64. doi:10.1016/j.ecoleng.2014.03.057
22. Wang X, and Hu J. Research on Virtual Water in the Chinese International Grain Trade. *Me* (2015) 06:735–46. doi:10.4236/me.2015.66070
23. Ang BW, and Zhang FQ. A Survey of index Decomposition Analysis in Energy and Environmental Studies. *Energy* (2000) 25:1149–76. doi:10.1016/S0360-5442(00)00039-6
24. Ang BW. Decomposition Analysis for Policymaking in Energy:. *Energy Policy* (2004) 32:1131–9. doi:10.1016/S0301-4215(03)00076-4
25. Cazcarro I, Duarte R, and Sánchez-Chóliz J. Economic Growth and the Evolution of Water Consumption in Spain: A Structural Decomposition Analysis. *Ecol Econ* (2013) 96:51–61. doi:10.1016/j.ecolecon.2013.09.010

26. Liu J, Zhao X, Yang H, Liu Q, Xiao H, and Cheng G. Assessing China's "developing a Water-Saving Society" Policy at a River basin Level: A Structural Decomposition Analysis Approach. *J Clean Prod* (2018) 190:799–808. doi:10.1016/j.jclepro.2018.04.194
27. Newman MEJ. The Structure and Function of Complex Networks. *SIAM Rev* (2003) 45:167–256. doi:10.1137/S003614450342480
28. Dong G, Fan J, Shekhtman LM, Shai S, Du R, Tian L, et al. Resilience of Networks with Community Structure Behaves as if under an External Field. *Proc Natl Acad Sci USA* (2018) 115:6911–5. doi:10.1073/pnas.1801588115
29. Liu Y, Sanhedrai H, Dong G, Shekhtman LM, Wang F, Buldyrev SV, et al. Efficient Network Immunization under Limited Knowledge. *Natl Sci Rev* (2020) 8(8). doi:10.1101/2020.04.07.20056606
30. Dong G, Wang F, Shekhtman LM, Danziger MM, Fan J, Du R, et al. Optimal Resilience of Modular Interacting Networks. *Proc Natl Acad Sci USA* (2021) 118:e1922831118. doi:10.1073/pnas.1922831118
31. Chen K, Luo P, Sun B, and Wang H. Which Stocks Are Profitable? A Network Method to Investigate the Effects of Network Structure on Stock Returns. *Physica A: Stat Mech its Appl* (2015) 436:224–35. doi:10.1016/j.physa.2015.05.047
32. Gao X, Fang W, An F, and Wang Y. Detecting Method for Crude Oil price Fluctuation Mechanism under Different Periodic Time Series. *Appl Energ* (2017) 192:201–12. doi:10.1016/j.apenergy.2017.02.014
33. Du R, Dong G, Tian L, Wang Y, Zhao L, Zhang X, et al. Identifying the Peak point of Systemic Risk in International Crude Oil Importing Trade. *Energy* (2019) 176:281–91. doi:10.1016/j.energy.2019.03.127
34. Du R, Wang Y, Dong G, Tian L, Liu Y, Wang M, et al. A Complex Network Perspective on Interrelations and Evolution Features of International Oil Trade, 2002-2013. *Appl Energ* (2017) 196:142–51. doi:10.1016/j.apenergy.2016.12.042
35. Sun X, Li J, Qiao H, and Zhang B. Energy Implications of China's Regional Development: New Insights from Multi-Regional Input-Output Analysis. *Appl Energ* (1962) 196:118–31. doi:10.1016/j.apenergy.2016.12.088
36. Jiang M, An H, Gao X, Liu S, and Xi X. Factors Driving Global Carbon Emissions: A Complex Network Perspective. *Resour Conservation Recycling* (2019) 146:431–40. doi:10.1016/j.resconrec.2019.04.012
37. Fan J, Meng J, Ashkenazy Y, Havlin S, and Schellnhuber HJ. Network Analysis Reveals Strongly Localized Impacts of El Niño. *Proc Natl Acad Sci USA* (2017) 114:7543–8. doi:10.1073/pnas.1701214114
38. Meng J, Fan J, Ashkenazy Y, and Havlin S. Percolation Framework to Describe El Niño Conditions. *Chaos* (2017) 27:035807. doi:10.1063/1.4975766
39. Dong H, Geng Y, Fujita T, Fujii M, Hao D, and Yu X. Uncovering Regional Disparity of China's Water Footprint and Inter-provincial Virtual Water Flows. *Sci Total Environ* (2014) 500-501:120–30. doi:10.1016/j.scitotenv.2014.08.094
40. Liu W, Chen J, Tang Z, Liu H, Han D, and Li F. *Theory and Practice of Compiling China 30-province Inter-regional Input-Output Table of 2007*. Beijing: China Statistics Press (2012). (in Chinese).
41. Liu W, Chen J, Tang Z, Liu H, Han D, and Li F. *Input-output Table of China's 30 Provinces, Autonomous Regions and Municipalities in 2010*. Beijing: China Statistics Press (2014). (in Chinese).
42. Cai B, Zhang W, Hubacek K, Feng K, Li Z, Liu Y, et al. Drivers of Virtual Water Flows on Regional Water Scarcity in China. *J Clean Prod* (2019) 207:1112–22. doi:10.1016/j.jclepro.2018.10.077
43. National Bureau of Statistics of China. *China Statistical Yearbook 2008*. Beijing: China Statistics Press (2008).
44. National Bureau of Statistics of China. *China Statistical Yearbook 2011*. Beijing: China Statistics Press (2011).
45. National Bureau of Statistics of China. *China Statistical Yearbook 2013*. Beijing: China Statistics Press (2013).
46. National Bureau of Statistics of China. *China Statistical Yearbook 2016*. Beijing: China Statistics Press (2016).
47. Ministry of Housing and Urban-Rural Development. *China Urban-Rural Construction Statistical Yearbook 2008*. Beijing: China Statistics Press (2008).
48. Ministry of Housing and Urban-Rural Development. *China Urban-Rural Construction Statistical Yearbook 2011*. Beijing: China Statistics Press (2011).
49. Ministry of Housing and Urban-Rural Development. *China Urban-Rural Construction Statistical Yearbook 2013*. Beijing: China Statistics Press (2013).
50. Ministry of Housing and Urban-Rural Development. *China Urban-Rural Construction Statistical Yearbook 2016*. Beijing: China Statistics Press (2016).
51. Miller R, and Blair P. *Input-output Analysis: Foundations and Extensions*. Cambridge: Cambridge University Press (2009).
52. Jiang M, Gao X, Guan Q, Hao X, and An F. The Structural Roles of Sectors and Their Contributions to Global Carbon Emissions: A Complex Network Perspective. *J Clean Prod* (2019) 208:426–35. doi:10.1016/j.jclepro.2018.10.127
53. Bhattacharya S, Sinha S, and Roy S. Impact of Structural Properties on Network Structure for Online Social Networks. *Proced Comput Sci* (2020) 167:1200–9. doi:10.1016/j.procs.2020.03.433
54. Furukoshi A, and Damke M. *System and Method for Operating a Large-Scale Wireless Network*. US (2013). p. US8391183 B2.
55. Wang X, Wei W, Ge J, Wu B, Bu W, Li J, et al. Embodied Rare Earths Flow between Industrial Sectors in China: A Complex Network Approach. *Resour Conservation Recycling* (2017) 125:363–74. doi:10.1016/j.resconrec.2017.07.006
56. Freeman LC. Centrality in Social Networks Conceptual Clarification. *Social Networks* (1978) 1:215–39. doi:10.1016/0378-8733(78)90021-7
57. Carvalho VM. From Micro to Macro via Production Networks. *J Econ Perspect* (2014) 28:23–48. doi:10.1257/jep.28.4.23
58. Pfister S, Koehler A, and Hellweg S. Assessing the Environmental Impacts of Freshwater Consumption in LCA. *Environ Sci Technol* (2009) 43:4098–104. doi:10.1021/es802423e
59. Zhang C, Zhong L, Liang S, Sanders KT, Wang J, and Xu M. Virtual Scarce Water Embodied in Inter-provincial Electricity Transmission in China. *Appl Energ* (2017) 187:438–48. doi:10.1016/j.apenergy.2016.11.052
60. Avazdahandeh S, and Khalilian S. The Effect of Urbanization on Agricultural Water Consumption and Production: the Extended Positive Mathematical Programming Approach. *Environ Geochem Health* (2021) 43:247–58. doi:10.1007/s10653-020-00668-2

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

APPENDIX

TABLE 1A | Provinces and their codes.

Province	Code	Province	Code	Province	Code
Bejing	BJ	Zhejiang	ZJ	Hainan	HI
Tianjin	TJ	Anhui	AH	Chongqing	CQ
Shanxi	SX	Fujian	FJ	Sichuang	SC
Hebei	HE	Jiangxi	JX	Guizhou	GZ
Inner Mongolia	NM	Shandong	SD	Yunnan	YN
Liaoning	LN	Henan	HA	Shannxi	SN
Jilin	JL	Hubei	HB	Gansu	GS
Helongjiang	HL	Hunan	HN	Qinghai	QH
Shanghai	SH	Guangdong	GD	Ningxia	NX
Jiangsu	JS	Guangxi	GX	Xinjiang	XJ

frontiers in Physics

ORIGINAL RESEARCH
published: 20 December 2021
doi: 10.3389/fphy.2021.792410

Network Robustness Analysis Based on Maximum Flow

Meng Cai[1]*, *Jiaqi Liu*[1] *and Ying Cui*[2]

[1]School of Humanities and Social Sciences, Xi'an Jiaotong University, Xi'an, China, [2]School of Mechano-Electronic Engineering, Xidian University, Xi'an, China

Network robustness is the ability of a network to maintain a certain level of structural integrity and its original functions after being attacked, and it is the key to whether the damaged network can continue to operate normally. We define two types of robustness evaluation indicators based on network maximum flow: flow capacity robustness, which assesses the ability of the network to resist attack, and flow recovery robustness, which assesses the ability to rebuild the network after an attack on the network. To verify the effectiveness of the robustness indicators proposed in this study, we simulate four typical networks and analyze their robustness, and the results show that a high-density random network is stronger than a low-density network in terms of connectivity and resilience; the growth rate parameter of scale-free network does not have a significant impact on robustness changes in most cases; the greater the average degree of a regular network, the greater the robustness; the robustness of small-world network increases with the increase in the average degree. In addition, there is a critical damage rate (when the node damage rate is less than this critical value, the damaged nodes and edges can almost be completely recovered) when examining flow recovery robustness, and the critical damage rate is around 20%. Flow capacity robustness and flow recovery robustness enrich the network structure indicator system and more comprehensively describe the structural stability of real networks.

Keywords: network robustness, maximum flow, connectivity, resilience, critical damage rate

OPEN ACCESS

Edited by:
Gaogao Dong,
Jiangsu University, China

Reviewed by:
Guangquan Xu,
Tianjin University, China
Yilun Shang,
Northumbria University,
United Kingdom

***Correspondence:**
Meng Cai
mengcai@mail.xjtu.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *10 October 2021*
Accepted: *29 November 2021*
Published: *20 December 2021*

Citation:
Cai M, Liu J and Cui Y (2021) Network Robustness Analysis Based on Maximum Flow. Front. Phys. 9:792410. doi: 10.3389/fphy.2021.792410

INTRODUCTION

Nowadays, the network exists in every aspect of human life, and our life is convenient and complicated because of the network. Whether it is a technical network such as a computer network or a social network such as an interpersonal relationship, it will inevitably be disturbed or damaged, thus affecting the normal operation of the network, or worse, leading to the paralysis of the network. In the case of interference or disruption, robustness becomes the key to whether the network system can continue to operate normally. Specifically, network robustness describes the ability of a network to maintain a certain level of structural integrity and original functionality after nodes or edges experience random or deliberate attacks [1]. For example, robustness will be the decisive factor when a cell encounters external environmental changes or internal genetic variations, when an ecosystem encounters man-made disturbances and when a piece of computer software encounters disk failures, network overloads, or deliberate attacks [2]. Therefore, the robustness of a complex network has become an important topic of academic research due to the widespread existence of the complex network and the important role it plays for nature and human society. The early researchers of complex network robustness were Albert et al. [3], who pointed out that the

scale-free network is more vulnerable under deliberate attack and more robust when subjected to random attack; Holme et al. [4] conducted an in-depth study on the robustness of the network as reflected by the changes in various indicators under different types of attack; Paul et al. [5] discussed how to effectively improve network robustness; He C-Q et al. [6] summarized the changing trend of robustness under different network topologies; Du W and Cai M et al. [7] proposed connection robustness and recovery robustness based on the connectivity and resilience of the network and selected four types of complex networks, including the random network and the scale-free network, for extensive experiments, and it is concluded that the random network is the best robust to deliberate attacks, and the node resilience of the scale-free network is better than the edge; Lu P-L et al. [8] explored the impact of the initial clustering coefficient on robustness when attacked by different conditions for three complex networks with the same degree distribution and different clustering coefficients and showed that the larger the initial clustering coefficient, the worse is the robustness of the network.

In research studies of the complex network robustness, the establishment of robustness evaluation indicators provides a certain basis for it. To ensure that the evaluation indicators can truly reflect the robustness of the complex network, measurability, sensitivity, and objectivity are required. Nowadays, robustness evaluation indicators generally include the network global effect, average path length, connectivity, relative size of the maximum connected subgraph, betweenness, circle rate, clustering coefficient [9], *k*-core structure [10, 11], core [12], and generalized *k*-cores [13, 14]. Among them, as the level of network damage caused by the attack increases, the average shortest path becomes larger and then smaller [9], and this trend of change is not a significant guide for practical applications; the betweenness index takes into account the changes of nodes and edges in the network but does not consider changes in the network size and structure as a whole [9]; the clustering coefficient reflects the tightness of connections between nodes in the network and is also an indicator of local change in the network; considering the maximum connected subgraph, the robustness of the complex network is defined as the size of the maximum connected subgraph in the network after randomly or deliberately removing a certain percentage of nodes from the network [15]; in single networks, *k*-core is defined as a maximal set of nodes that have at least *k* neighbors within the set [16], and the generalized *k*-core (*Gk*-core) is a core structure, which is obtained by implementing a *k*-leaf pruning procedure that progressively removes nodes with degree less than *k* alongside their nearest neighbors [14]. It can be seen that the existing robustness evaluation indicators mostly consider local changes in the network. No research has been carries out to measure robustness from the perspective of network flow, a metric that describes the global topology of the network, and it can reflect the structural characteristics of network connections comprehensively and break the limitations on network weights and propagation methods [17]. In addition, the failure mechanism of the nodes when the network is attacked is also an important factor in network robustness analysis [1]. Most of the existing studies have focused on the mechanism of system failure, but in real life, except the occurrence of failure, it also includes the repair of failure, which is the recovery of damaged nodes or edges according to certain recovery mechanisms. Therefore, it is necessary to consider the resilience after the network is damaged in the construction of the network robustness evaluation indicators.

In this study, we propose two types of network structural robustness measurement indicators, namely, capacity robustness based on maximum flow and recovery robustness based on maximum flow, in terms of the ability of the network to resist damage and the ability of the network structure to recover after damage, respectively. We use non-global information to recover deleted nodes and edges after the network is destroyed. In order to verify the effectiveness of the robustness indicators proposed in this study, we perform robustness experimental analysis on several typical networks such as the BA scale-free network (a scale-free network proposed by Barabasi and Albert), ER random network (a random network proposed by Erdos and Renyi), nearest neighbor coupled (NNC) regular network, and WS small-world network (a small-world network proposed by Watts and Strogatz) and finally explore the relationship between network structure characteristics and network structure robustness.

MATERIALS AND METHODS

Related Work

The complex network theory emerged in the 1960s and generally refers to the network with some or all of the properties in self-organization, self-similarity, attractor, small-world, and scale-free [9]. The complex network is an abstract complex system whose complexity is mainly reflected in the number of connected nodes and its complex topological structure. It is often used to study the structural properties, formation mechanisms, and evolution laws of the real network. The network robustness and destruction resistance are important parts of the current research on complex networks.

Generally, when a network is attacked, depending on intensity and extensity of error, the attacked nodes are impaired to become non-functional nodes or partially functional nodes (nodes as being a state that is functional but not at full power) [18], and these lost functions will be shared by the coupling relationships of neighboring nodes. This additional functional commitment puts a lot of pressure on the normal operation of the neighboring nodes and the entire network system, and in severe cases, it may lead to failure of other nodes or a whole network crash. The ability to maintain the function and property of the network that the damaged network has is network robustness. Similar to robustness, destruction resistance indicates the performance changes when a network is under attack. The difference is that the destruction resistance prefers the ability to maintain or recover to an acceptable level when the network is damaged.

Existing correlational researches mostly focus on the measurement of the robustness and destruction resistance of the network, make structural optimizations to them, and

further apply them in relevant practical areas: In an earlier study, Albert et al. [3] compared the robustness of ER network and scale-free (SF) network under deliberate and random attacks, and the results showed that SF network is significantly more robust than ER network during random attack, while the robustness of SF network is much less weak under deliberate attack, and simply deleting a small number of nodes with the largest degree may cause the network to collapse completely. Cohen et al. proposed the theoretical analytical conditions for network collapse under random attack based on percolation theory and applied them to the Internet and found high robustness of the Internet against random attack [19]; then they analyzed the robustness of SF network such as the Internet under deliberate attack through theoretical calculations and numerical simulations and argued that the Internet is highly sensitive and vulnerable to deliberate attack [20]. Darren et al. [21] achieved the identification of road segment importance using the road network robustness index and considered the road network robustness index in terms of topological attributes, capacity, and traffic flow characteristics of the road segments in the network. Tan Y-J and Wu J et al. [22] conducted research from the analysis and optimization of destruction resistance, proposed the influence of network aggregation and mixing on destruction resistance of network, and combined with the actual network researches to analyze optimization and control of destruction resistance, which provided a direction for the study of destruction resistance of complex network at that time. Du W and Cai M et al. [7] proposed connectivity robustness and recovery robustness based on the connectivity and recovery ability of the network and simulated a certain scale of regular network, small-world network, scale-free network, and random network for a large number of experiments, and it is concluded that random network has the best robustness against deliberate attack compared with the other three networks and that the node resilience of scale-free network is better than the edge resilience. Based on the complex network theory, Lu S [23] selected an aviation system as the research object modeled and analyzed the aviation network using Pajck software, summarized the changes of various parameters in the system, and proposed ideas to improve the robustness of air cargo. Focusing on interdependent networks, Dong G-G [24] et al. investigated the case of interdependent networks by generalizing feedback and non-feedback conditions, and specifically, they developed a new mathematical framework and used percolation theory to investigate numerically and analytically the percolation of interdependent networks with partial multiple-to-multiple dependency links. Shi H [25] proposed a shock resistance assessment method based on complex network, using peak ground acceleration as a reference to assess the destruction resistance of complex network buildings in an earthquake environment, and the assessment results were consistent with reality, which helped the timely measurement of building shock resistance. Dong G-G and Wang F et al. [26] developed two types of coupled giant network theoretical research frameworks, “deterministic coupled modes” and “coupled modes under arbitrary distribution”, to study the resilient behavior of the system, and concluded that there is indeed an optimum coupling structure among the subnetworks, which makes the entire system has the best connectivity and destruction resistance. Mariani et al. [27] focused on one of the non-random structure patterns in networks—nestedness, and concentrated on their discussion on three main aspects: the existing methodologies to nestedness in networks, the key theoretical mechanisms to explain nestedness in ecological and socioeconomic networks, and implications of the nested topology of interactions for the stability and viability of a given interacting systems. Wuellner et al. [28] analyzed the individual structures of the seven largest U.S. passenger carriers and found that networks with dense interconnectivity are extremely resilient to both targeted removal of airports (nodes) and random removal of flight paths (edges), and here, they measured the interconnectivity of the network using the *k-core* structure, which is a subgraph of the network constructed by iteratively pruning all vertices with a degree less than *k*. Shang Y-L [14] developed a mathematical framework for understanding the robustness of networks based on the number of nodes and edges in the *Gk*-core (a generalization of the ordinary *k*-core decomposition) under two general attacks with limited knowledge (min-n and max-n attacks), and it was found that knowing one more node (from n = 1 to n = 2) during attacks is most beneficial in terms of changing the robustness of the *Gk*-core. Therefore, research studies related to network robustness can help people understand the mechanisms and rules of network system failure or collapse and can identify better ways to prevent the failure of real network systems and build more robust systems, making real life more stable [29].

It can be seen that the research studies on network robustness pay more attention to measurement models and indicator changes and are devoted to the optimization of network destruction resistance and defense capability, while the in-depth studies of network resilience performance are not as mature as the research on network robustness. Resilience is the ability of a system to recover from an unfavorable state to a normal state (i.e., the initial state, or adjust itself to a new state according to new demands or conditions), which reflects the system’s adaptability and survivability [30]. Through the propagation and diffusion effects of the network, the behavior and recoverability of the nodes in the network can have a significant impact on the resilience of the network community and the entire network; at the same time, by adjusting the network structure and characteristics, the overall local and node-level resilience of the network will be optimized [31]. Thus, network resilience, although a relatively new concept, is an important field of network research.

Bai Y-N et al. [32] stated that a coupled network can be recovered only when the proportion of failed nodes in that network is less than the resilience threshold. In recent years, some scholars have further explored the influencing factors of network resilience performance and concluded that the coupling strength of the coupled network [33], the node recovery order of the dependent network [34], and the node importance ranking of the fault network [35] all have impact on the network resilience performance. Some scholars have optimized the network recovery model based on the equal probability recovery mechanism [36] and proposed a weighted probability recovery mechanism [35]. However, we can find that existing studies on

network resilience measurements mostly focus on different typical networks and different network sizes, and network resilience is analyzed by comparing the number of nodes after recovery of the damaged network and the number of original network nodes, ignoring the impact of the network structure on the overall network function. The number of nodes, node-to-node connections, change in the overall structural characteristics of the network, and the magnitude of the change after recovery of the damaged network are important elements in the study of network resilience.

Definition of Structural Robustness Indicators Based on Maximum Flow

Network Model and Related Definitions

For a given capacity-containing network denoted as $G = (V, E, c)$, where $V = \{v_1, v_2, \ldots, v_n\}$ is the set of nodes, $E = \{(v_i, v_j) | \, v_i, v_j \in V\}$ is the set of edges, (v_i, v_j) is the outgoing arc of node v_i and is also the incoming arc of the node v_j, c is the capacity set of edges, and the set element $c(v_i, v_j)$ represents the capacity of the edge (v_i, v_j), when G is the directed network, set c is symmetric, namely, $c(v_i, v_j) = c(v_j, v_i)$, and when G is an undirected network, set c is asymmetric. In the capacity network $G = (V, E, c)$, the flow from the source point v_s to the sink point v_t is denoted as f_{st}. Suppose f_{st} meets the following requirements (see **Eqs 1**, **2**):

$$\sum_j \boldsymbol{f}(v_i, v_j) - \sum_j \boldsymbol{f}(v_j, v_i) = \begin{cases} \boldsymbol{f_{st}}, & v_i = v_s \\ \boldsymbol{0}, & v_i \neq v_s, v_t \\ \boldsymbol{-f_{st}}, & v_i = v_t \end{cases}, \tag{1}$$

$$\boldsymbol{0} \leq \boldsymbol{f}(v_i, v_j) \leq \boldsymbol{c}(v_i, v_j), \ \forall (v_i, v_j) \in \boldsymbol{E}, \tag{2}$$

then f_{st} is one of the feasible flows of the capacity network G. If this flow is the largest of all feasible flows, it is called the maximum flow and is denoted as f_{max} [15]. (v_i, v_j) is the edge of the directed network, and for the undirected network, it is expressed as $\{v_i, v_j\}$.

Network Robustness Based on Maximum Flow

Complex network robustness refers to the ability of a network to remain connected even under random or deliberate attack, and its concept is widely used in various fields such as physics, sociology, and transportation. In the presence of uncertainty and crisis, robustness has become critical to whether the system can continue to operate. The existing robustness indicators mainly consider whether the network is connected or not and reflect the robustness of the network after a disruption from the network structure, that is, it only considers whether the nodes are connected or not but does not measure whether the circulation between the nodes is damaged. The network maximum flow considers not only whether the connections of nodes exist but also how the transmission capacity of the already existing nodes and connections, that is, it considers both the fact of existence and the quality of existence of the nodes. Therefore, in view of the maximum flow's ability to characterize the connectivity of the network structure, this study uses maximum flow as a basic index to evaluate the robustness of the network and then proposes "capacity robustness based on maximum flow" and "recovery robustness based on maximum flow," and the former reflects the ability of the network structure itself to resist attacks, while the latter reflects the resilience of the network after damage [7].

Capacity Robustness Based on Maximum Flow

Capacity robustness based on maximum flow (later referred to as flow capacity robustness) is the ability of the remaining nodes in the network to maintain circulation among themselves after some nodes have been damaged by an attack. There are two general ways to attack a network: one is a deliberate attack and the other is a random attack. The former refers to a purposeful and planned attack on the network such as prioritizing attacks on the more important nodes or edges; the latter refers to a network in which nodes or edges are attacked in a certain proportion at random. In this study, two types of damage strategies are used: deliberate attack and random attack. Specifically, a deliberate attack is to select the top n% of nodes with the largest degree to destroy, and a random attack is to randomly select n% of nodes for damage, and both strategies use one-time damage.

First, the network maximum flow matrix W is defined as the matrix consisting of the maximum flow values between all pairs of nodes in the network (see **Eq. 3**):

$$\boldsymbol{W} = \begin{bmatrix} \boldsymbol{0} & \boldsymbol{c}_{f_{max}}(\boldsymbol{v}_1, \boldsymbol{v}_2) & \cdots & \boldsymbol{c}_{f_{max}}(\boldsymbol{v}_1, \boldsymbol{v}_N) \\ \boldsymbol{c}_{f_{max}}(\boldsymbol{v}_2, \boldsymbol{v}_1) & \boldsymbol{0} & \cdots & \boldsymbol{c}_{f_{max}}(\boldsymbol{v}_2, \boldsymbol{v}_N) \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{c}_{f_{max}}(\boldsymbol{v}_N, \boldsymbol{v}_1) & \boldsymbol{c}_{f_{max}}(\boldsymbol{v}_N, \boldsymbol{v}_2) & \cdots & \boldsymbol{0} \end{bmatrix}, \tag{3}$$

where N is the size of the network $G = (V, E, c)$; $V = \{v_1, v_2, \ldots, v_N\}$ is the set of nodes, $c_{f_{max}}(v_i, v_j)$ is the maximum flow value between nodes v_i and v_j, and $c_{f_{max}}(v_i, v_i) = 0$. Note that the method applies not only to directed network but also to the undirected network, and not only to 0–1 network but also to the weighted network. The difference in application to different networks lies in the calculation of maximum flow. For example, in the undirected network, $c_{f_{max}}(v_i, v_j) = c_{f_{max}}(v_j, v_i)$; in the directed network, $c_{f_{max}}(v_i, v_j) \neq c_{f_{max}}(v_j, v_i)$. Similarly, for 0–1 network and weighted network, the corresponding maximum flow matrix is calculated to bring in the method.

Then V_d is defined as the set of damaged nodes, N_d is the number of nodes in V_d, $p = n$% is the node damage rate, $N_d = pN$, V_s is the set of remaining nodes in the network after destruction, N_s is the number of nodes in V_s, and $V = V_d + V_s$ means the set V is equal to the union of the set V_d and the set V_s. Therefore, the damaged network satisfies $G_s^* = (V_s, E_s, c_s)$, where E_s is the set of edges of the network G_s^*, and c_s is the capacity set of edges.

Based on the maximum flow matrix, W_c is defined as the matrix after removing the nodes in the set V_d from the maximum flow matrix W at one time (see **Eq. 4**):

$$\boldsymbol{W_c} = \begin{bmatrix} \boldsymbol{0} & \boldsymbol{c}_{f_{max}}(\boldsymbol{v}_i, \boldsymbol{v}_{i+1}) & \cdots & \boldsymbol{c}_{f_{max}}(\boldsymbol{v}_i, \boldsymbol{v}_{i+N_s-1}) \\ \boldsymbol{c}_{f_{max}}(\boldsymbol{v}_{i+1}, \boldsymbol{v}_i) & \boldsymbol{0} & \cdots & \boldsymbol{c}_{f_{max}}(\boldsymbol{v}_{i+1}, \boldsymbol{v}_{i+N_s-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{c}_{f_{max}}(\boldsymbol{v}_{i+N_s-1}, \boldsymbol{v}_i) & \boldsymbol{c}_{f_{max}}(\boldsymbol{v}_{i+N_s-1}, \boldsymbol{v}_{i+1}) & \cdots & \boldsymbol{0} \end{bmatrix}, \tag{4}$$

where $c_{f_{max}} \in W$ and node $v_i \in V_s$.

W_c^* is defined as the maximum flow matrix recomputed from the damaged network (see **Eq. 5**):

$$W_c^* = \begin{bmatrix} 0 & c^*_{f_{max}}(v_i, v_{i+1}) & \cdots & c^*_{f_{max}}(v_i, v_{i+N_s-1}) \\ c^*_{f_{max}}(v_{i+1}, v_i) & 0 & \cdots & c^*_{f_{max}}(v_{i+1}, v_{i+N_s-1}) \\ \vdots & \vdots & \ddots & \vdots \\ c^*_{f_{max}}(v_{i+N_s-1}, v_i) & c^*_{f_{max}}(v_{i+N_s-1}, v_{i+1}) & \cdots & 0 \end{bmatrix}, \tag{5}$$

where $c^*_{f_{max}} \notin W$, that is, $c^*_{f_{max}}$ is the maximum flow matrix calculated from the network G_s^*; node $v_i \in V_s$. It is important to state that the maximum flow takes into account not only the fact that the nodes are connected to each other but also more importantly, the quality of the transmission between the nodes. That means the disruption or attack will lead to a reduction in the quality of data transmission, even if the connectivity is intact. Therefore, the recomputed maximum flow matrix, even if the nodes are still connected to each other, may produce a change in the quality of the traffic and thus affect the overall network transmission capacity.

Finally, the flow capacity robustness C is defined as follows (see **Eq. 6**):

$$\begin{aligned} C &= \frac{\sum W_c^*}{\sum W_c} \\ &= \frac{\sum \begin{bmatrix} 0 & c^*_{f_{max}}(v_i, v_{i+1}) & \cdots & c^*_{f_{max}}(v_i, v_{i+N_s-1}) \\ c^*_{f_{max}}(v_{i+1}, v_i) & 0 & \cdots & c^*_{f_{max}}(v_{i+1}, v_{i+N_s-1}) \\ \vdots & \vdots & \ddots & \vdots \\ c^*_{f_{max}}(v_{i+N_s-1}, v_i) & c^*_{f_{max}}(v_{i+N_s-1}, v_{i+1}) & \cdots & 0 \end{bmatrix}}{\sum \begin{bmatrix} 0 & c_{f_{max}}(v_i, v_{i+1}) & \cdots & c_{f_{max}}(v_i, v_{i+N_s-1}) \\ c_{f_{max}}(v_{i+1}, v_i) & 0 & \cdots & c_{f_{max}}(v_{i+1}, v_{i+N_s-1}) \\ \vdots & \vdots & \ddots & \vdots \\ c_{f_{max}}(v_{i+N_s-1}, v_i) & c_{f_{max}}(v_{i+N_s-1}, v_{i+1}) & \cdots & 0 \end{bmatrix}} \\ &= \frac{\sum_{v_i, v_j \in V_s} c^*_{f_{max}}(v_i, v_j)}{\sum_{v_i, v_j \in V_s} c_{f_{max}}(v_i, v_j)}. \end{aligned} \tag{6}$$

Recovery Robustness Based on Maximum Flow

In the real world, if it is difficult to obtain information about a specific individual, the information can be recovered to some extent by asking people who are related to the individual, and similar approaches have been used to find keyman in terrorist groups through connections between network nodes [37]. In this study, we recover the network through non-global information and define recovery robustness based on maximum flow (later referred to as flow recovery robustness), for example, the ability to recover disappeared network structure elements (broken nodes and edges) from information related to unbroken nodes after some nodes in a network have been attacked. **Figure 1** visualizes the network structure of a network after attack and recovery. Specifically, **Figure 1A** shows a network of size 10 with node set $V = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and edge set E. We attack the network by removing the nodes and corresponding edges of the node set $V_d = \{2, 3, 4, 9\}$ (red points and edges in **Figure 1A**), and the damaged network is shown in **Figure 1B**. After that, the network is

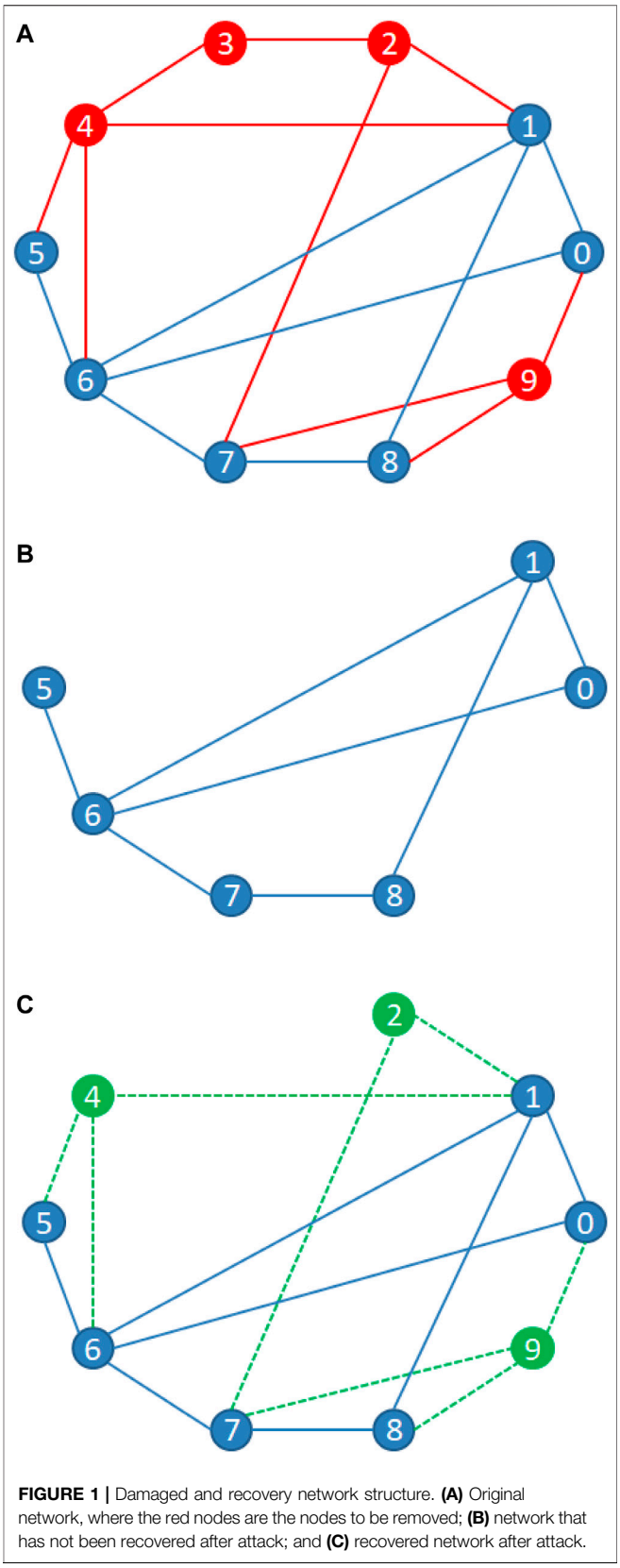


FIGURE 1 | Damaged and recovery network structure. **(A)** Original network, where the red nodes are the nodes to be removed; **(B)** network that has not been recovered after attack; and **(C)** recovered network after attack.

recovered by the information of the remaining nodes of the network, where the set of recovered nodes $V_r = \{2, 4, 9\}$ (in **Figure 1C**, the recovered nodes and edges are represented by green notes and green dashed lines, respectively) and the set of unrecovered nodes $V_u = \{3\}$. And, it can be seen that node 9 is a fully recovered node (i.e., both the node and the corresponding edges are fully recovered) and nodes two and four are not fully recovered nodes (that is, the node is recovered and the corresponding edges are not fully recovered).

We define $G_r^* = (V_r, E_r, c_r)$ as the recovered network based on the damaged network $G_s^* = (V_s, E_s, c_s)$, where V_r is the set of nodes of the recovered network based on the information related to the nodes in V_s, N_r is the number of nodes in the set V_r, E_r is the set of edges of the network G_r^*, and c_r is the capacity set of edges; when V_u is the set of unrecovered nodes, then $V = V_r + V_u$ means the set V is equal to the union of the set V_r and the set V_u.

Based on the maximum flow matrix, W_r is defined as the matrix that removes the nodes in the set V_u from the maximum flow matrix W at one time (see **Eq. 7**); that is, it retains the nodes in the recovered network:

$$W_r = \begin{bmatrix} 0 & c_{f_{max}}(v_i, v_{i+1}) & \cdots & c_{f_{max}}(v_i, v_{i+N_r-1}) \\ c_{f_{max}}(v_{i+1}, v_i) & 0 & \cdots & c_{f_{max}}(v_{i+1}, v_{i+N_r-1}) \\ \vdots & \vdots & \ddots & \vdots \\ c_{f_{max}}(v_{i+N_r-1}, v_i) & c_{f_{max}}(v_{i+N_r-1}, v_{i+1}) & \cdots & 0 \end{bmatrix}, \tag{7}$$

where $c_{f_{max}} \in W$ and node $v_i \in V_r$.

W_r^* is defined as the maximum flow matrix recomputed according to the recovered network (see **Eq. 8**):

$$W_r^* = \begin{bmatrix} 0 & c_{f_{max}}^*(v_i, v_{i+1}) & \cdots & c_{f_{max}}^*(v_i, v_{i+N_r-1}) \\ c_{f_{max}}^*(v_{i+1}, v_i) & 0 & \cdots & c_{f_{max}}^*(v_{i+1}, v_{i+N_r-1}) \\ \vdots & \vdots & \ddots & \vdots \\ c_{f_{max}}^*(v_{i+N_r-1}, v_i) & c_{f_{max}}^*(v_{i+N_r-1}, v_{i+1}) & \cdots & 0 \end{bmatrix}, \tag{8}$$

where $c_{f_{max}}^* \notin W$; that is, $c_{f_{max}}^*$ is the maximum flow matrix calculated from the network G_r^*; node $v_i \in V_r$.

Finally, the flow recovery robustness R is defined as follows (see **Eq. 9**):

$$R = \frac{\sum W_r^*}{\sum W_r} = \frac{\sum \begin{bmatrix} 0 & c_{f_{max}}^*(v_i, v_{i+1}) & \cdots & c_{f_{max}}^*(v_i, v_{i+N_r-1}) \\ c_{f_{max}}^*(v_{i+1}, v_i) & 0 & \cdots & c_{f_{max}}^*(v_{i+1}, v_{i+N_r-1}) \\ \vdots & \vdots & \ddots & \vdots \\ c_{f_{max}}^*(v_{i+N_r-1}, v_i) & c_{f_{max}}^*(v_{i+N_r-1}, v_{i+1}) & \cdots & 0 \end{bmatrix}}{\sum \begin{bmatrix} 0 & c_{f_{max}}(v_i, v_{i+1}) & \cdots & c_{f_{max}}(v_i, v_{i+N_r-1}) \\ c_{f_{max}}(v_{i+1}, v_i) & 0 & \cdots & c_{f_{max}}(v_{i+1}, v_{i+N_r-1}) \\ \vdots & \vdots & \ddots & \vdots \\ c_{f_{max}}(v_{i+N_r-1}, v_i) & c_{f_{max}}(v_{i+N_r-1}, v_{i+1}) & \cdots & 0 \end{bmatrix}} = \frac{\sum_{v_i, v_j \in V_r} c_{f_{max}}^*(v_i, v_j)}{\sum_{v_i, v_j \in V_r} c_{f_{max}}(v_i, v_j)}. \tag{9}$$

In order to explore the relationship between the aforementioned robustness indicators and the network topology, this study analyzes and verifies them through simulation experiments of typical networks.

RESULTS

Four Typical Network Structures

In general, network models can be divided into three categories [38]: the first category is the random network; the second category is the regular network; and the third category is network structures between random and regular networks, which have some characteristics of both regular and random networks, including scale-free network and small-world network. In this study, four types of typical network, including regular network, random network, scale-free network, and small-world network, will be analyzed for structural robustness using the robustness indicators based on maximum flow.

Regular Network

A regular network is the network structure obtained by connecting nodes according to defined rules, and its structure is symmetric. A nearest neighbor coupled network and star network are two typical types of the regular network. In this study, we use the nearest neighbor coupled network (NNC) as the test network; that is, for a given even value of k, the N nodes in the network are connected to a ring, where each node is connected to only $k/2$ neighboring nodes.

BA Scale-free Network

The concept of the scale-free network started with an article by Barabasi and Albert published in ⟪Science⟫ in 1999 [39]. By studying the topology of the World Wide Web, they found that the node degree distribution obeys a power law distribution and proposed a classical model (BA model) for constructing a scale-free network. The initial number of nodes in the network is u_0, and the growth rate is u. Through growth and meritocratic connection, the probability that a new node is connected to an already existing node v_i in the network is $\Pi_i = \frac{k_i}{\sum_j k_j}$, and a scale-free network of size $N = t + u_0$ nodes and ut edges is formed after time t. The node degree obeys the probability distribution of $p(k) = \frac{2u^2}{k^3}$. Most nodes in a scale-free network are connected to only a few nodes, while a small number of nodes have an extremely large number of node connections.

ER Random Network

The ER random network was proposed by Erdos and Renyi in 1960 [40], and it is one of the main reference models for network research. The connections between network nodes of a random network are random, given the network size N and the total number of edges n, any two nodes, are connected at a time with probability $q = \frac{2n}{N(N-1)}$ without repetition until the total number of edges of the network reaches n, and an ER random network is obtained. The degree values of most nodes in the network are concentrated around a particular value, the average degree $k = q(N-1)$, and the degrees of nodes obey

the Poisson distribution $P(k) = \frac{e^{-\lambda}\lambda^k}{k!}$, where λ is the average incidence of random events per unit time.

WS Small-World Network

A small-world network is a type of network with short mean path lengths and high clustering coefficients. The first to propose a method for constructing a small-world network were Watts and Strogatz [41]. The specific construction algorithm is as follows:

1) Constructing a regular network encloses a nearest neighbor coupled network containing N nodes to a ring, where each node is connected to the $k/2$ nodes adjacent to its left and right, where$k$ is an even number.
2) Random reconnection randomly reconnects each edge in a regular network with probability p, that is, leaving one end of the edge unchanged and connecting the other endpoint randomly at a new location, but self-connections and repeated connections should be excluded.

$p = 0$ corresponds to the nearest neighbor coupled network, $p = 1$ corresponds to the ER random network, and $0 < p < 1$ corresponds to the WS small-world network, which is a transitional network between the regular network and random network, taking into account the characteristics of both.

Simulation Experiment and Discussion

The simulation experiments were all implemented using Python 3.8 programming. Our method is applicable to many types of networks, such as the directed network, undirected network, 0–1 network, and weighted network, but in order to facilitate comparison with other methods and to focus on reflecting the impact of differences in the network structure on robustness, the networks chosen for the experiments were all undirected and unweighted 0–1 benchmark networks; that is, the same maximum flow value between the same node pairs $c_{f_{max}}(v_i, v_j) = c_{f_{max}}(v_j, v_i)$. The size N of all four typical networks was incremented from 50 to 550, with steps of 10 from 50 to 100 and 30 from 100 to 550. Specifically, the average degree of the NNC regular network was incremented from 2 to 20 in steps of 2, and the average degree here is the average number of neighboring nodes of each node; ER random network density increased from 0.01 to 0.1 in steps of 0.01 and from 0.1 to 0.5 in steps of 0.1, and it should be noted that the network density is numerically equal to the probability of connection q between two points; the growth rate of BA scale-free network increased from 2 to 20 in steps of 2, and the growth rate indicates the number of edges added to the network per unit of time; the average degree of the WS small-world network increased from 2 to 10 in steps of 2, and the reconnection probability increased from 0.002 to 0.01 in steps of 0.002 and then from 0.01 to 0.1 in steps of 0.01. It should be noted that the experimental results are the statistical mean of 10 independent randomized experiments.

The attack strategies used in this study are random attack and deliberate attack. The random attack randomly selects n% of the nodes from the network nodes for damage, and the deliberate attack selects the top n% of the nodes with the largest degree value in the network for damage, where the damage rate n% is taken as [1, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70%]. The network recovery strategy used in the experiment is a non-global information-based network recovery, that is, the network is restored by adding points and edges to the network using the information of neighboring nodes and edges of the remaining nodes in the network after the damage. For ease of understanding, we provide a brief explanation of attack and recovery strategies based on real-life scenarios: a random attack in the definition can be understood as natural disasters (such as earthquakes), which occur independent of human factors and attack humans at random; a deliberate attack can be understood as traffic jams, road controls, and accidents caused by human factors, or in the case of police arrest operation, the collapse of an entire criminal organization by arresting the key figures. For a non-global information recovery strategy, project onto the social interactions, if it is difficult to obtain information about a particular individual, a feasible approach is to recover information about the individual to some extent by asking people who are related to the individual, and a similar strategy has been used to find key individuals in terrorist groups [37]. In order to facilitate the comparison of network parameters and network structures, we fixed the network size N, so this article only analyzes the experimental results of the network size of 100.

Analysis of Experimental Results of Flow Capacity Robustness

Figure 2 gives the changing situation of the flow capacity robustness for BA scale-free network of size 100, where **Figure 2A** and **Figure 2B** show the flow capacity robustness under deliberate and random attacks with the change in the node damage rate and growth rate, respectively, and **Figure 2C** shows the difference in flow capacity robustness under two types of attacks. From **Figure 2A** and **Figure 2B**, it can be seen that the overall network flow shows a significant decreasing trend as the node damage rate increases, regardless of whether it is a deliberate attack or a random attack. Specifically, when the network is deliberately attacked, the circulation capacity of the BA scale-free network, which has a small network growth rate, decreases rapidly when the nodes start to be damaged, showing the "emergent" phenomenon. It shows that the network with a small growth rate is more dependent on nodes with a larger degree, and only a few nodes with a large degree are damaged deliberately and can have a significant influence on the network, while the increase in the network growth rate can improve the flow capacity robustness. In contrast, for a BA scale-free network under random attack, the network growth rate has little effect on its flow capacity robustness, and there is almost a synchronous trend under different growth rates. **Figure 2C** shows the change in the difference between the flow capacity robustness under random attack minus the flow capacity robustness under deliberate attack (all similar differences below are for random attack minus deliberate attack, referred to as the flow capacity robustness difference). It can be seen that the flow capacity robustness differences are all greater than 0, reflecting to some extent that the robustness of the BA scale-free network against a random attack is better than that of the network against a deliberate attack. And the larger the growth rate of the

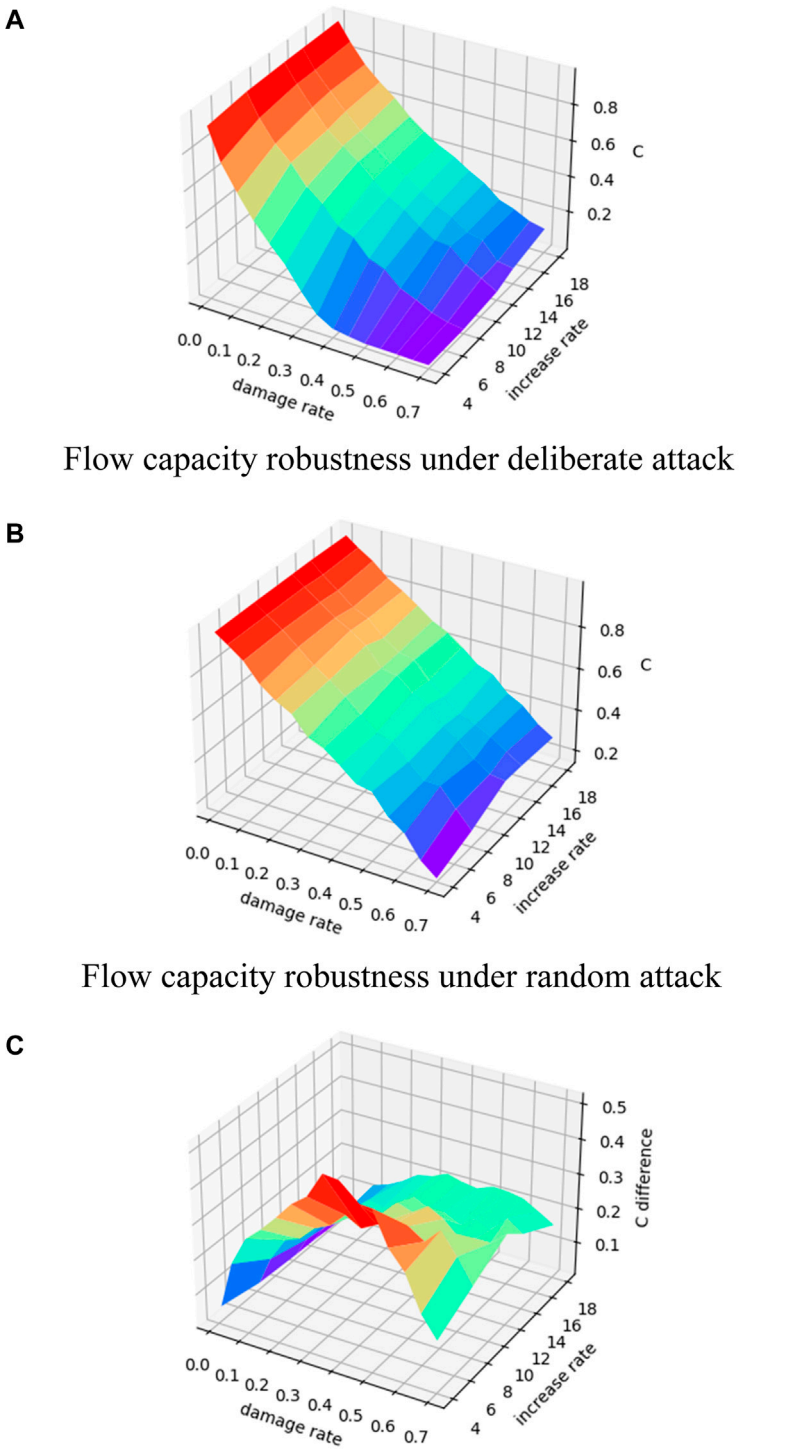


FIGURE 2 | Changes in flow capacity robustness of the BA scale-free network. **(A)** Change in flow capacity robustness under different damage rates and increase rates for BA scale-free network under deliberate attack; **(B)** change in flow capacity robustness under different damage rates and increase rates for BA scale-free network under random attack; **(C)** change in the difference between the flow capacity robustness under random attack minus the flow capacity robustness under deliberate attack.

network, the smaller is the flow capacity robustness difference, while the network with a larger growth rate has smoother flow capacity robustness change as the node damage rate increases.

Figure 3 shows the results of the flow capacity robustness of the ER random network with size 100. It can be seen that the flow capacity robustness shows a decreasing trend with increasing node damage rate under both attack strategies, and the change of node damage rate brings an unstable change in network flow when network density is small (around 0.1). In contrast, network flow decreases smoothly at higher network densities. A deliberate attack can cause the "emergent" phenomenon of the ER random network with low network density when the node damage rate is small, suggesting that the flow capacity robustness of the low-density random network is more dependent on nodes with higher degrees. From **Figure 3C**, it can be seen that the flow capacity robustness difference is greater at smaller network densities (around 0.1), indicating that a low-density random network is not truly "random," and therefore, the destructiveness of a deliberate attack in a low-density ER random network is much higher than that in a random attack. As network density increases, the gap between the destructiveness of the two attack strategies narrows significantly.

The flow capacity robustness results for an NNC regular network of size 100 are shown in **Figure 4**. The results show that the trend of network flows for deliberate and random attacks is very similar, that is, the overall decreases with the increase in the node damage rate, and an early "emergent" phenomenon of the flow capacity robustness emerges earlier in the regular network with a small average degree. Unlike the BA scale-free network and ER random network, the "emergent" phenomenon occurs in the NNC regular network under a random attack, that is, it is most sensitive to the initially disrupted 10% of nodes, and network flow decreases rapidly. This is also consistent with the case that NNC regular network nodes' degree is the same, indicating that random and deliberate attacks have the same effect on the regular network. The change in the flow capacity robustness difference is also concentrated in a narrow range ([-0.025,0.025]), which indicates that the two attack strategies do not differ much for the NNC regular network and confirms that the same value of node degree of the regular network makes the two attacks essentially indistinguishable.

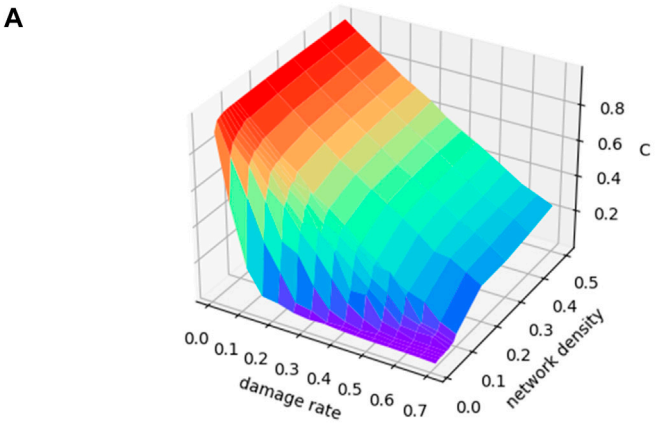
Figure 5 shows the experimental results of the flow capacity robustness for a WS small-world network of size 100, average degree 10, and reconnection probability increasing from 0.002 to 0.1. With the increases in the node damage rate, the overall network flow still shows a decreasing trend, but it can be seen that the flow capacity robustness under random attack decreases more regularly and smoothly, while the flow capacity robustness with a small reconnection probability does not change significantly during a deliberate attack (**Figure 5A**). From the results of the change of the flow capacity robustness difference, the difference at low reconnection probability and high damage rate is more obvious, and the destructive effect of a deliberate attack is significantly higher than that of a random attack.

The results of the flow capacity robustness experiments with a size of 100, a fixed reconnection probability of 0.1, and a mean degree increasing from 2 to 10 are shown in **Figure 6**. It can be seen that under the two attack methods, the smaller the network average, the earlier is the "emergent" phenomenon, and with the damage intensity increases, the overall network flow still shows a downtrend. The flow capacity robustness difference shows a large variation with the node damage rate's change at smaller average degree; specifically, the change from a positive to negative flow robustness difference is accompanied by the change from a small to large node damage rate.

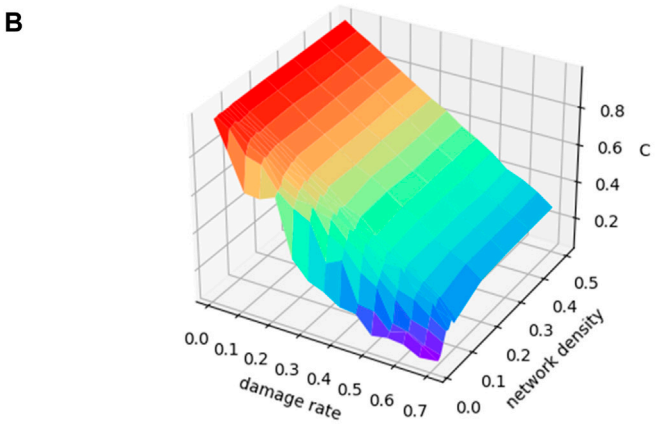
Based on the previous experiments, **Figure 7** shows how the flow capacity robustness indicator of several representative network parameters changes with the increase in the node damage rate, and the corresponding error bars are also shown in the figure, which is the standard of the mean (standard error).

For a deliberate attack (**Figure 7A**), an "emergent" phenomenon of a low-density ER random network is more obvious, and almost no "emergent" phenomenon occurs for higher network densities, with a smooth decrease in network flow transmission capability. As for a BA scale-free network, although the flow capacity robustness is not as good as that of the high-density ER random network, it also shows a relatively stable downtrend, and the network flow transmission capacity of a low growth rate decreases faster than that of a high-growth network. The network flow transmission capability of an NNC regular network is similar to that of a BA scale-free network, and both show a steady decline. For a WS small-world network, when the network average degree is fixed, the smaller the reconnection probability, the larger is the flow capacity robustness and the more robust is the network. This also reflects small-world network between theeregular network and random network, where the higher the reconnection probability and the closer to random network, the more fragile is the network; conversely, the closer to the regular network, the more stable is the network. When network reconnection probability is fixed, the larger the average degree, the stronger is the network flow transmission capability and the greater is the flow capacity robustness; on the contrary, the weaker the network flow transmission capability and the smaller the flow capacity robustness. It can be seen that there are several small-scale rebounds in the network flow capacity robustness, which is due to the fact that the nodes with the same degree value are not unique and the order of nodes of two adjacent attacks is much more likely different, that is, the $n + 1$ th attack is not necessarily carried out on the basis of the nth damaged node, which leads to a rebound of robustness in a small range. It can be seen that the error bars in some results are relatively obvious, which may be related to the network size and the number of experiments repeated.

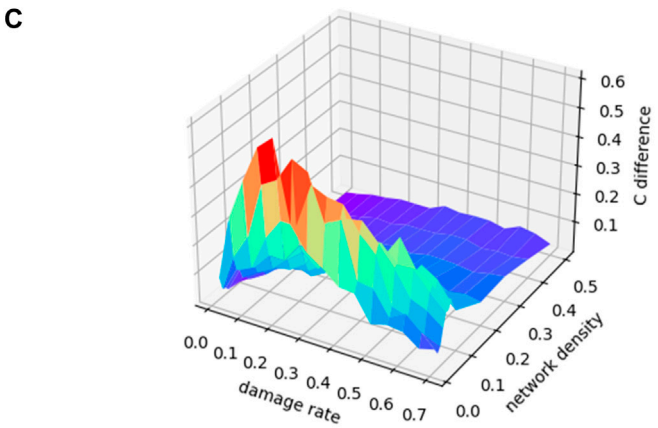
For random attack (**Figure 7B**), in the ER random network, the low-density network appears "emergent" phenomenon faster, and the trend of change is unstable. In contrast, the growth rate of the BA scale-free network is not as sensitive to the random attack as deliberate attack, and it can be seen that there is little difference in the flow capacity robustness for growth rates of 6 and 16. NNC regular network flow is steadily decreasing with an increasing node damage rate, and the greater the average degree, the greater is the flow capacity robustness, which is basically consistent with the situation of the deliberate attack. The results of the WS small-world network show that after fixing reconnection probability,



Flow capacity robustness under deliberate attack



Flow capacity robustness under random attack



Flow capacity robustness difference after different attacks

FIGURE 3 | Changes in flow capacity robustness of the ER random network. **(A)** Change in flow capacity robustness under different damage rates and network density for ER random network under deliberate attack; **(B)** change in flow capacity robustness under different damage rates and network density for the ER random network under random attack; **(C)** change of the difference between the flow capacity robustness under random attack minus the flow capacity robustness under deliberate attack.

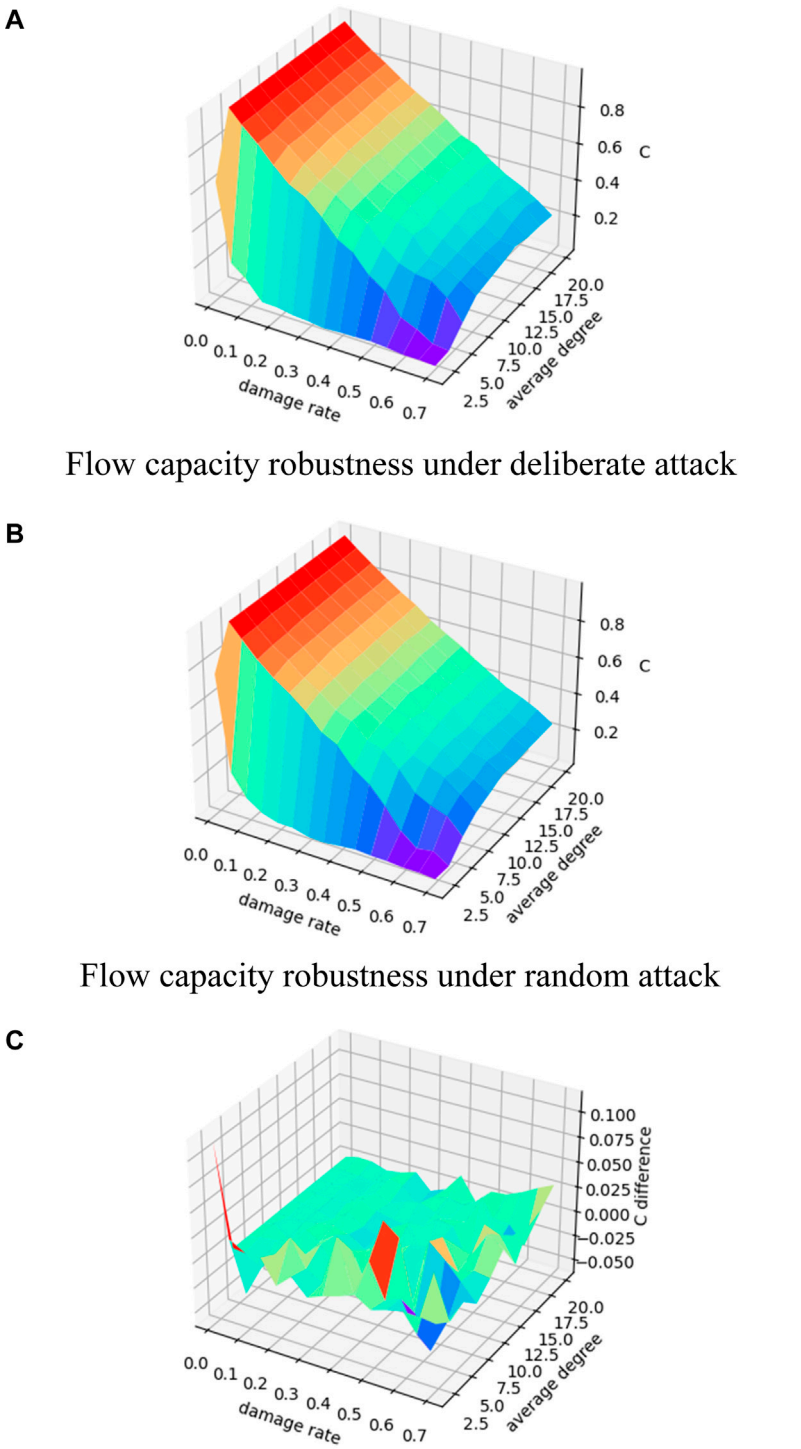


FIGURE 4 | Changes in flow capacity robustness of NNC regular network. **(A)** Change in flow capacity robustness under different damage rates and average degree for the NNC regular network under deliberate attack; **(B)** change in flow capacity robustness under different damage rates and average degree for an NNC regular network under random attack; **(C)** change in the difference between the flow capacity robustness under random attack minus the flow capacity robustness under deliberate attack.

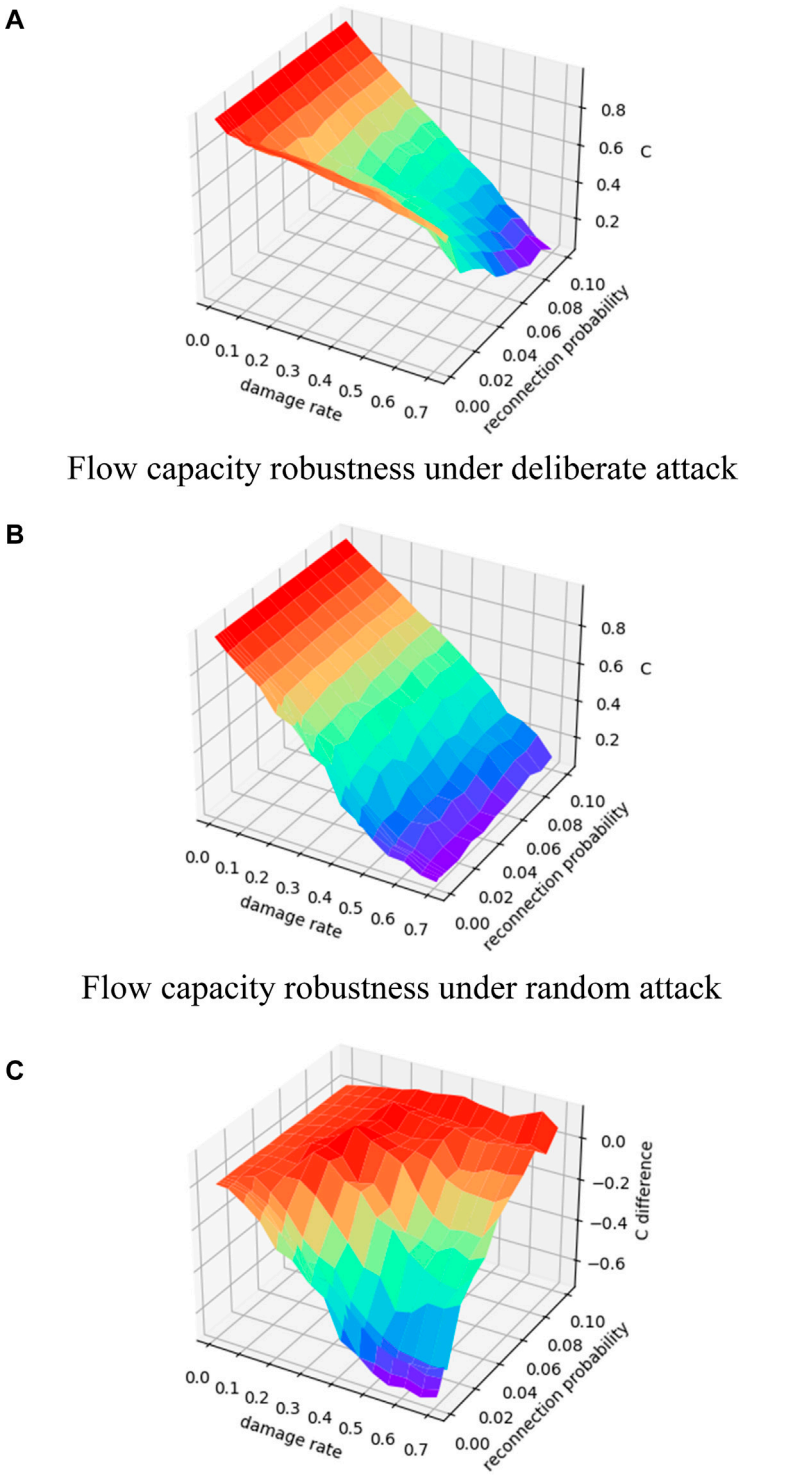


FIGURE 5 | Changes in flow capacity robustness of the WS small-world network with 10 average degrees. **(A)** Change in flow capacity robustness under different damage rates and reconnection probability for the WS small-world network with 10 average degrees under deliberate attack; **(B)** change in flow capacity robustness under different damage rates and reconnection probability for the WS small-world network with 10 average degrees under random attack; **(C)** change in the difference between the flow capacity robustness under random attack minus the flow capacity robustness under deliberate attack.

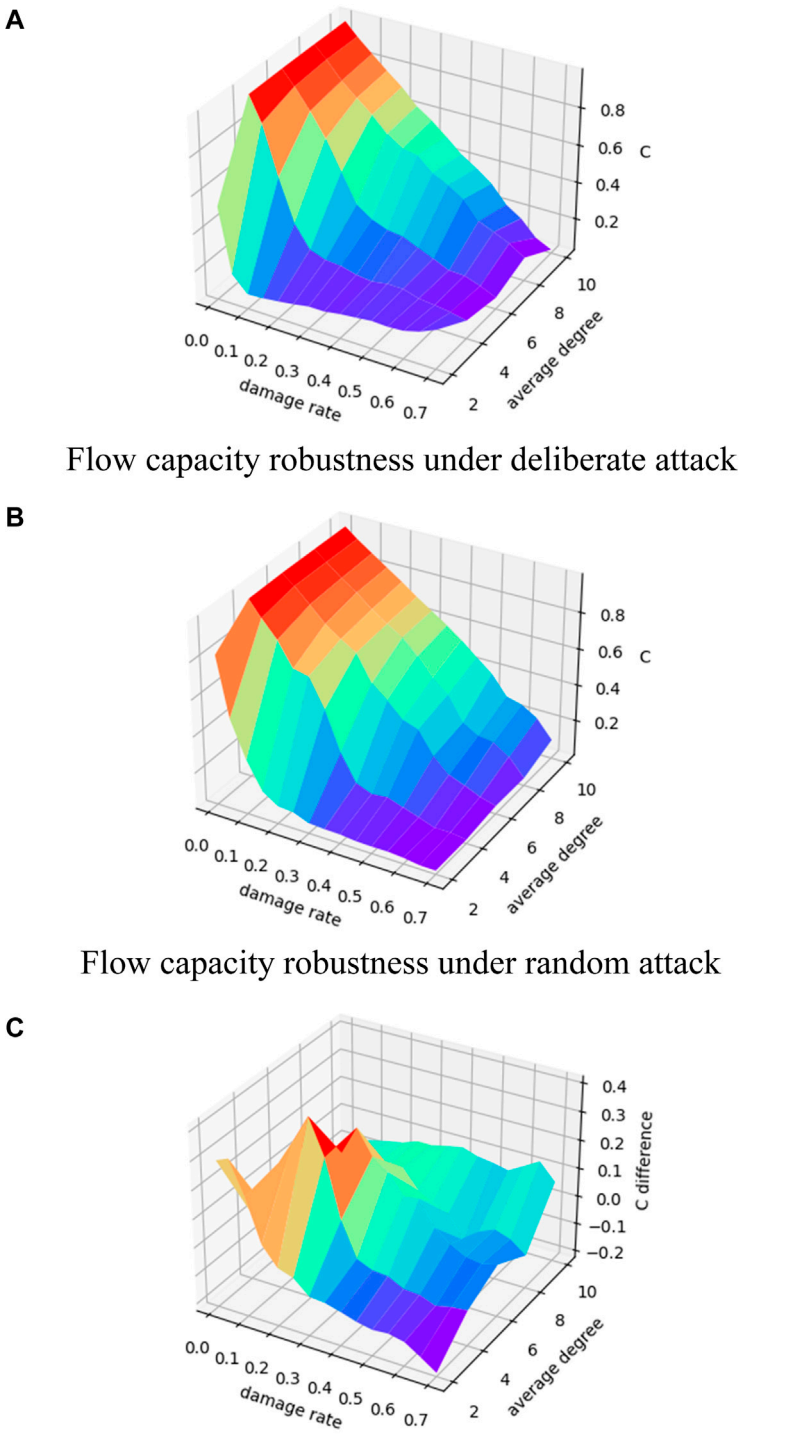


FIGURE 6 | Changes in flow capacity robustness of the WS small-world network with 0.1 reconnection probability. **(A)** Change in flow capacity robustness under different damage rates and average degree for the WS small-world network with 0.1 reconnection probability under deliberate attack; **(B)** change in flow capacity robustness under different damage rates and average degree for the WS small-world network with 0.1 reconnection probability under random attack; **(C)** change in the difference between the flow capacity robustness under random attack minus the flow capacity robustness under deliberate attack.

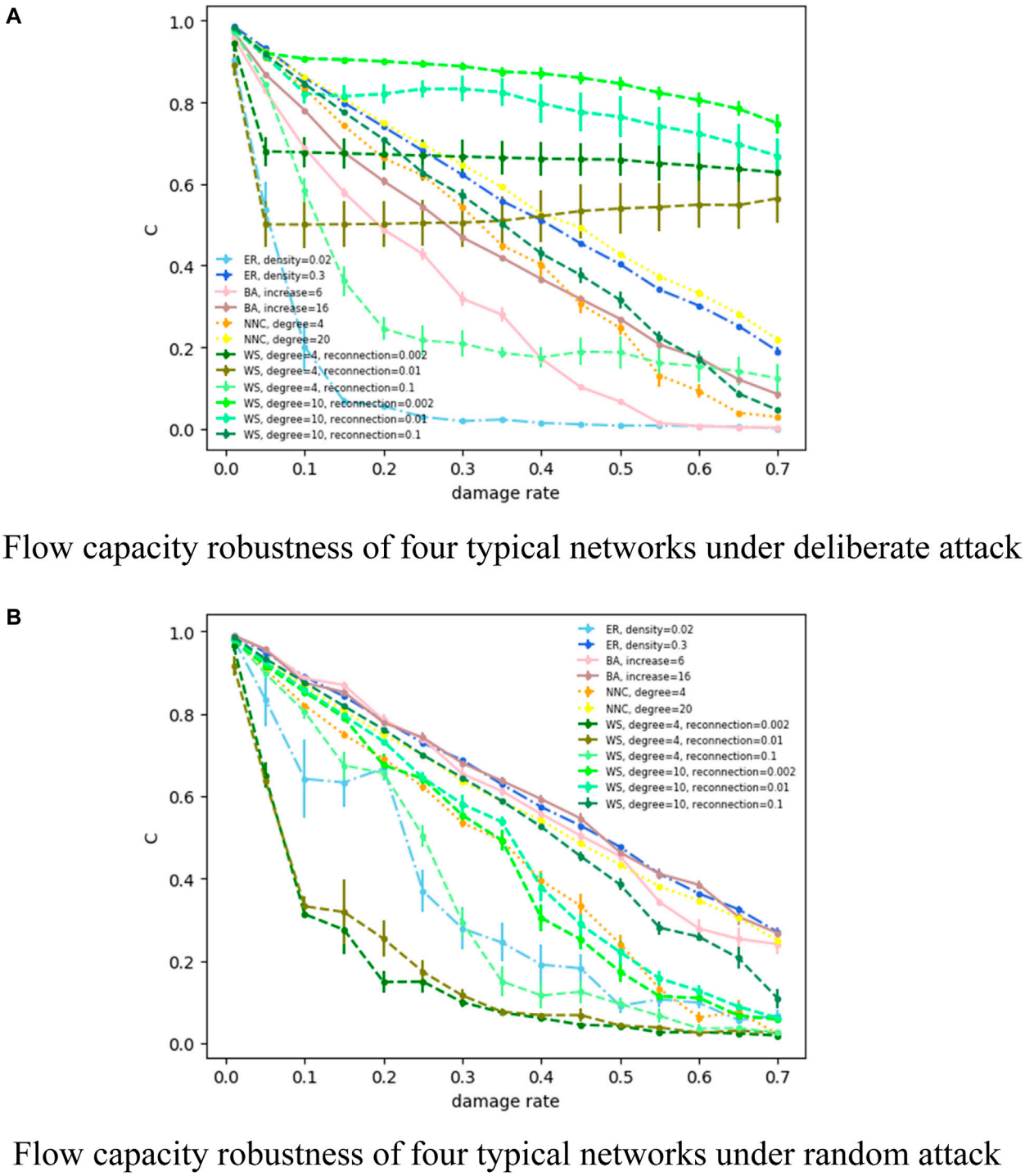


FIGURE 7 | (A) Flow capacity robustness of four typical networks under deliberate attack. **(B)** Flow capacity robustness of four typical networks under random attack.

the larger the average degree, the larger is the flow capacity robustness; after fixing the average degree, the smaller the reconnection probability, the faster the "emergent" phenomenon appears.

Figure 7 shows how the flow capacity robustness indicator of several representative network parameters changes with the increase in the node damage rate under deliberate and random attacks. Furthermore, we conducted experiments on

the same network with classical robustness, and the results are shown in **Figure 8**. Here, we chose the robustness based on the maximum connected subgraph as the classical robustness indicator, which is defined as follows:

$$M = \frac{N_m}{N - N_d}, \tag{10}$$

where N is the size of the initial network; N_d is the number of nodes removed from the network; and N_m is the number of nodes in the maximum connected subgraph in the network when the nodes are removed.

Figure 8A shows how the classical robustness indicator changes under a deliberate attack. It can be seen that similar to flow capacity robustness, the robustness of a small-density ER random network (network density = 0.02) is relatively poor, and as network density increases, the network robustness increases. Compared with a small increase rate (increase rate = 6), a BA scale-free network is more robust at a large increase rate (increase rate = 16). The robustness of the NNC regular network is also stronger at a large average degree. The reconnection probability of a WS small-world network has little effect on network robustness, while the network average degree has a more significant impact on robustness, with the higher the average degree, the stronger is the robustness. For a random attack (**Figure 8B**), the classical robustness indicator shows a similar pattern of variation, that is, high network density is stronger than low network density (ER random network), high increase rate is stronger than low increase rate (BA scale-free network), and high network average degree is stronger than low network average degree (NNC regular network, WS small-world network). Compared to the results of flow capacity robustness (**Figure 7**), due to the different standards of the indicators, the result curves of robustness are not exactly the same, but the trend in relative magnitude of network robustness is basically consistent. This also demonstrates the reasonableness of our method compared with the classical robustness indicator. **Figure 8** shows how the classical robustness indicator of several representative network parameters changes with the increase in the node damage rate under deliberate and random attacks.

Analysis of Experimental Results of the Flow Recovery Robustness

We still use two attack strategies, deliberate and random attacks, and the node recovery strategy is based on the non-global information: nodes v_i and v_j are adjacent nodes, after node v_i is removed, and if node v_j is still in the remaining network V_s, then node v_i and edge $\{v_i, v_j\}$ can be recovered by the information of node v_j. The pseudo-code for the node recovery strategy is given as follows:

Program Network Recovery
Dim is Adjacent As Boolean
For v_j in Vs
For v_i in Vd
If is Adjacent (v_i, v_j) = True
add node v_i to network G
add edge $\{v_i, v_j\}$ to network G
End If
End For
End For
End Network Recovery

Figure 9 shows the flow recovery robustness indicator, and its difference varies with the change in the node damage rate and growth rate for the BA scale-free network of size 100. It can be seen that the recovered network flow shows similar changes with the increase in the node damage rate under both two attack strategies; that is, when fewer nodes are damaged (damage rate less than 20%), the network resilience is strong, and almost all of the damaged nodes can be recovered. In this study, we call this damage rate "critical damage rate" for the flow recovery robustness, and the damaged network can be fully recovered when the node damage rate is less than or equal to this critical damage rate. As the number of damaged nodes increases, the recovery ability of the network becomes weaker, and the "emergent" phenomenon appears. At the same time, it can be seen that when the number of attacked nodes reaches a large value (the damage rate is around 70%), the network flow recovered from a deliberate attack is less than that from a random attack. The flow recovery robustness difference increases with the increase in the node damage rate, indicating that as the level of network damage increases, the gap between the random attack and deliberate attack in the recovery ability of the network after damage becomes more and more significant.

Figure 10 shows the experimental results of the flow recovery robustness of ER random network of size 100 under deliberate and random attacks. The resilience of the network remains strong when the node damage rate is small, and the damaged nodes can be almost fully recovered. As the damage rate increases, the recovered network flow attenuates. In addition, when network density is small (less than 0.1), the number of nodes that cannot be recovered from the initial damage of the ER random network under deliberate attack increases rapidly, that is, the "emergent" phenomenon occurs at the early stage of attack. The flow recovery robustness difference demonstrates the same condition: two attack strategies have a significant difference in the impact of network resilience, that is, a deliberate attack leads to an "emergent" phenomenon in the early stage of damage, but not in a random attack. As the network density increases, the resilience of the ER random network is almost the same for both attacks.

Figure 11 shows results of the flow recovery robustness for the NNC regular network of size 100. When the network average degree is small, unrecovered nodes increase rapidly at the beginning of damage, showing an "emergent" phenomenon. As a larger average degree, the nodes can recover completely at the initial stage of damage and then the flow recovery robustness begins to decrease smoothly. The flow recovery robustness difference shows that the difference is large only when a small average degree and low damage rate are present

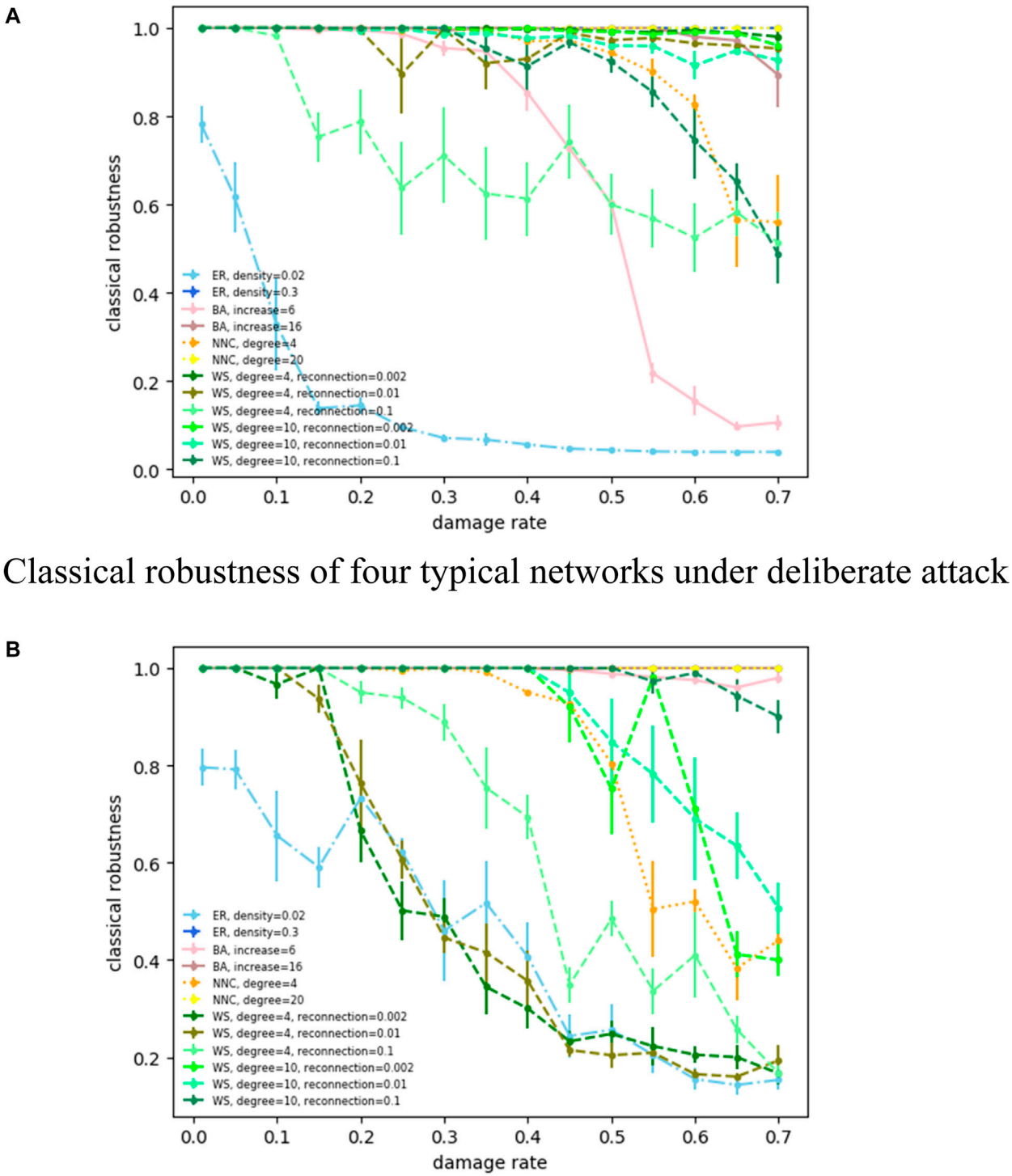


FIGURE 8 | (A) Classical robustness of four typical networks under deliberate attack. **(B)** Classical robustness of four typical networks under random attack.

at the same time. In other cases, the difference converges to 0, that is, the difference in the impact of the two attack strategies on the network is not significant.

The experimental results of the WS small-world network with fixed mean degree are shown in **Figure 12**, and we set a network average degree to 10. As the attack level increases, the network

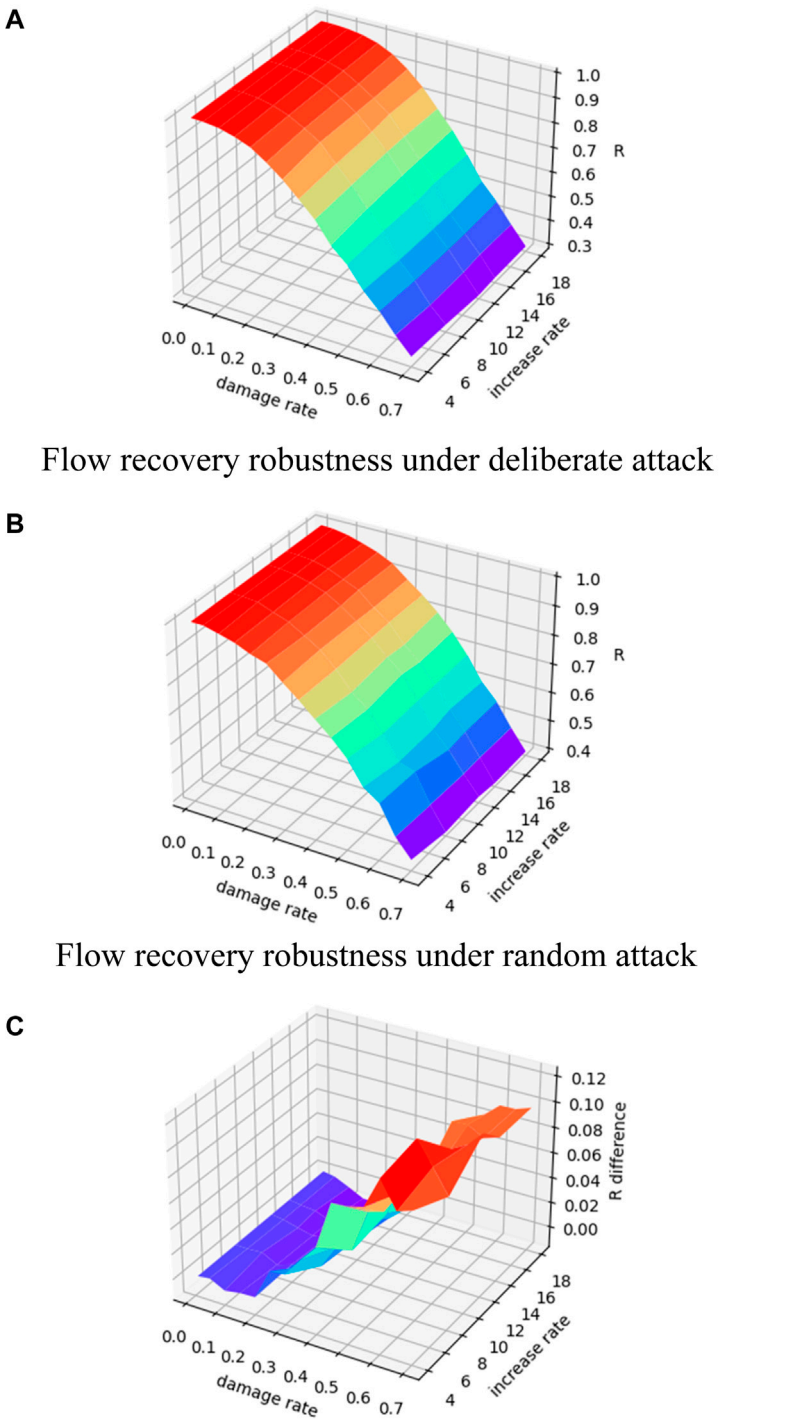


FIGURE 9 | Changes of flow recovery robustness of the BA scale-free network. **(A)** Change in flow recovery robustness under different damage rates and increase rates for BA scale-free network under deliberate attack; **(B)** change in flow recovery robustness under different damage rates and increase rates for BA scale-free network under random attack; **(C)** change in the difference between the flow recovery robustness under random attack minus the flow capacity robustness under deliberate attack.

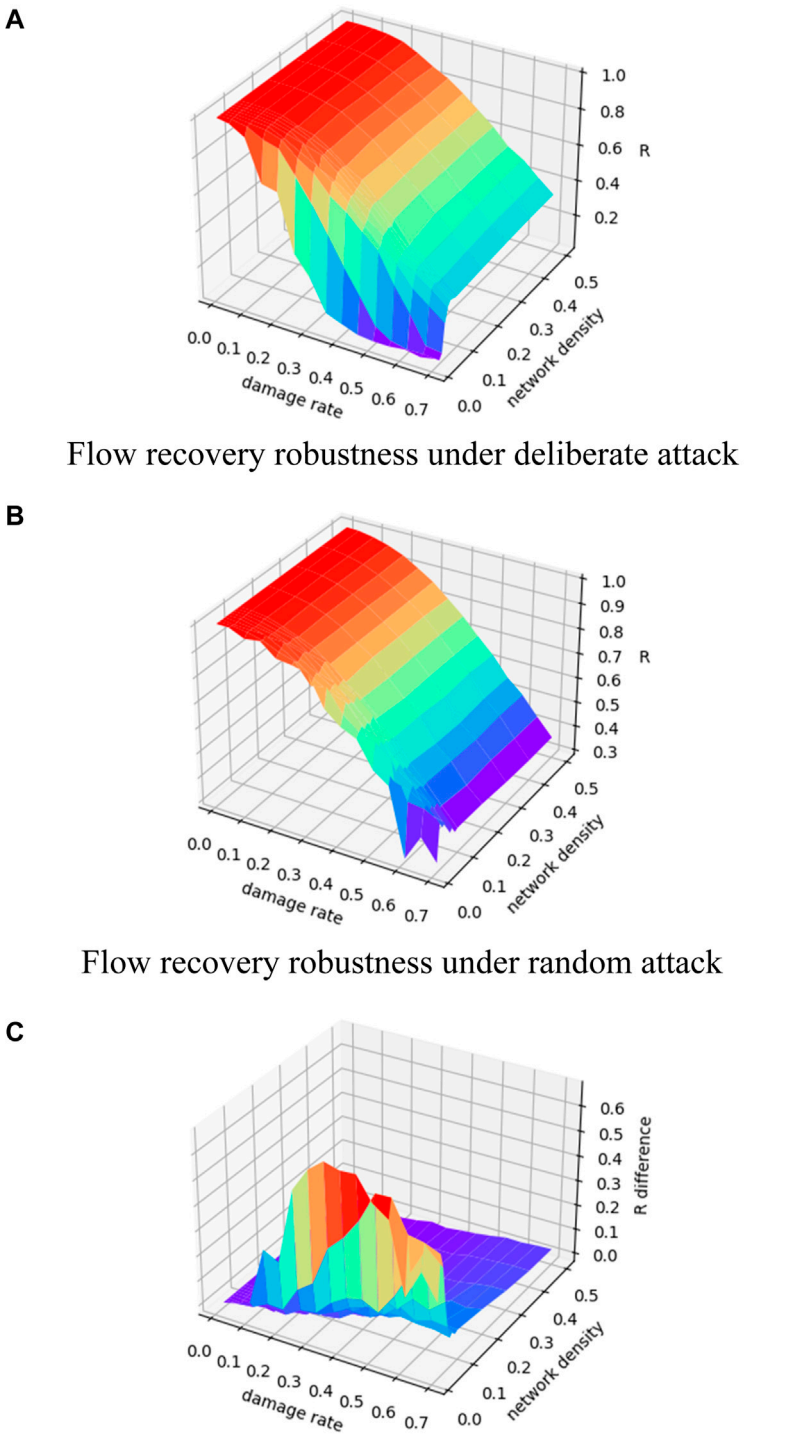


FIGURE 10 | Changes in flow recovery robustness of ER random network. **(A)** Change in flow recovery robustness under different damage rates and network density for ER random network under deliberate attack; **(B)** change in flow recovery robustness under different damage rates and network density for ER random network under random attack; **(C)** change in the difference between the flow recovery robustness under random attack minus the flow capacity robustness under deliberate attack.

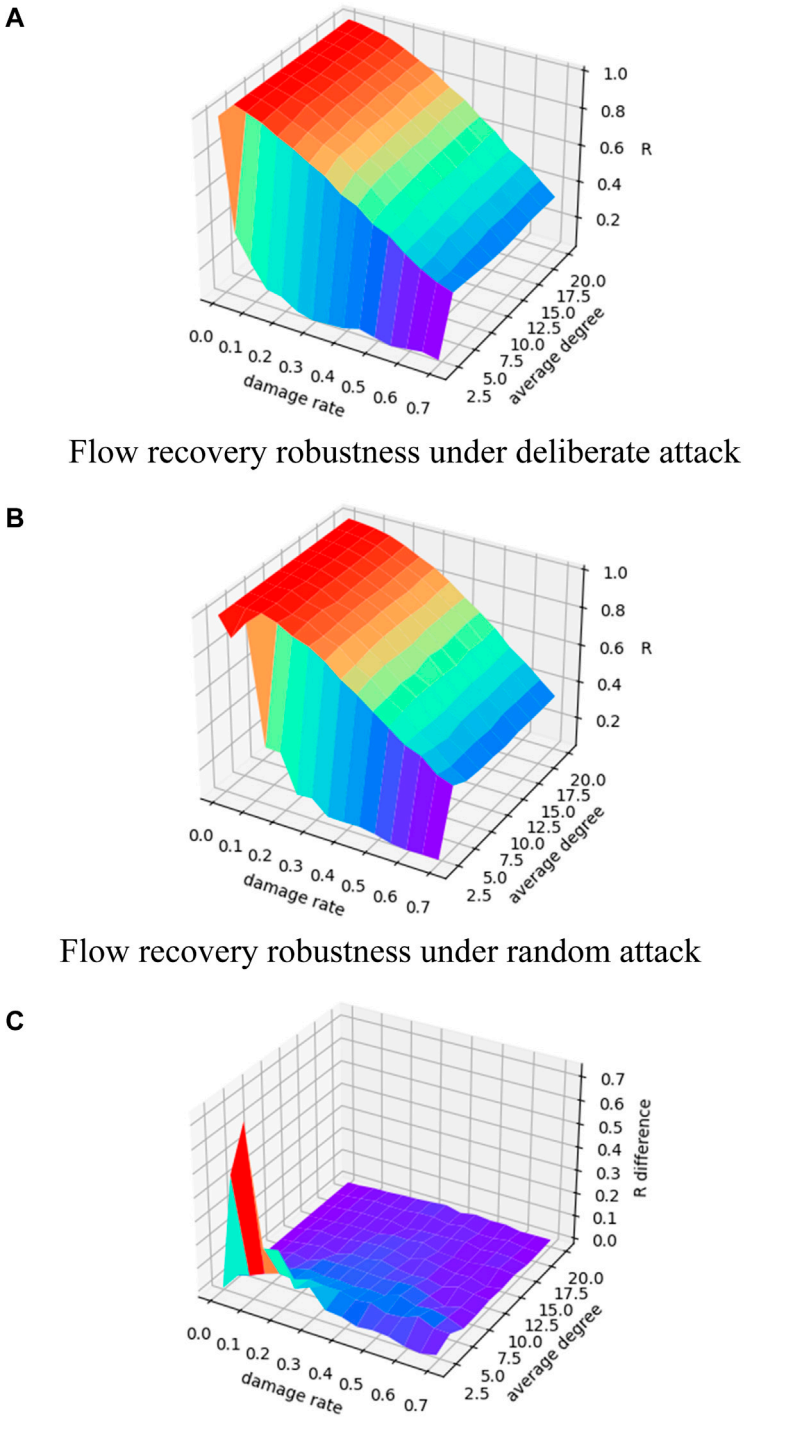


FIGURE 11 | Changes in flow recovery robustness of NNC regular network. **(A)** Change in flow recovery robustness under different damage rates and average degree for NNC regular network under deliberate attack; **(B)** change in flow recovery robustness under different damage rates and average degree for NNC regular network under random attack; **(C)** change in the difference between the flow recovery robustness under random attack minus the flow capacity robustness under deliberate attack.

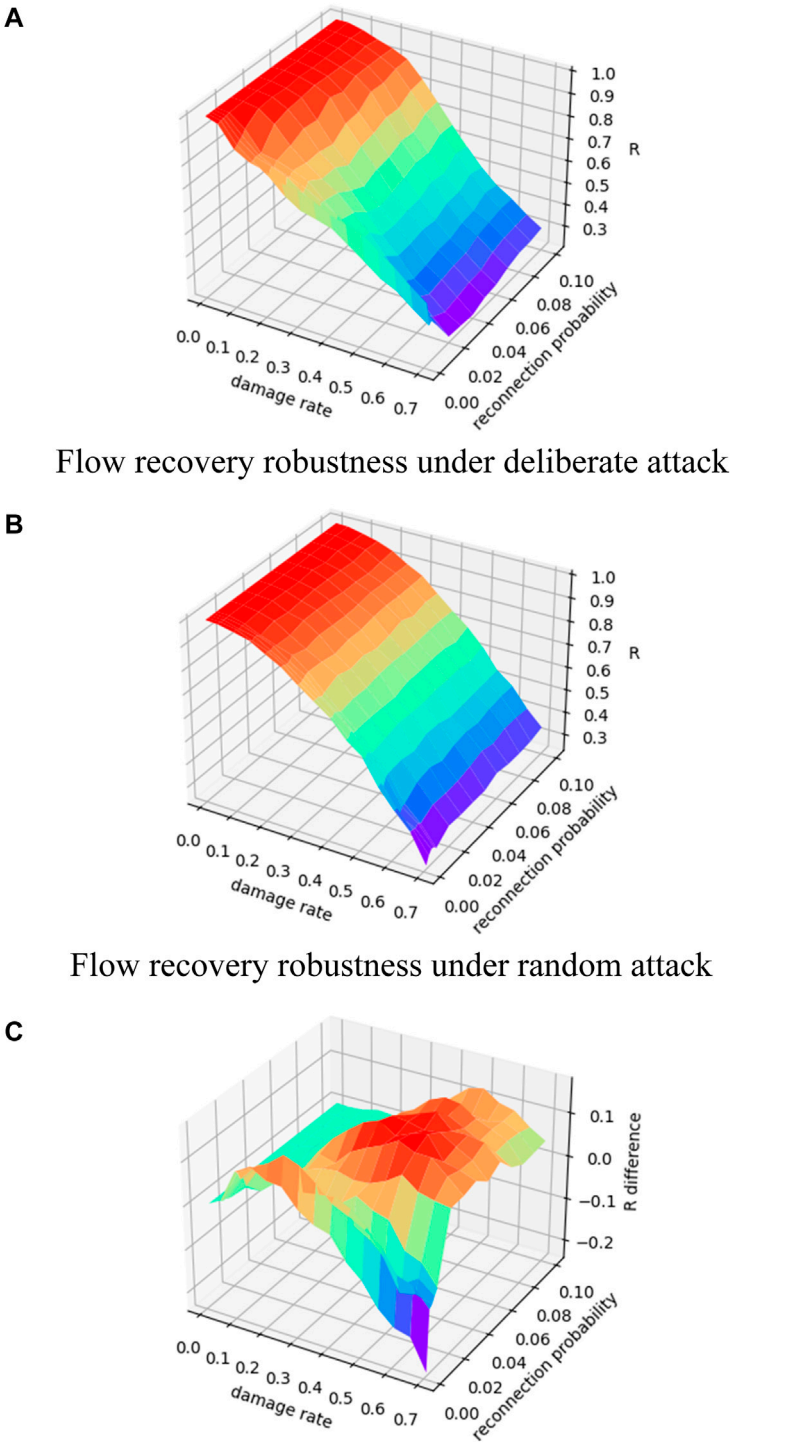


FIGURE 12 | Changes of flow recovery robustness of WS small-world network with 10 average degrees. **(A)** Change in flow recovery robustness under different damage rates and reconnection probability for the WS small-world network with 10 average degrees under deliberate attack; **(B)** change in flow recovery robustness under different damage rates and reconnection probability for the WS small-world network with 10 average degrees under random attack; **(C)** change in the difference between the flow recovery robustness under random attack minus the flow capacity robustness under deliberate attack.

recovery flow goes from almost fully recoverable to significantly reduced. We can also find that reconnection probability has almost no effect on the network resilience, especially under random attack. The flow recovery robustness difference also varies with the change in the node damage rate, and there is no significant pattern to follow in the effect of reconnection probability on this difference.

Figure 13 shows the experimental results of a WS small-world network with a fixed reconnection probability, which is fixed at 0.1. It can be seen that the resilience of a low–average degree network decreases and is more prone to an "emergent" phenomenon, and during a deliberate attack, as the network average degree increases, the flow recovery robustness shows a downtrend. It can be seen from **Figure 13C** that when the network average degree is low, the changes of the flow recovery robustness have their own patterns, and after the average degree increases, the difference change shows a certain pattern, that is, the change is more stable.

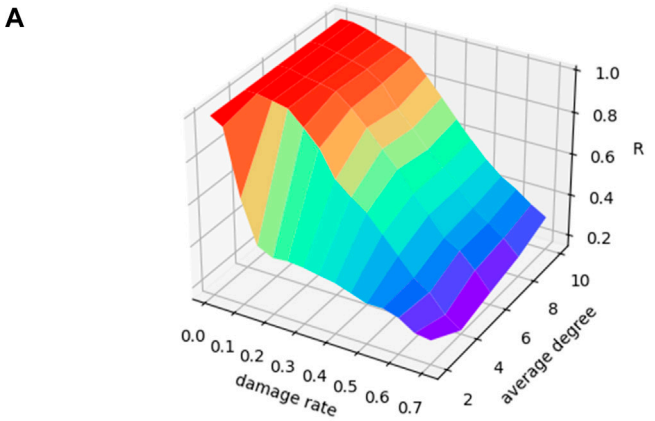
Next, **Figure 14** shows the changes of the flow recovery robustness indicator for the network with different parameters. In case of a deliberate attack (**Figure 14A**), for ER random networks, the low-density network is more unstable than the high-density network in terms of network resilience. Specifically, the flow recovery robustness of the low-density network shows a rapid decline in the early stage, while the recovery ability of the high-density network is almost 100% until the damage rate reaches the critical value (20%), and the flow recovery robustness decreases smoothly after exceeding the critical damage rate. The BA scale-free network, on the other hand, presents an almost coincident resilience with an ER random network of higher density (network density = 0.3), and it can be seen that the growth rate does not have much influence on the flow recovery robustness of the BA scale-free network. The recovery capability of the NNC regular network also shows a steady decrease with the increase in damage rate, and there is no critical damage rate in the NNC regular network, that is, the flow recovery robustness decreases when the network is initially damaged on a small scale (damage rate <20%), especially in the NNC regular network with a small average degree. For the WS small-world network, when the network average degree is fixed, the higher the reconnection probability, the better is the network's resilience, and there is a corresponding critical damage rate. Conversely, the smaller the reconnection probability, the worse is the recovery capability and there is no corresponding critical damage rate. When the reconnection probability is fixed, the larger is the network average degree, the higher is the flow recovery robustness.

During a random attack (**Figure 14B**), the ER random network does not appear as an "emergent" phenomenon similar to the rapid decrease in network recovery ability during a deliberate attack and has a corresponding critical damage rate, regardless of network density. The BA scale-free network shows a steady decline after critical damage rate is reached, and the growth rate does not have a significant impact on recovery ability. Similarly, the NNC regular network shows a trend of strong recovery ability in the early stage and a steady decline in the later stage, and the greater the average network degree, the greater is the flow recovery robustness. For the WS small-world network, the overall trend of the flow recovery robustness is more stable than for deliberate attack, but still, after fixing the network average degree, the flow recovery robustness increases as reconnection probability increases, and the change in resilience is more stable for the network with higher reconnection probability; after fixing reconnection probability, the network average degree increases, and the network's resilience is enhanced, and the change of the flow recovery robustness is smoother for the network with a larger average degree. It can be seen that a small rebound in the flow recovery robustness during random attack occurs. It is normal for a small rebound to occur because the latter of two adjacent attacks does not based on the previous one but randomly damages a certain percentage of nodes again.

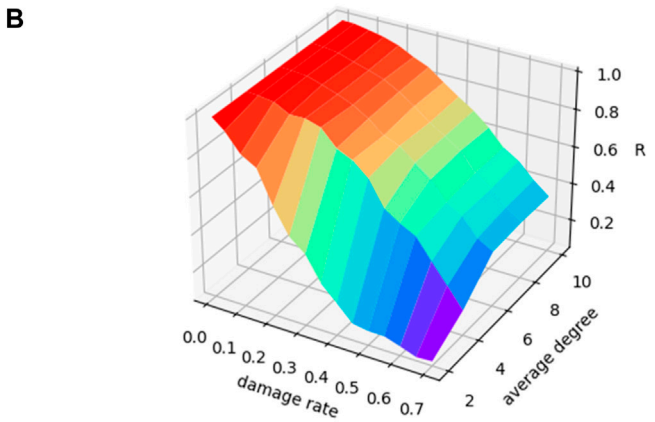
Figure 14 shows how the flow recovery robustness indicator of several representative network parameters changes with the increase in the node damage rate under deliberate and random attacks. Finally, in order to verify the effectiveness of the recovery strategy in this study, we make the difference between the flow recovery robustness and the flow capacity robustness, which is intended to consider the difference between the network flows after network recovery and before recovery. As can be seen from **Figure 15**, the flow recovery robustness after recovery is greater than the flow capacity robustness before recovery in varying levels for all four typical networks, whether under a deliberate or random attack, which reflects the effectiveness of the recovery strategy based on non-global information.

DISCUSSION

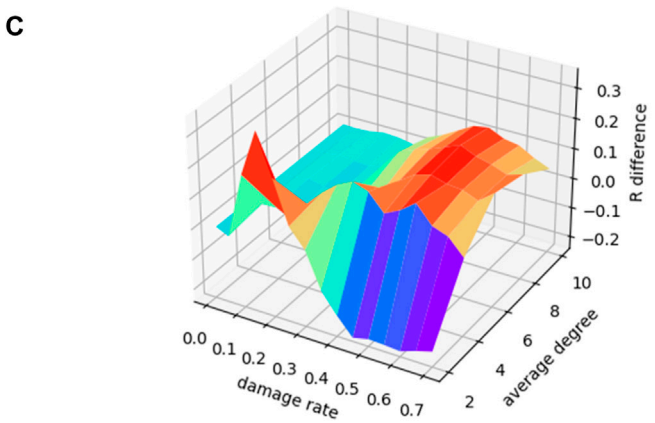
In this study, we define two types of robustness evaluation indicators based on network maximum flow: the flow capacity robustness, which assesses the ability of the network to resist attack, and the flow recovery robustness, which assesses the ability to rebuild the network after an attack on the network. In order to verify the effectiveness of the proposed robustness evaluation indicators, this study conducts experimental analysis on four typical networks, and the experimental results show that after ER random network is attacked, the high-density network outperforms the low-density network in terms of connectivity and resilience; network growth rate of the BA scale-free network does not have a significant effect on robustness changes in most cases; robustness of the NNC regular network decreases steadily as the node damage rate increases, and the greater the average degree, the greater is the robustness; for the WS small-world network, when we fix the network average degree, the larger the reconnection probability, the better is the connectivity and recovery ability of the network after attack, and when we fix reconnection probability, the bigger the network average degree, the greater is the robustness. When examining the flow recovery robustness, we find that there is a critical damage rate (nodes and edges that are damaged can be almost completely recovered when the node damage rate is less than this critical value), and the critical damage rate is located around 20%. In addition, the



Flow recovery robustness under deliberate attack



Flow recovery robustness under random attack



Flow recovery robustness difference after different attacks

FIGURE 13 | Changes in flow recovery robustness of a WS small-world network with 0.1 reconnection probability. **(A)** Change in flow recovery robustness under different damage rates and average degree for the WS small-world network with 0.1 reconnection probability under deliberate attack; **(B)** change in flow recovery robustness under different damage rates and average degree for the WS small-world network with 0.1 reconnection probability under random attack; **(C)** change in the difference between the flow recovery robustness under random attack minus the flow capacity robustness under deliberate attack.

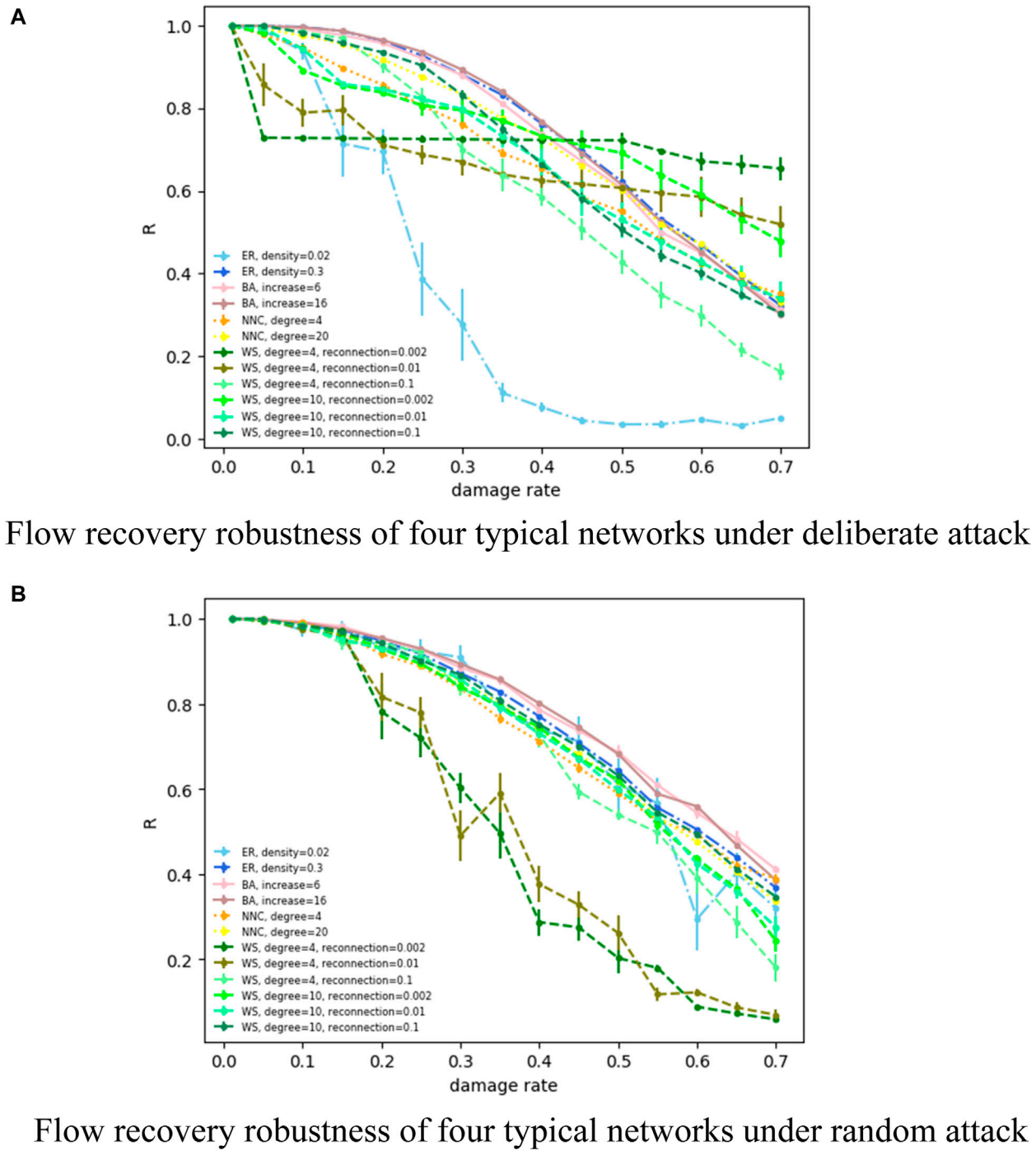


FIGURE 14 | (A) Flow recovery robustness of four typical networks under deliberate attack. **(B)** Flow recovery robustness of four typical networks under random attack.

decline in robustness based on network maximum flow not only appears an "emergent" phenomenon as the number of attacked nodes increases but also presents a certain "emergent" phenomenon with the change in network structure parameters. Finally, this study also verifies the effectiveness of our adopted non-global information-based recovery strategy for attacked network through difference values between the flow recovery robustness and the flow capacity robustness. The flow capacity robustness and the flow recovery robustness based on network maximum flow proposed in this study enrich the

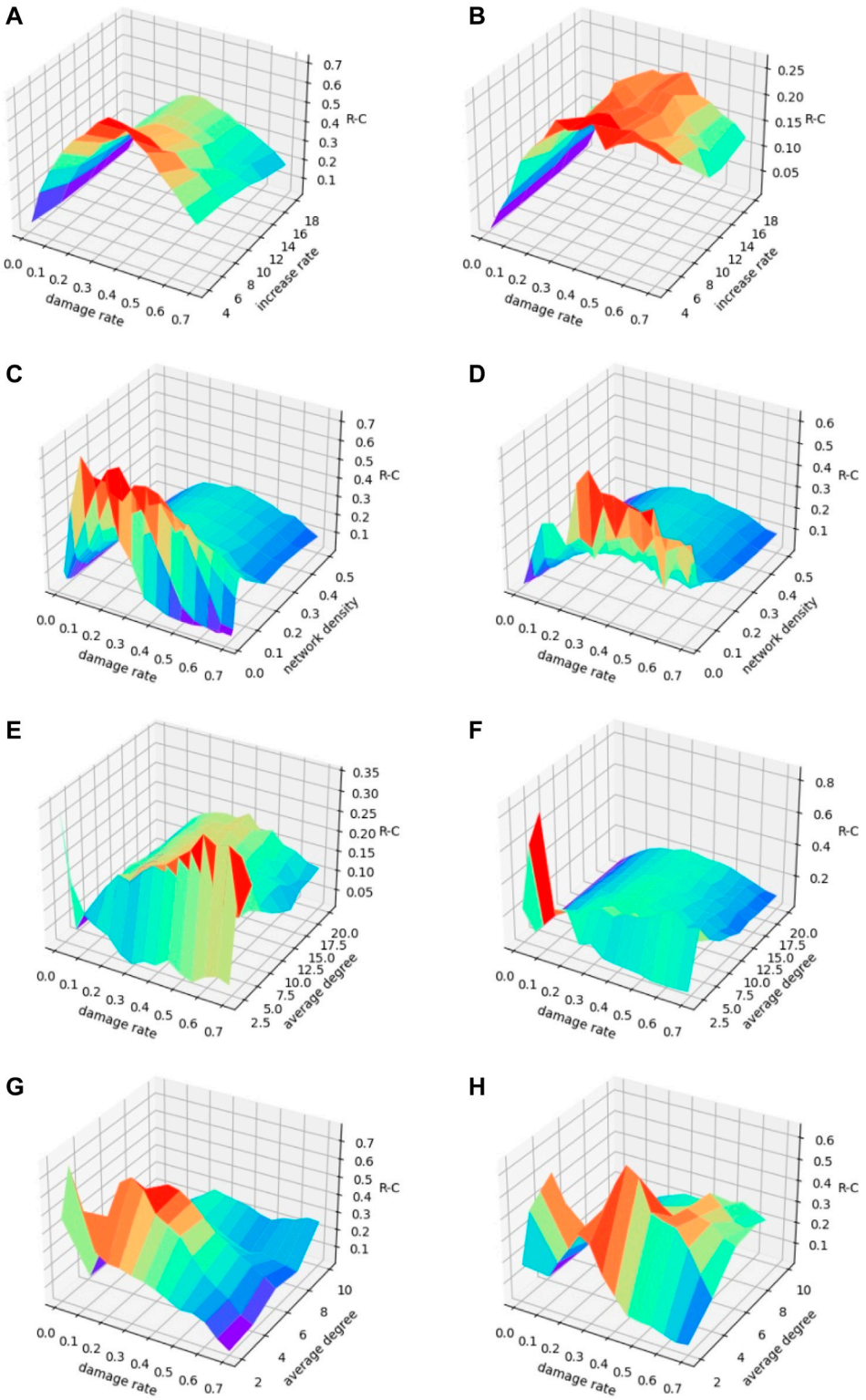


FIGURE 15 | Difference between the flow recovery robustness and the flow capacity robustness of four typical networks. **(A, B)**, respectively, show the difference between the flow recovery robustness and the flow capacity robustness in BA scale-free network under deliberate attack and random attack; **(C, D)**, respectively, show the difference between the flow recovery robustness and the flow capacity robustness in ER random network under deliberate attack and random attack; **(E, F)**, respectively, show the difference between the flow recovery robustness and the flow capacity robustness in the NNC regular network under deliberate attack and random attack; **(G, H)**, respectively, show the difference between the flow recovery robustness and the flow capacity robustness in the WS small-world network under deliberate attack and random attack.

network structure indicator system and more comprehensively describe structural stability of real networks such as interpersonal networks and Internet. The main work in this study focuses on the design of two types of the robustness evaluation indicators based on network maximum flow and the experimental characterization of typical networks, and more in-depth theoretical analysis and quantitative description are the main elements of the subsequent study. Furthermore, we will try to extend our method from static networks to dynamic networks. Methods that have been used to deal with dynamic networks include exponential random graph models [42], stochastic block models [43, 44], continuous latent space models [44, 45], latent feature models [46, 47], and majority dynamics [48]. We will extend our indicators to dynamic networks by referring to existing methods.

DATA AVAILABILITY STATEMENT

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

AUTHOR CONTRIBUTIONS

MC conceived and put forward the research ideas and carried out the research. JL and YC were in charge of the calculation and experimental data. MC, JL, and YC collected information and wrote the manuscript. All authors have read and agreed to the published version of the manuscript.

FUNDING

This research was funded by the National Natural Science Foundation of China under Grant No. 71501153, the Innovation Capability Support Project of Shaanxi Province of China under Grant No. 2021KRM135, the Research Fund of Grand Theory and Practical Problem in Philosophy and Social Science of Shaanxi Province of China under Grant No. 2021ND0221, and the Research Fund of the Education Department of Shaanxi Province of China under Grant No. 20JG020.

REFERENCES

1. Liu X-M. *Research on the Robustness and Controllability of Complex Networks*. Wuhan, China: Huazhong University of Science & Technology (2016).
2. Jie J. Study of Robustness in the World. *J Syst Eng* (2005) 2:153–9. doi:10.3969/j.issn.1000-5781.2005.02.009
3. Albert R, Jeong H, Barabási A-L. Error and Attack Tolerance of Complex Networks. *Nature* (2000) 406(6794):378–82. doi:10.1016/j.physa.2004.04.03110.1038/35019019
4. Holme P, Kim BJ, Yoon CN, Han SK. Attack Vulnerability of Complex Networks. *Phys Rev E* (2002) 65(5):056109. doi:10.1103/PhysRevE.65.056109
5. Paul G, Tanizawa T, Havlin S, Stanley HE. Optimization of Robustness of Complex Networks. *Eur Phys J B* (2004) 38:187–91. doi:10.1140/epjb/e2004-00112-3
6. He C-Q. *Research on Robustness during Network Evolution*. Shanghai, China: Shanghai Jiaotong University (2009).
7. Du W, Cai M, Du H-F. Study on Indices of Network Structure Robustness and Their Application. *J Xi'an Jiaotong Univ* (2010) 44(4):93–7.
8. Lu P-L, Dong M, Cao L. Analysis of Influence of Clustering Coefficient as its index on Robustness of Complex Network. *J Lanzhou Univ Technol* (2019) 45(3):101–7.
9. Zhang J-Y. *Robust Analysis of Urban Road Network under Different Attack Conditions*. Dalian, China: Dalian Jiaotong University (2020).
10. Dorogovtsev SN, Goltsev AV, Mendes JFF. K-Core Organization of Complex Networks. *Phys Rev Lett* (2006) 96:040601. doi:10.1103/PhysRevLett.96.040601
11. Morone F, Del Ferraro G, Makse HA. The K-Core as a Predictor of Structural Collapse in Mutualistic Ecosystems. *Nat Phys* (2019) 15:95–102. doi:10.1038/s41567-018-0304-8
12. Liu Y-Y, Csóka E, Zhou H, Pósfai M. Core Percolation on Complex Networks. *Phys Rev Lett* (2012) 109:205703. doi:10.1103/PhysRevLett.109.205703
13. Shang Y. Attack Robustness and Stability of Generalized K-Cores. *New J Phys* (2019) 21:093013. doi:10.1088/1367-2630/ab3d7c
14. Shang Y-L. Generalized K -cores of Networks under Attack with Limited Knowledge. *Chaos Solitons Fractals* (2021) 152:111305. doi:10.1016/j.chaos.2021.111305
15. Dorogovtsev SN, Mendes JFF, Samukhin AN. Giant Strongly Connected Component of Directed Networks. *Phys Rev E* (2001) 64(2 Pt 2):025101. doi:10.1103/PhysRevE.64.025101
16. Panduranga NK, Gao J, Yuan X, Stanley HE, Havlin S. Generalized Model for K -Core Percolation and Interdependent Networks. *Phys Rev E* (2017) 96(3-1):032317. doi:10.1103/PhysRevE.96.032317
17. Linton CF, Stephen PB, Douglas RW. Centrality in Valued Graphs: a Measure of Betweenness Based on Network Flow. *Soc Networks* (1992) 13(2):141–54. doi:10.1016/0378-8733(91)90017-N
18. Shang Y. Vulnerability of Networks: Fractional Percolation on Random Graphs. *Phys Rev E Stat Nonlin Soft Matter Phys* (2014) 89(1):012813. doi:10.1103/physreve.89.01281342
19. Cohen R, Erez K, Ben-Avraham D, Havlin S. Resilience of the Internet to Random Breakdowns. *Phys Rev Lett* (2000) 85(21):4626–8. doi:10.1103/PhysRevLett.85.4626
20. Cohen R, Erez K, Ben-Avraham D, Havlin S. Breakdown of the Internet under Intentional Attack. *Phys Rev Lett* (2001) 86:3682–5. doi:10.1103/PhysRevLett.86.3682
21. Scott DM, Novak DC, Aultman-Hall L, Guo F. Network Robustness index: a New Method for Identifying Critical Links and Evaluating the Performance of Transportation Networks. *J Transport Geogr* (2006) 14(3):215–27. doi:10.1016/j.jtrangeo.2005.10.003
22. Tan Y-J, Wu J, Deng H-Z, Zhu D-Z. Invulnerability of Complex Networks: a Survey. *Syst Eng* (2006) 10:1–5.
23. Lu S. *Robust Analysis of Aviation Logistics System Based on Complex Network Theory*. Changchun, China: Jilin University (2014).
24. Dong G, Chen Y, Wang F, Du R, Tian L, Stanley HE. Robustness on Interdependent Networks with a Multiple-To-Multiple Dependent Relationship. *Chaos* (2019) 29(7):073107. doi:10.1063/1.5093074
25. Shi H. Invulnerability Estimation Model of Buildings with Complex Networks under strong Earthquakes. *China Earthquake Eng J* (2017) 39(6):1024–8.
26. Dong G, Wang F, Shekhtman LM, Danziger MM, Fan J, Du R, et al. Optimal Resilience of Modular Interacting Networks. *Proc Natl Acad Sci USA* (2021) 118(22):e1922831118. doi:10.1073/pnas.1922831118
27. Mariani MS, Ren Z-M, Bascompte J, Tessone CJ. Nestedness in Complex Networks: Observation, Emergence, and Implications. *Phys Rep* (2019) 813:1–90. doi:10.1016/j.physrep.2019.04.001
28. Wuellner DR, Roy S, D'Souza RM. Resilience and Rewiring of the Passenger Airline Networks in the United States. *Phys Rev E* (2010) 82(5):056101. doi:10.1103/PhysRevE.82.056101
29. Liu Y, Sanhedrai H, Dong G, Shekhtman LM, Wang F, Buldyrev SV, et al. Efficient Network Immunization under Limited Knowledge. *Natl Sci Rev* (2021) 8(1):nwaa229. doi:10.1093/nsr/nwaa229
30. McDaniels T, Chang S, Cole D, Mikawoz J, Longstaff H. Fostering Resilience to Extreme Events within Infrastructure Systems: Characterizing Decision Contexts for Mitigation and Adaptation. *Glob Environ Change* (2008) 18(2):310–8. doi:10.1016/j.gloenvcha.2008.03.001

31. van der Vegt GS, Essens P, Wahlström M, George G. Managing Risk and Resilience. *Amj* (2015) 58(4):971–80. doi:10.5465/amj.2015.4004
32. Bai Y-N, Huang N, Sun L-N, Zhang Y (2017). "Failure Propagation of Dependency Networks with Recovery Mechanism," In: 2017 Annual Reliability and Maintainability Symposium (RAMS), Orlando, FL, January 23–26, 2017 (IEEE), 1–6. doi:10.1109/RAM.2017.7889721
33. Liu R-R, Li M, Jia C-X. Cascading Failures in Coupled Networks: the Critical Role of Node-Coupling Strength across Networks. *Sci Rep* (2016) 6:35352. doi:10.1038/srep35352
34. Hong S, Lv C, Zhao T, Wang B, Wang J, Zhu J. Cascading Failure Analysis and Restoration Strategy in an Interdependent Network. *J Phys A: Math Theor* (2016) 49(19):195101–12. doi:10.1088/1751-8113/49/19/195101
35. Wang L-X. *Study on Key Fault Node Location and Recovery Technology in Complex Networks*. Xi'an, China: Xidian University (2019).
36. Li Zhao Z, Guo Yan-Hui Y-H, Xu Guo-Ai G-A, Hu Zheng-Ming Z-M. Analysis of Cascading Dynamics in Complex Networks with an Emergency Recovery Mechanism. *wlxb* (2014) 63(15):158901–428. doi:10.7498/aps.63.158901
37. Bohannon J. Counterterrorism's New Tool: 'Metanetwork' Analysis. *Science* (2009) 325(5939):409–11. doi:10.1126/science.325-40910.1126/science.325_409
38. Wang X-F, Li X, Chen G-R. *Complex Network Theory and Application*. Beijing: Tsinghua University Press (2006). p. 18.
39. Baraba´si A-L, Albert R. Emergence of Scaling in Random Networks. *Science* (1999) 286(5439):509–12. doi:10.1126/science.286.5439.509
40. Erdös P, Rényi A. (2011). *On The Evolution of Random Graphs. The Structure and Dynamics of Networks*. New Jersey, US: Princeton University Press, 38–82. doi:10.1515/9781400841356.38
41. Watts DJ, Strogatz SH. Collective Dynamics of 'small-World' Networks. *Nature* (1998) 393(6684):440–2. doi:10.1038/30918
42. Guo F, Hanneke S, Fu W-J, Xing EP(2007). "Recovering Temporally Rewiring Networks: A Model-Based Approach," In: Proceedings of the 24th International Conference on Machine Learning, Corvallis, USA, January 1, 2007, 321–8.
43. Xing EP, Fu W, Song L. A State-Space Mixed Membership Blockmodel for Dynamic Network Tomography. *Ann Appl Stat* (2010) 4(2):536–66. doi:10.1214/09-AOAS311
44. Hoff PD. Hierarchical Multilinear Models for Multiway Data. *Comput Stat Data Anal* (2011) 55(1):530–43. doi:10.1016/j.csda.2010.05.020
45. Sarkar P, Moore AW. Dynamic Social Network Analysis Using Latent Space Models. *SIGKDD Explor Newsl* (2005) 7(2):31–40. doi:10.1145/1117454.1117459
46. Heaukulani C, Ghahramani Z (2013). "Dynamic Probabilistic Models for Latent Feature Propagation in Social Networks," In: Proceedings of the 30th International Conference on Machine Learning, Atlanta, US, June 16, 2013, 28, 275–83.
47. Kim M, Leskovec J. Nonparametric Multi-Group Membership Model for Dynamic Networks. *Adv Neural Inf Process Syst* (2013) 25:1385–93.
48. Shang Y. A Note on the Majority Dynamics in Inhomogeneous Random Graphs. *Results Math* (2021) 76(3):1–17. doi:10.1007/s00025-021-01436-z

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

frontiers in Physics

ORIGINAL RESEARCH
published: 21 December 2021
doi: 10.3389/fphy.2021.805584

Computing Effective Mixed Strategies for Protecting Targets in Large-Scale Critical Infrastructure Networks

*Zhen Wang, Mengting Jiang, Yu Yang, Lili Chen and Hong Ding**

School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China

Most critical infrastructure networks often suffer malicious attacks, which may result in network failures. Therefore, how to design more robust defense measures to minimize the loss is a great challenge. In recent years, defense strategies for enhancing the robustness of the networks are developed based on the game theory. However, the aforementioned method cannot effectively solve the defending problem on large-scale networks with a full strategy space. In this study, we achieve the purpose of protecting the infrastructure networks by allocating limited resources to monitor the targets. Based on the existing two-person zero-sum game model and the Double Oracle framework, we propose the EMSL algorithm which is an approximation algorithm based on a greedy search to compute effective mixed strategies for protecting large-scale networks. The improvement of our approximation algorithm to other algorithms is discussed. Experimental results show that our approximation algorithm can efficiently compute the mixed strategies on actual large-scale networks with a full strategy space, and the mixed defense strategies bring the highest utility to a defender on different networks when dealing with different attacks.

Keywords: network robustness, complex network, game theory, mixed strategies, defense

OPEN ACCESS

Edited by:
Gaogao Dong,
Jiangsu University, China

Reviewed by:
Jiuchuan Jiang,
Nanjing University of Finance and Economics, China
Zhihai 'Rong,
University of Electronic Science and Technology of China, China

****Correspondence:***
Hong Ding
dinghong@hdu.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *30 October 2021*
Accepted: *24 November 2021*
Published: *21 December 2021*

Citation:
Wang Z, Jiang M, Yang Y, Chen L and Ding H (2021) Computing Effective Mixed Strategies for Protecting Targets in Large-Scale Critical Infrastructure Networks. Front. Phys. 9:805584. doi: 10.3389/fphy.2021.805584

1 INTRODUCTION

In recent years, malicious activities against the critical infrastructures lead to new challenges to the world's security, which have inflicted enormous economic losses and threatened public safety. For instance, in July 2019, a cyber attack on a Venezuelan hydroelectric power plant collapsed the water grid in the capital and more than 10 states, plunging the entire country into darkness [1]. Very recently, the largest oil pipeline company in the United States, Colonial Pipeline, was attacked by the hacker organization DarkSide, which led the country to announce an emergency state [2]. Thus, analyzing the robustness of the critical infrastructure networks against the malicious attacks and accordingly improving the efficiency of defending the targets with limited resources remain major problems.

Prior works have designed methods to protect the critical infrastructure networks against malicious attacks, and we summarize them into three classes. The first class comes up with adding nodes (e.g., adding additional base stations), adding edges (e.g., adding additional power lines), or swapping edges (e.g., rewiring power lines) to enhance the network robustness [3–5]. But these methods will change the network structure, while the structure of a network is a defining characteristic that can identify its functionality and thus should remain unchanged. The second class proposes resource-allocation methods to significantly reduce the time cost of allocating resources and increase the probability of successful defending tasks, considering the cooperativity between resources and tasks [6, 7], which will increase the complexity of the defending problem. The third

class develops algorithms to monitor (e.g., closely monitor substation) or immunize important nodes for protecting networks, according to a range of network centrality measures (e.g., degree centrality and betweenness centrality) [8–13]. However, all these existing centrality metrics do not consider the protector's combinatorial pure policy space. Though these defending policies can protect the network against attacks to a certain extent, we can consider mixing the pure strategies and scheduling the defense resources dynamically to design more protective defending strategies.

To address the problem of designing more robust measures for defending the critical infrastructure networks, we can model the urban infrastructure cybersecurity problem as a problem with both defender and attacker participants. The infrastructure-based confrontation between the attacker and the defender can be modeled using game theory. However, most of the research studies that compute the attack and defense strategies by establishing different game models only consider a few typical strategies to shrink the space of strategies, rather taking a large strategy set into account [14–19]. Only one article is distinct; Li et al. proposed the two-player zero-sum simultaneous-move game model to solve the defending problem [20]. Their algorithm enumerates all strategies for obtaining the Nash equilibrium (ESE) on the network with 20 nodes and computes mixed strategies for both players. Unfortunately, their algorithm cannot solve the problem of computing the global equilibrium in large-scale networks. So, the challenge is how to compute effective strategies with the full strategy space of both players growing exponentially with the increase of the network size.

To solve the pervious challenge, based on the existing two-person zero-sum model and settings, we propose our solution containing four key contributions:

1) First, we extend the defending problem to a real large-scale infrastructure network that is vulnerable.
2) Second, we propose the effective mixed strategies for large-scale networks (EMSL) algorithm, which is based on greed under the Double Oracle framework to obtain an effective defense solution.
3) Third, we design mixed-integer linear programming (MILP) to compute the best pure attack strategy for an attacker.
4) Finally, we conduct extensive experiments on two networks of different sizes by comparing with other defense strategies under different attacks. The experimental results show that the mixed defense strategies obtained by our approximation algorithm bring the highest utility to a defender on different networks when dealing with different attacks.

2 INFRASTRUCTURE NETWORK PROTECTING GAME

As in the pioneering work [14], we define the problem of protecting targets in infrastructure networks as a single-round defender–attacker zero-sum game. The defender chooses a subset of nodes to protect, while the attacker chooses some nodes to attack in the target network. Only the nodes chosen by the attacker, meanwhile not protected by the defender, will be removed from the network, and then the payoff function for both players is determined by the remaining network. Both players are assumed to have the complete information of the target network and full knowledge about the opponent. Hence, they are fully aware of all the strategies that the opponent may adopt, as well as the payoffs to each other under each combination of strategies. Nevertheless, the game is a simultaneous one, that is to say, the players do not know exactly which nodes the opponent will choose when making their own decisions.

2.1 Network

The infrastructure system can be easily abstracted as a target network, which is formalized in terms of a simple undirected graph $G = (V, E)$. Each node $v \in V$ represents an infrastructure, where V is the set of nodes in the network. An edge $e_{ij} = (v_i, v_j) \in E$ denotes a directionless edge with v_i and v_j as endpoints, while $E \subseteq V \times V$ denotes the set of edges. We define $N = |V|$ as the number of nodes in the network.

The connectivity between nodes is the equivalence relation on the node $v \in V$. Based on the equivalence relation, V can be divided into several non-empty subsets $V_1, V_2, \ldots, V_n$, and each non-empty subset V_i determines a connected subgraph $G(V_i)$. Especially for a node $v \in V$, we denote the node's connected neighbors as follows:

$$V' = \{u \in V \setminus \{v\} | (u, v) \in E, distance(u, v) \neq \infty, v \in V\}, \quad (1)$$

where $distance(u, v) \neq \infty$ indicates that there always exists a path from u to v. The connected subgraph $(V', E \cap (\frac{V'}{2}))$ induced by V' is denoted by $G(V')$. So, $G(V_1), G(V_2), \ldots, G(V_n)$ are defined as the connected components of G. Let $G(V_{max})$ represent the largest connected component (LCC) of G, where V_{max} is defined as the largest connected node subset of V.

Let $\tilde{V} \subseteq V$ denote the subset of nodes in V and $\tilde{E} \subseteq E$ denote the set of edges where each edge in $\tilde{E}$ is connected to at least one node in $\tilde{V}$. The graph $\hat{G} = (\hat{V}, \hat{E})$ obtained by removing all nodes in $\tilde{V}$ and all associated edges in $\tilde{E}$ from G is expressed as follows:

$$\hat{G} = G - \tilde{V}. \quad (2)$$

2.2 Strategies

A pure defender strategy $D = \langle d_v \rangle$ is an assignment of the R_D defending resources to R_D vertices, that is, $\sum_{v \in V} d_v = R_D$, where $d_v \in \{0, 1\}$. $d_v = 1$ indicates the node v is protected by a defender and will never be deleted. We define the set of nodes protected by the defender as $V^D = \{v \in V | d_v = 1\}$, where $|V^D| = R_D$. The defender's strategy space is defined as $\mathbb{D}$. So, a mixed attacker strategy $\mathbf{x} = \langle x_D \rangle$ is a probability distribution over pure strategies, with x_D representing the probability that the pure strategy D is played.

Meanwhile, the attacker can choose a subset of nodes $V^A \subseteq V$ to plan an attack. A pure attacker strategy is defined as a vector $A = \langle a_v \rangle \in \mathbb{A}$, where $\mathbb{A}$ represents the attacker's strategy space and $\sum_{v \in V} a_v = R_A$ indicates that the attacker's resource number is R_A. If $v \in V^A$, then $a_v = 1$; otherwise, $a_v = 0$. A mixed attacker strategy $\mathbf{y} = \langle y_A \rangle$ is a probability distribution over pure strategies,

with y_A representing the probability that the pure strategy A is played.

2.3 Utility

In our defender–attacker zero-sum game, given a defender's strategy D and an attacker's strategy A, only when $a_v = 1$, and $d_v = 0$, the node v will be deleted from the network by the attacker; otherwise, the defender protects the targets successfully. If the attacker succeeds, he will receive a payoff P_A and the defender's payoff P_D will be $-P_A$; otherwise, both players will gain 0.

In many critical infrastructure systems, the targets are networked and the functionality relies heavily on the connectivity and topology structures. If the network connectivity decreases during the node deletion, the performance of the networks will degrade. The node number of the largest connected component (N_{LCC}) of the graphs is a robust measure function which is widely used to evaluate the network performance. Hence, we adopt N_{LCC} to construct the payoff functions. $N_{LCC}(G)$ is calculated by determining the maximal connected node subset $V_{max} \subseteq V$ in G [21], and it can be expressed as follows:

$$N_{LCC}(G) = |V_{max}|. \tag{3}$$

If the defender's strategy D and the attacker's strategy A select sets of nodes differently, that is, $V^A \cap V^D \neq V^D$, which means the defender fails in protecting the targets and the attacker succeeds, then the node subset $\tilde{V} = V^A - V^A \cap V^D$ and its associated edge set $\tilde{E}$ will be deleted from the target network, and we define $\hat{V}_{max} \subseteq (V - \tilde{V})$ as the largest connected node subset of the residual graph $\hat{G}$. $N_{LCC}(\hat{G})$ is computed by determining the size of $\hat{V}_{max}$ as follows:

$$N_{LCC}\left(\hat{G}\right) = |\hat{V}_{max}|, \tag{4}$$

where $\hat{V}_{max} \subseteq (V - (V^A - V^A \cap V^D))$ in $\hat{G}$. Otherwise, if the defender protects the network successfully, that is, $V^A \cap V^D = V^D = V^A$, which means that no node will be deleted from G, then $N_{LCC}(\hat{G}) = N_{LCC}(G)$.

Hence, the payoff function of the attacker P_A is defined as follows:

$$P_A = \frac{N_{LCC}(G) - N_{LCC}\left(\hat{G}\right)}{N_{LCC}(G)} \in [0, 1] \tag{5}$$

and the defender's payoff function P_D is given as follows:

$$P_D = \frac{N_{LCC}\left(\hat{G}\right) - N_{LCC}(G)}{N_{LCC}(G)} \in [-1, 0], \tag{6}$$

where N_{LCC} can be replaced by any other measure functions that meet the monotonicity assumption.

After the payoff functions of the players are obtained, we define U_D as the expected utility function of the defender. Given a defender's mixed strategy $\mathbf{x}$ and an attacker's pure strategy A, the expected defender utility $U_D(\mathbf{x}, A)$ is given as follows:

$$U_D(\mathbf{x}, A) = \sum_{D \in \mathbb{D}} (1 - z_{D,A}) x_D P_D, \tag{7}$$

where $z_{D,A}$ indicates whether the defender strategy D successfully protects the targets that are attacked by A, that is, $z_{D,A} = 0$ if $D \cap A = D$ or 1 otherwise.

The defender's expected utility $U_D(D, \mathbf{y})$ of playing a pure defense strategy D against the mixed attack strategy $\mathbf{y}$ is

$$U_D(D, \mathbf{y}) = P_D \sum_{A \in \mathbb{A}} (1 - z_{D,A}) y_A. \tag{8}$$

When playing a mixed defense strategy $\mathbf{x}$ against the mixed attack strategy $\mathbf{y}$, the defender's expected utility $U_D(\mathbf{x}, \mathbf{y})$ is given as follows:

$$U_D(\mathbf{x}, \mathbf{y}) = \sum_{D \in \mathbb{D}} x_D U_D(D, \mathbf{y}) = \sum_{A \in \mathbb{A}} y_A U_D(\mathbf{x}, A). \tag{9}$$

Generally, based on the two-person zero-sum game, we note $U_A = -U_D$.

2.4 Equilibrium

The Nash equilibrium of two-person zero-sum games is the maximum equilibrium. The aim of the defender is to protect the target nodes of the network to maximize their minimum utility and minimize the attacker's maximum utility. We use linear programming to solve the zero-sum game. The defender's optimal mixed strategy $\mathbf{x}$ can be computed by solving the following linear programming (LP):

$$\max \quad U \tag{10}$$

$$s.t. \quad U \leq U_D(\mathbf{x}, A), \forall A \in \mathbb{A}, \tag{11}$$

$$\sum_{i=1}^{N} d_v = R_D, \tag{12}$$

$$\sum_{D \in \mathbb{D}} x_D = 1, \tag{13}$$

$$x_D \geq 0, \forall D \in \mathbb{D}. \tag{14}$$

When the strategy spaces of both sides are small, the optimal solution can be obtained by solving the programming **Equations 10–14**. However, as the network scale expands, the defender's strategy space $\mathbb{D}$ and the attacker's strategy space $\mathbb{A}$ will grow exponentially with the number of resources R_D. At this time, it is difficult to calculate the optimal solution in a short time by mathematical programming, so it is necessary to design new algorithms to get efficient strategies for both players.

3 APPROACH

In this section, we first give a brief introduction to the ESE algorithm, which is very similar to the problem solved in this study [20], and analyze the limitations of the algorithm. Then we propose our EMSL algorithm and describe it in detail.

3.1 Limitation of ESE Algorithm

The ESE algorithm is adopted by Li et al., which solves the attacker–defender game by computing the global equilibrium with full strategy space on a small network [20]. First, they enumerate all possible attack and defense strategies and

calculate the payoffs of the players in each strategy to construct the payoff matrix. Next, they start the two-person zero-sum game by choosing nodes with the largest degrees to attack, satisfying the resource constraint, and identify the defender's best response to the attacker's strategy. Then they compute the best response pure strategies over the payoff matrix for the players. Finally, the Nash equilibrium is computed to calculate the players' best mixed response strategies over each pure strategy.

Unfortunately, the ESE algorithm can only be solved on the network with 20 nodes. Since the strategy space is too large as the network scale grows, it is very time-consuming to calculate the payoffs in each strategy profile one by one. It is impossible to solve the problem by enumerating all strategies to maximize the benefits of both the attacker and the defender. So, the ESE algorithm cannot be applied to real large-scale networks due to its limited computing power.

We find that the interaction process of the players in the ESE algorithm is similar to the Double Oracle (DO) framework. The DO framework is a standard method for solving zero-sum games with large strategy spaces.

However, there are two challenges to solving the INP game under the DO framework: 1) We can only present the MILP for computing the best response strategy of the attacker (in **Section 4.2**), and we solve it on the network with 20 nodes. The best attack method is used as an attack method for comparison in the experiments. But it is difficult to present the MILP for computing the best response strategy of the defender because of the weakness of high complexity. 2) Computing the MILP is time-consuming, and it is difficult to solve it for an optimal solution on large networks. We aim to find an efficient solution for the INP problem, but not an optimal solution. The effective solution can be obtained by designing an approximate algorithm under the suboracles of DO framework. Hence, we propose the effective mixed strategies for large-scale networks (EMSL) algorithm for computing the improved solution.

3.2 EMSL Algorithm

To solve the INP problem, we propose our EMSL algorithm based on greedy search under the DO framework. The DO framework can efficiently solve the zero-sum games on real large networks. For instance, Jain et al. proposed the SNARES algorithm to solve the security scheduling problem on the Mumbai road network with 9,503 nodes and 20,416 edges [22]. And Wang et al. introduced the DO-TPD algorithm to compute an optimal monitoring strategy for detecting terrorist plots on realistic-sized problems, which contains about 100 such potential terrorists in some 1,400 French nationals [23]. The DO framework is formed from Defender Oracle and Attacker Oracle. And both of the oracles contain Best Oracle and Better Oracle. Best Oracle can compute the optimal solution by solving the MILP, instead of enumerating all possible strategies, while Better Oracle can improve the computing efficiency for an approximate solution. Due to the challenges of solving Best Oracle mentioned in **Section 3.1**, we design the EMSL algorithm under Better Oracle (EMSL-Better-O). It is sketched in Algorithm 1.

Algorithm 1. EMSL-Better-O overview (G, R_D, R_A).

Input: $G = \langle V, E \rangle$, R_D, R_A
Output: Mixed strategies $(\mathbf{x}, \mathbf{y})$
1 **Initialize** $\mathbb{D}'$, $\mathbb{A}'$ **randomly** ;
2 **repeat**
3 $\quad (\mathbf{x}, \mathbf{y}) \leftarrow CoreLP(\mathbb{D}', \mathbb{A}')$;
4 $\quad \mathbb{D}^+ \leftarrow betterO - D(\mathbf{x}, \mathbf{y})$;
5 $\quad \mathbb{D}' \leftarrow \mathbb{D}' \cup \mathbb{D}^+$; /*Lines 4-5: Defender Oracle */
6 $\quad \mathbb{A}^+ \leftarrow betterO - A(\mathbf{x}, \mathbf{y})$;
7 $\quad \mathbb{A}' \leftarrow \mathbb{A}' \cup \mathbb{A}^+$; /*Lines 6-7: Attacker Oracle */
8 **until** $\mathbb{D}^+ = \emptyset$ *and* $\mathbb{A}^+ = \emptyset$;

Line 1 first initializes EMSL-Better-O by generating a small strategy space $\langle \mathbb{D}', \mathbb{A}' \rangle$ randomly. Then **Equation 9** computes the equilibrium with $\langle \mathbb{D}, \mathbb{A} \rangle$ replaced by $\langle \mathbb{D}', \mathbb{A}' \rangle$ to solve the restricted version of INP (CoreLP, Line 3). The restricted INP can be solved efficiently because the strategy space $\langle \mathbb{D}', \mathbb{A}' \rangle$ is small. Obviously, the solution obtained is an equilibrium of the restricted INP and does not form an equilibrium to the original INP. So, both players want to improve their utilities with other strategies out of $\langle \mathbb{D}', \mathbb{A}' \rangle$. EMSL-Better-O allows them to do so with Better Oracle (Lines 4–5 and Lines 6–7). Specifically, EMSL-Better-O calls BetterO-D (Better Oracle for Defender) to search a set of improving strategies for the defender (Lines 4–5). And in the similar manner, EMSL-Better-O calls BetterO-A (Better Oracle for Attacker) to find improving strategies for the attacker (Lines 6–7). The process repeats until no improving strategy can be found for both players (Line 8), when the final solution obtained for the original INP is close to optimal.

The EMSL-Better-O algorithm of Defender Oracle (EMSL-Better-OD) is presented in Algorithm 2. EMSL-Better-OD generates a defender pure strategy D_{Better}. The core of each iteration (Lines 5–8) is designed based on the greedy search.

Algorithm 2. EMSL-Better-OD $(\mathbf{x}, \mathbf{y})$.

Input: $(\mathbf{x}, \mathbf{y})$
Output: $\mathbb{D}_{Better}$
1 **Initialize** $D_{Better} = \emptyset$;
2 **Start with** D randomly, $A \leftarrow \mathbf{y}$;
3 **repeat**
4 $\quad$ **for** $v \in V$ **do**
5 $\quad\quad$ **while** *no termination condition is met* **do**
6 $\quad\quad\quad D' \leftarrow GreedySearch(v, D, \mathbf{y})$;
7 $\quad\quad\quad$ **if** $U_D(D', \mathbf{y}) > U_D(D, \mathbf{y})$ **then**
8 $\quad\quad\quad\quad D \leftarrow D'$;
9 $\quad\quad$ **if** $U_D(D, \mathbf{y}) > U_D(\mathbf{x}, \mathbf{y})$ **then**
10 $\quad\quad\quad \mathbb{D}_{Better} \leftarrow \mathbb{D}_{Better} \cup D$;
11 **until** $U_D(\mathbb{D}_{Better}, \mathbf{y}) = U_D(\mathbf{x}, \mathbf{y})$;

EMSL-Better-OD repeatedly starts from an empty strategy space $\mathbb{D}_{Better}$ and initializes a random pure strategy $D \in \mathbb{D}$ (Lines 1–2). Then in a greedy manner, it iteratively applies $GreedySearch(v, D, \mathbf{x})$ (Algorithm 3) for a new local optimal strategy D' that brings the maximum utility to the defender (Line

6). Afterward, the strategy set D is updated systematically by D' (Lines 7–8). The loop repeats until the termination conditions are met: 1) $U_D(D, \mathbf{y}) > U_D(\mathbf{x}, \mathbf{y})$; 2) $D^+ = \varnothing$; and 3) $U_D(D, \mathbf{y}) - U_D(\mathbf{x}, \mathbf{y}) < \epsilon$, where ϵ is a pre-defined global variable to constrain the total number of iterations. The defense strategy $\mathbb{D}_{Better}$ is computed over the local optimal strategies (Lines 9–10). Compared with enumerating all strategies to construct a payoff matrix and calculating the global equilibrium, our algorithm based on greedy search effectively improves the computing power.

Algorithm 3. *GreedySearch*(v, D, $\mathbf{x}$).

```
   Input: (x, y)
   Output: A pure defense strategy D
1  Start with D = ∅;
2  repeat
3      for v ∈ V do
4          v' ← argmax_{v∈V^D} U_D(D ∪ {v}, y);
5          if U_D(D ∪ {v'}, y) > U_D(D, y) then
6              D ← D ∪ {v'};
7          else
8              v' ← argmax_{v∈D\(V^D∪{v})} U_D(D\{v}, y);
9              if U_D(D\{v'}, y) > U_D(D, y) then
10                 D ← D\{v'};
11 until |D| = R_D;
```

The goal of *GreedySearch* (v, D, $\mathbf{x}$) is to find a pure defense strategy that can improve the defender's utility. It repeatedly starts from an empty strategy $D = \varnothing$, and it consecutively tries to add a best node v' in the hope of improving the defender's utility U_D (Line 4). If the node v' satisfies $U_D(D \cup \{v'\}, \mathbf{y}) > U_D(D, \mathbf{y})$, then $D \leftarrow D \cup \{v'\}$ (Lines 5–6); otherwise, it tries to add a best node v' from the rest node set $D\backslash\{v'\}$ (Line 8). If $U_D(D\backslash\{v'\}, \mathbf{y}) > U_D(D, \mathbf{y})$, then $D \leftarrow D\backslash\{v'\}$ (Line 9–10). Finally, it stops when $|D| = R_D$. Note that the utility function is a submodular set function, which guarantees the approximate solution a $(1 - \frac{1}{e})$ approximation ratio to the optimal solution [24].

The time complexity of our approximate algorithm is $O(N^2)$, and the spatial complexity is $S(N^2)$, where N is the size of the networks. Our algorithm can be solved within a limited time complexity.

4 EXPERIMENTAL RESULTS AND ANALYSIS

We assess the performance of our approach through a number of experiments. The algorithms proposed in this article are coded in Visual Studio. Core-LP and MILP are solved by calling CPLEX. All computations are performed on a machine with a 3.60 GHz quad core CPU and 8.00 GB memory. The parameter ϵ in EMSL-Better-OD (Algorithm 2) is set to be 0.05. The number of defense resources R_D is set to be $\frac{1}{5}*N$ (see **Section 4.3.1**), and the attack resource number R_A is set to be equal and variable from 0 to N. We conduct experiments on two types of graphs with $N_1 = 20$ and $N_2 = 500$.

In this section, the defense methods for comparison and the attack methods for confrontation are introduced first. Then the solution of the approximate algorithm on two different networks is presented and analyzed.

4.1 Defense Methods for Comparison

It is essential to prove the effect of the defender's mixed strategies with other defense methods. The typical defense methods we used for comparison are as follows:

1) ID Defense [25]: In the initial network, the degree of each node is first calculated in the network, and then the vertex is chosen in descending order from the highest vertex to defense. After each attack, the network structure will change, and the degree of each node may also change, but it will not be recalculated. That is to say, the defending strategy uses the initial degree distribution, so we call it the "ID Defense" method.
2) IB Defense [25]: In the initial network, the betweenness of each node is calculated first, and then the vertex is selected for defense according to the descending order of betweenness. Similarly, this defending strategy is also distributed according to the initial mediation degree, so it is called the "IB Defense" method.
3) RA Defense: In the initial network, nodes are randomly selected for defense. In this article, we call it the "RA Defense" method. It should be noted that although random selection seems to be the most convenient way, some key nodes may be selected, which makes the experimental results accidental. In order to avoid the occurrence of the previous situation, we will repeat the process of selecting nodes randomly and calculating the results when carrying out RA Defense. Finally, the average of all the results is calculated as the final result.
4) DCM Defense [26]: In the initial network, nodes are defended by the mixed strategies, where the marginal coverage probability of each vertex is normalized degree centrality. Given the marginal coverage probabilities, the mixed strategies are generated using the comb sampling algorithm.

4.2 Attack Methods

Considering the actual situation that attackers may take many kinds of attacks to achieve their goals, it is also important to verify that the defender's mixed strategy obtained by the approximate algorithm is efficient due to different attacks. Many relative works analyze the robustness of the critical infrastructure networks against malicious attacks. The first class estimates the robustness by removing nodes or edges based on the load capacity [27–30]. The second class comes up with removing some nodes or edges based on the degree distribution or betweenness distribution of the networks [10, 28, 29, 25, 13, 31, 32]. The third class develops the method of the tabu search into the network disintegration problem to identify the optimal attack strategy is introduced [33].

So, based on the model and scenario of this study, the attack methods we chose for confrontation are as follows:

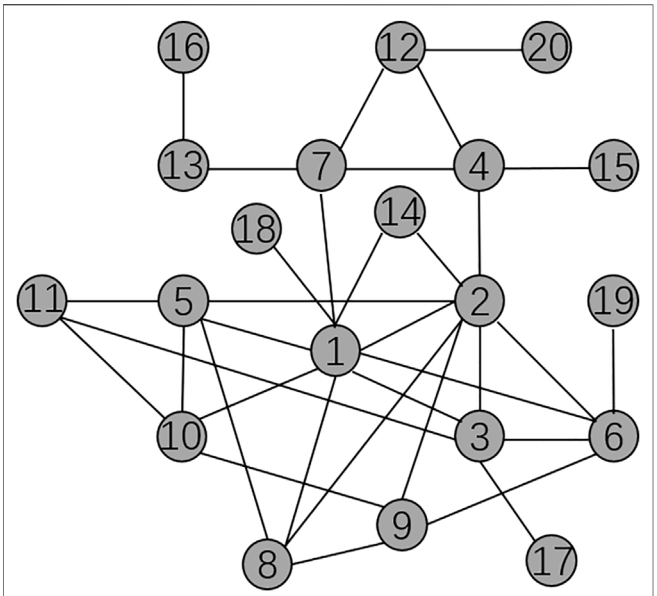


FIGURE 1 | Topology structure of a small network with 20 nodes [20].

1) ID Attack: Attacking nodes based on the initial degree distribution of the network.
2) IB Attack: Attacking nodes based on the initial betweenness distribution of the network.
3) RA Attack: Attacking nodes randomly in the networks.
4) BEST-OA Attack: Attacking nodes with the best attack strategy. We consider the worst case, that is, assuming that the attacker always chooses the most destructive attack method. So, we use mixed-integer linear programming (MILP) to solve the best pure attack strategy for an attacker, and it is called the "BEST-OA Attack" method. The MILP is shown in the following equations:

$$\max \quad \sum_{D\in\mathbb{D}} \left(\frac{N_{LCC}(G) - N_{LCC}\left(\hat{G}\right)}{N_{LCC}(G)} \right) \cdot x_D \tag{15}$$

$$s.t. \quad \sum_{D\in\mathbb{D}} x_D = 1, x_D \geq 0, \forall D \in \mathbb{D}, \tag{16}$$

$$\sum_{i=1}^{N} a_v = R_A, a_v \in V^A, a_v \in \{0,1\}, \tag{17}$$

$$\sum_{i=1}^{N} d_v = R_D, d_v \in V^D, d_v \in \{0,1\}, \tag{18}$$

$$d_v \cdot a_v - d_v < v_i^{DA} < d_v \cdot a_v - d_v + 2, \tag{19}$$

$$v_i^{DA} + v_j^{DA} - 1 \leq e_{ij}^{DA}, v_i^{DA} \in \{0,1\}, e_{ij}^{DA} \in \{0,1\}, \tag{20}$$

$$e_{ij}^{DA} \leq v_i^{DA}, e_{ij}^{DA} \leq v_j^{DA}, \tag{21}$$

$$\sigma_{jk}^{DA} - \sigma_{ik}^{DA} \geq e_{ij}^{DA} - 1, \sigma_{ij}^{DA} \in \{0,1\}, \tag{22}$$

$$N_{LCC}\left(\hat{G}\right) \geq \sum_{v_i\in V^D} \sigma_{ij}^{DA}, \tag{23}$$

where $v_i^{DA} = 1$ represents the node v_i is still in $\hat{G}$ when it is attacked by A under the protection of D; otherwise, $v_i^{DA} = 0$. $e_{ij}^{DA} = 1$ represents the edge between nodes v_i and v_j is still in $\hat{G}$ when it is attacked by A under the protection of D; otherwise, $e_{ij}^{DA} = 0$. $\sigma_{ij}^{DA} = 1$ represents nodes v_i and v_j are still in the same connected subgraph when they are attacked by A under the protection of D; otherwise, $\sigma_{ij}^{DA} = 0$. Specifically, $\sigma_{ii} = 1$. **Equations 19–23** constrain the existence of connected subgraphs after attack. The goal of defenders in best attack oracle is to verify an optimal attack strategy over the entire pure strategy space. Unfortunately, solving best attack oracle turns out to be NP-hard, and the MILP only can be solved on small networks [23].

4.3 Solution of the Approximation Algorithm

To verify the performance of the mixed defense strategies, we solve the defender–attacker model by conducting experiments on a small network with 20 nodes first, which is used by Li [20], and then extend to the U.S. air transportation network with 500 nodes [34]. At the same time, the evolution of robustness of networks is analyzed under two topological changes.

4.3.1 Effectiveness of the Mixed Defense Strategies on Small Network

A small network topology structure with 20 nodes is shown in **Figure 1**. The numbers of attack resources R_A and defense resources R_D are set to be equal and variable from 0 to 20. To validate the effectiveness of the mixed strategy in small networks, we compare the results with those of some other typical defense strategies under different attack methods. The typical defense strategies for comparison here are ID Defense, IB Defense, RA Defense, DCM Defense, and NO Defense which means $R_D = 0$. The curve of NO Defense is shown as a baseline. And the attack strategies used in this section are ID Attack, IB Attack, RA Attack, and BEST-OA Attack. These comparison defense strategies and attack strategies have been introduced in the previous subsections.

• Effectiveness Analysis

As shown in **Figures 2A–D**, what the curves represent are the defender's utility, while $R_D = 4$ and R_A is variable from 0 to 20 on a small network. The vertical axis represents the defender's utility, and the horizontal axis represents the number of attack resources. A higher defender utility indicates a lower attacker utility given the zero-sum assumption as well as better performance of the mixed defense strategy. The results show that with the increase of attack resources, the decline rate of defender's utility is the slowest under the protection of the mixed defense strategy. And no matter in which attack mode, the defender's utility obtained by the mixed defense strategy is higher than that obtained by other defense methods, especially in the case of RA Attack. Although under IB Attack, the results of IB defense, RA Defense, and mixed strategy defense are close to each other, the mixed strategy is still performing the best (**Figure 2B**). The results are sufficient enough to indicate the effectiveness of our approximation algorithm in small networks.

- Optimal defense resource number based on unit resource efficiency

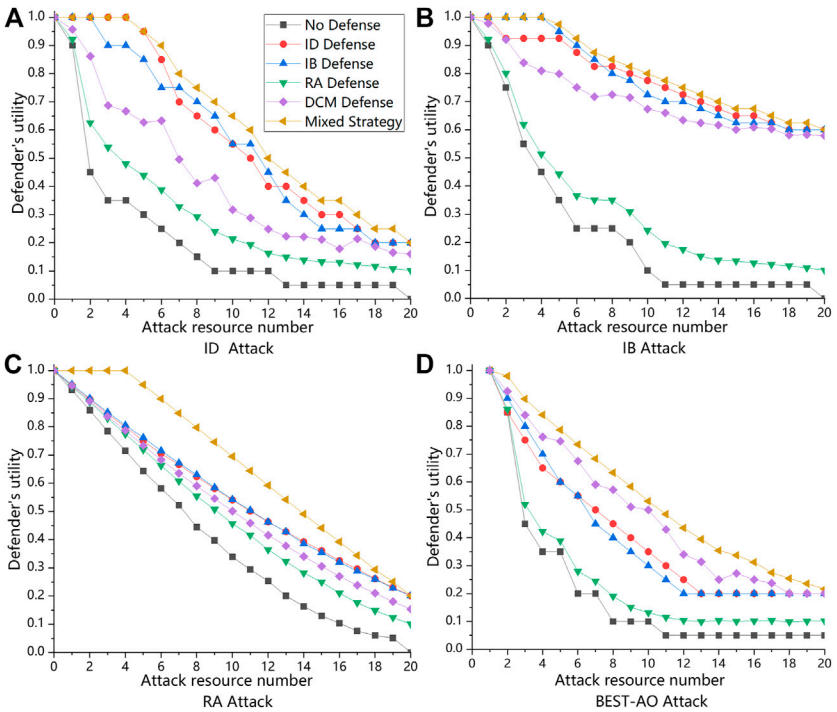


FIGURE 2 | These are defender's utility of the mixed defense strategy and other comparison defense methods under different attack methods while $R_A = 4$ on small network with $|V| = 20$. R_D is variable from 0 to 20. **(A)** is the defender's utility when playing ID Attack strategy with different defense strategies. **(B)** is the defender's utility when playing IB Attack strategy with different defense strategies. **(C)** is the defender's utility when playing RA Attack strategy with different defense strategies. **(D)** is the defender's utility when playing BEST-AO Attack strategy with different defense strategies.

TABLE 1 | Utility of the defender when the BEST-OA Attack method confronts the ID Defense method.

$R_A \mid R_D$	0	1	2	3	4	5	6	7	8	9	10
0	1	1	1	1	1	1	1	1	1	1	1
1	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.9	0.9	0.9	0.9
2	0.45	0.65	0.65	0.65	0.75	0.75	0.75	0.8	0.8	0.8	0.8
3	0.35	0.55	0.55	0.55	0.65	0.65	0.7	0.75	0.75	0.75	0.75
4	0.35	0.45	0.45	0.5	0.6	0.6	0.65	0.7	0.7	0.7	0.7
5	0.2	0.4	0.4	0.45	0.55	0.55	0.6	0.65	0.65	0.65	0.65
6	0.2	0.3	0.3	0.4	0.5	0.5	0.55	0.6	0.6	0.6	0.6
7	0.1	0.25	0.25	0.35	0.45	0.45	0.5	0.55	0.55	0.55	0.55
8	0.1	0.15	0.2	0.3	0.4	0.4	0.45	0.5	0.5	0.5	0.5
9	0.1	0.1	0.15	0.25	0.35	0.35	0.4	0.45	0.45	0.45	0.5
10	0.05	0.1	0.1	0.2	0.3	0.3	0.35	0.4	0.4	0.45	0.5

TABLE 2 | Increment of the defender's utility.

$R_A \mid R_D$	1	2	3	4	5	6	7	8	9	10
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0.05	0	0	0
3	0.2	0	0	0.1	0	0	0.05	0	0	0
4	0.2	0	0	0.1	0	0.05	0.05	0	0	0
5	0.1	0	0.05	0.1	0	0.05	0.05	0	0	0
6	0.2	0	0.05	0.1	0	0.05	0.05	0	0	0
7	0.1	0	0.1	0.1	0	0.05	0.05	0	0	0
8	0.15	0	0.1	0.1	0	0.05	0.05	0	0	0
9	0.05	0.05	0.1	0.1	0	0.05	0.05	0	0	0
10	0	0.05	0.1	0.1	0	0.05	0.05	0	0	0.05

With the network growing, it is essential to define the optimal defense resource number R_D. We define the number of resources per unit as 1 resource, adding one unit of resources per experiment. Then we repeatedly calculate the increment of the defender's profit after adding the unit resource under different defense and attack methods. Finally, we calculate the defender's average profit increment. The number of defense resources that maximize the defender's average profit increment is defined as the optimal defense resources.

For example, **Table 1** shows the benefits of the defender when the BEST-OA Attack method confronts the ID Defense method,

TABLE 3 | Average value of the defender's utility increment.

R_D	1	2	3	4	5	6	7	8	9	10
Average	0.0548	0.0262	0.0524	0.0690	0.0214	0.0429	0.0476	0.0238	0.0262	0.0286

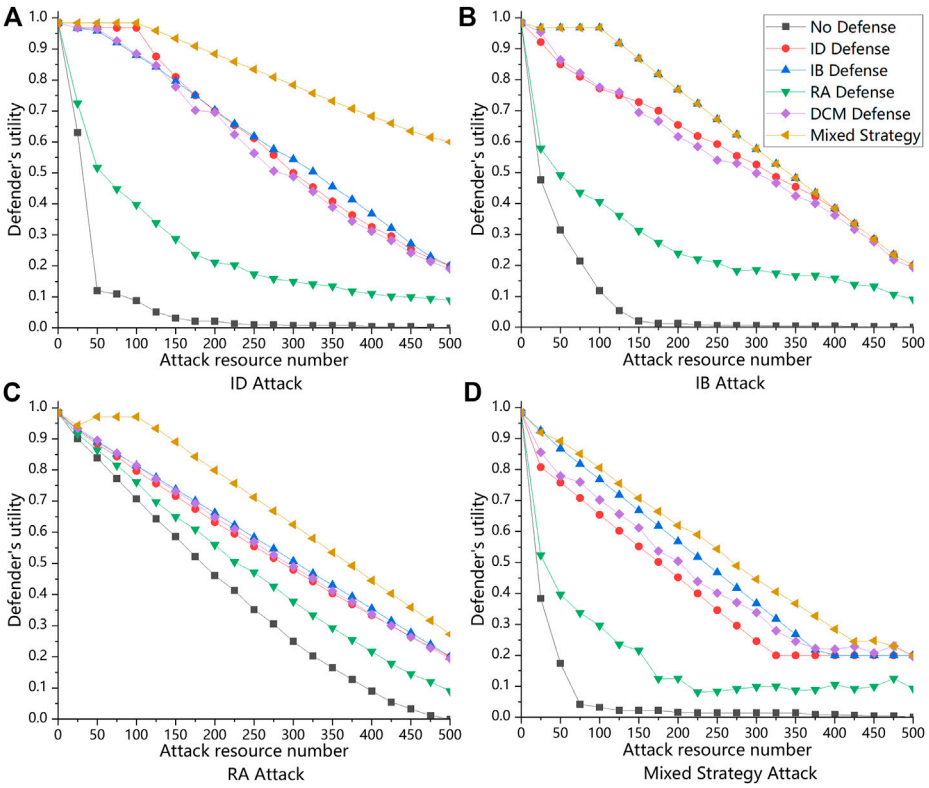


FIGURE 3 | These are defender's utility of the mixed defense strategy and other comparison defense methods under different attack methods while $R_D = 100$ on the air transportation network with $|V| = 500$. R_A is variable from 0 to 500. **(A)** is the defender's utility when playing ID Attack strategy with different defense strategies. **(B)** is the defender's utility when playing IB Attack strategy with different defense strategies. **(C)** is the defender's utility when playing RA Attack strategy with different defense strategies. **(D)** is the defender's utility when playing Mixed Attack strategy with different defense strategies.

while R_A and R_D are from 1 to 10. **Table 2** shows the increment of the defender's profit after each increase of unit resources. And **Table 3** shows the average value of the defender's profit increment. We find that when the number of resources is 4, the average increment of the defender's utility is the biggest. So, the optimal defense resource number is 4, which is equivalent to $\frac{1}{5}$ of the total node number on the network with 20 nodes. Hence, when we expand the experiments to a large network of 500 nodes, the corresponding optimal number of defense resources is 100. It is convenient to find the optimal defense resource number in large networks with the aforementioned method, which also can reflect the significance of the experimental results more clearly and intuitively.

4.3.2 Effectiveness of the Mixed Defense Strategies on Real Large-Scale Network

Then to evaluate the solution quality of the approximate algorithm on large-scale networks, we conduct experiments on the U.S. air transportation network with 500 nodes [34], and the defense resource number is set to be $R_D = 100$. We separately analyze the results of the mixed defense strategy and the mixed attack strategy to further test the performance of the mixed defense strategy. The experimental results are shown in **Figures 3A–D** and **Figures 4A–F**.

In **Figures 3A–D**, these graphs show the defender's utility when using the mixed defense strategy and other comparison defense methods under different attack methods while $R_D = 100$ on the real large-scale network. All the steps and comparison defense strategies of the experiments in this subsection are the same as in **Subsection 4.3.1**. The attack methods for confrontation are changed to ID Attack, IB Attack, RA Attack, and mixed strategy attack. Since the best attack strategy computed by MILP can only be solved in small networks due to its limited solving ability, we compute the mixed attack strategy by solving the approximate algorithm. In particular, we find that

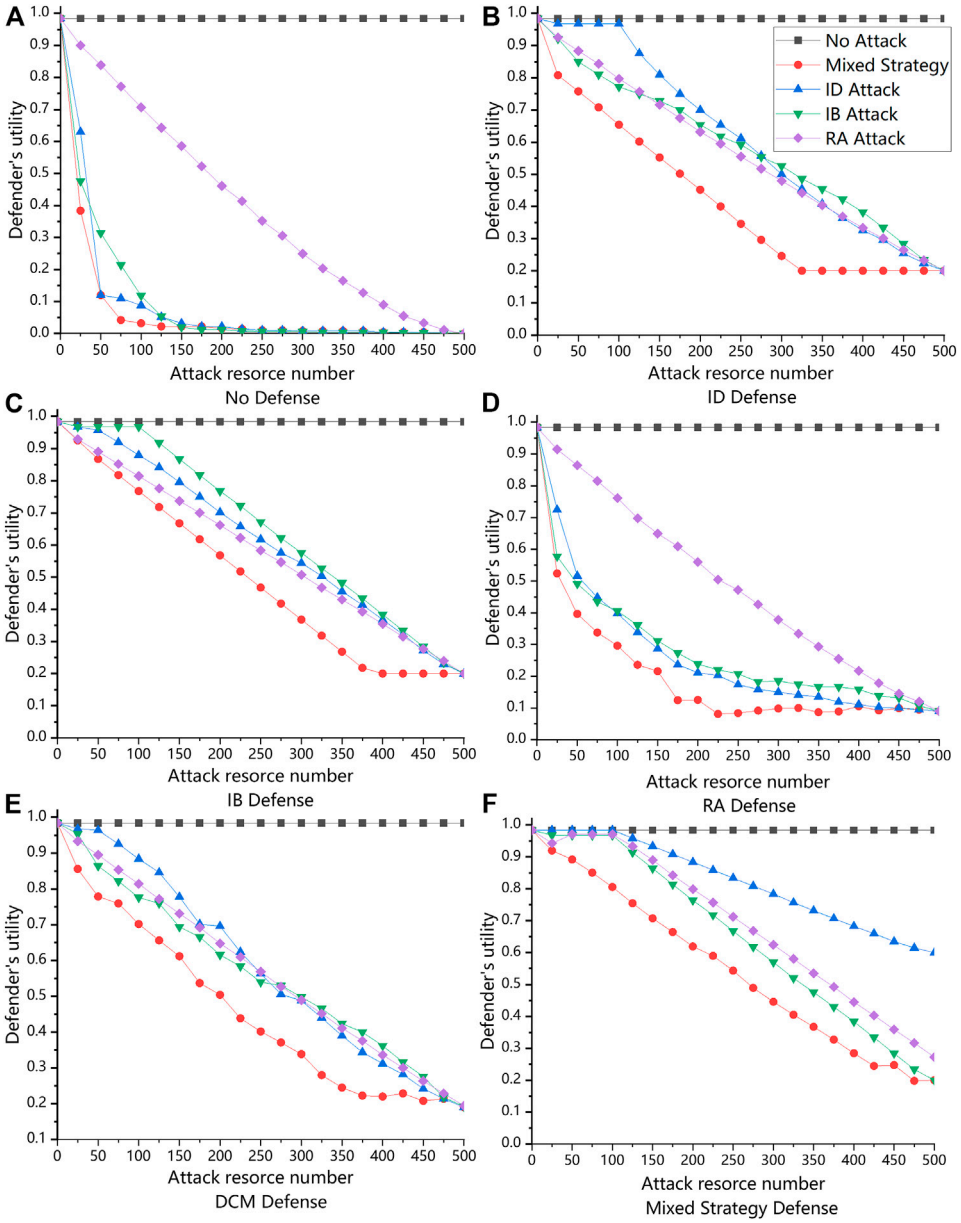


FIGURE 4 | These are defender's utility of the mixed defense strategy and other comparison defense methods under different defense methods while $R_D = 100$ on the air transportation network with $|V| = 500$. R_A is variable from 0 to 500. **(A)** is the defender's utility when playing different attack strategies with no defense. **(B)** is the defender's utility when playing ID Defense strategy with different attack strategies. **(C)** is the defender's utility when playing IB Defense strategy with different attack strategies. **(D)** is the defender's utility when playing RA Defense strategy with different attack strategies. **(E)** is the defender's utility when playing Mixed DCM strategy with different attack strategies. **(F)** is the defender's utility when playing Mixed Defense strategy with different attack strategies.

under IB Attack, the curves of IB Defense and mixed strategy defense are almost coincident (**Figure 3B**), which indicates that IB Defense performs well in dealing with IB Attack and also reflects that our approximation algorithm may fall into local optimization. The final result of our approximate algorithm depends in part on its initial solution. Anyway, in most cases, the results can be better than those of other methods. These figures obviously describe that under the mixed strategy defense, the decline rate of defender's utility is the slowest no matter which attack strategy is used, and the mixed defense strategy can still work well under different attacks in large-scale networks.

Figures 4A–F show the defender's utility when using the mixed attack strategy and other comparison attack methods confronting different defense strategies while $R_D = 100$ on the same real large-scale network. The comparison attack strategies and defense strategies are all the same. The results clearly show that no matter in which attack strategy, the mixed defense strategy always brings the highest utility to the defender and

can make the defender's utility decline the slowest in the shortest time. Moreover, it is worth mentioning that the defender's utility obtained by the mixed attack strategy declines the fastest, which also reflects the mixed defense strategy solved by the approximate algorithm can effectively destroy the networks. In summary, these results certainly reflect that the mixed defense strategy performs well in large-scale networks and our approximate algorithm can solve the problem efficiently when scaling up the networks.

5 CONCLUSION

It is a challenge to reasonably design effective defense strategies with limited resources to protect large-scale critical infrastructure networks against malicious attacks. In this study, we first develop an efficient approximation algorithm under the Double Oracle framework to speed up the calculation for computing the mixed defense strategy based on heuristics significantly with given resources. Then we extend the INP problem to a real large-scale infrastructure network to test the performance of the mixed defense strategy. Finally, we conduct extensive experiments on two networks of different sizes by comparing with other defense strategies under various attacks. The experimental results show that our approximation algorithm can ensure a robust enough solution to protect real large-scale networks.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, and further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

ZW contributed to the conception of the study. MJ performed the data analyses and wrote the manuscript. YY performed the experiments. LC and HD helped perform the analysis with constructive discussions.

FUNDING

This research was supported by the Zhejiang Provincial Natural Science Foundation of China (No. LY20F030012) and National Natural Science Foundation of China (62176080).

REFERENCES

1. Jasso C. *"cyberattacks Insider Sabotage": Venezuela's Power Grid Still under Attack – Maduro* (2019). Available at: https://www.rt.com/news/453434-venezuela-maduro-cyberattack-power-grid/ (Accessed October 8, 2021).
2. Wikipedia. *Colonial Pipeline Cyberattack* (2021). Available at: https://en.wikipedia.org/wiki/Colonial_Pipeline_cyber_attack/ (Accessed October 8, 2021).
3. Schneider CM, Moreira AA, Andrade JS, Havlin S, Herrmann HJ. Mitigation of Malicious Attacks on Networks. *Proc Natl Acad Sci* (2011) 108:3838–41. doi:10.1073/pnas.1009440108
4. Yang Y, Li Z, Chen Y, Zhang X, Wang S. Improving the Robustness of Complex Networks with Preserving Community Structure. *PloS one* (2015) 10: e0116551. doi:10.1371/journal.pone.0116551
5. Liu Y, Wei B, Wang Z, Deng Y. Immunization Strategy Based on the Critical Node in Percolation Transition. *Phys Lett A* (2015) 379:2795–801. doi:10.1016/j.physleta.2015.09.017
6. Jiang Y, Zhou Y, Li Y. Reliable Task Allocation with Load Balancing in Multiplex Networks. *ACM Trans Auton Adapt Syst* (2015) 10:1–32. doi:10.1145/2700327
7. Jiang J, An B, Jiang Y, Zhang C, Cao J. Group-oriented Task Allocation for Crowdsourcing in Social Networks. *IEEE Trans Syst Man, Cybernetics: Syst* (2019) 1–16.
8. Briesemeister L, Lincoln P, Porras P. Epidemic Profiles and Defense of Scale-free Networks. in " Proceedings of the 2003 ACM Workshop on Rapid Malcode, Washington, DC, USA, October 27, 2003 (2003) (New York, NY, USA: Association for Computing Machinery), 67–75. doi:10.1145/948187.948200
9. Beygelzimer A, Grinstein G, Linsker R, Rish I. Improving Network Robustness by Edge Modification. *Physica A: Stat Mech its Appl* (2005) 357:593–612. doi:10.1016/j.physa.2005.03.040
10. Leskovec J, Krause A, Guestrin C, Faloutsos C, VanBriesen J, Glance N. Cost-effective Outbreak Detection in Networks. in " Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, California, USA, August 12–15, 2007 (2007) (New York, NY, United States: Association for Computing Machinery), 420–9. doi:10.1145/1281192.1281239
11. Chen C, Tong H, Prakash BA, Tsourakakis CE, Eliassi-Rad T, Faloutsos C, et al. Node Immunization on Large Graphs: Theory and Algorithms. *IEEE Trans Knowledge Data Eng* (2015) 28:113–26.
12. Tong H, Prakash BA, Tsourakakis C, Eliassi-Rad T, Chau DH. *On the Vulnerability of Large Graphs*. IEEE International Conference on Data Mining (2010).
13. Liu Y, Sanhedrai H, Dong G, Shekhtman LM, Wang F, Buldyrev SV, et al. Efficient Network Immunization under Limited Knowledge. *Natl Sci Rev* (2021) 8:nwaa229. doi:10.1093/nsr/nwaa229
14. Li Y-P, Tan S-Y, Deng Y, Wu J. Attacker-defender Game from a Network Science Perspective. *Chaos* (2018) 28:051102. doi:10.1063/1.5029343
15. Zeng C, Ren B, Li M, Liu H, Chen J. Stackelberg Game under Asymmetric Information in Critical Infrastructure System: From a Complex Network Perspective. *Chaos* (2019) 29:083129. doi:10.1063/1.5100849
16. Li Y, Qiao S, Deng Y, Wu J. Stackelberg Game in Critical Infrastructures from a Network Science Perspective. *Physica A: Stat Mech its Appl* (2019) 521:705–14. doi:10.1016/j.physa.2019.01.119
17. Zeng C, Ren B, Liu H, Chen J. Applying the Bayesian Stackelberg Active Deception Game for Securing Infrastructure Networks. *Entropy* (2019) 21:909. doi:10.3390/e21090909
18. Zhang X, Ding S, Ge B, Xia B, Pedrycz W. Resource Allocation Among Multiple Targets for a Defender-Attacker Game with False Targets Consideration. *Reliability Eng Syst Saf* (2021) 211:107617. doi:10.1016/j.ress.2021.107617
19. Ma L, Liu J, Duan B. Evolution of Network Robustness under Continuous Topological Changes. *Physica A: Stat Mech its Appl* (2016) 451:623–31. doi:10.1016/j.physa.2016.01.088
20. Li Y, Xiao Y, Li Y, Wu J. Which Targets to Protect in Critical Infrastructures - A Game-Theoretic Solution from a Network Science Perspective. *IEEE Access* (2018) 6:56214–21. doi:10.1109/access.2018.2872767
21. Freitas S, Yang D, Kumar S, Tong H, Chau DH. *Graph Vulnerability and Robustness: A Survey*. arXiv preprint arXiv:2105.00419 (2021).
22. Jain M, Conitzer V, Tambe M. "Security Scheduling for Real-World Networks," in Proceedings of the 2013 International Conference on Autonomous Agents and Multi-Agent Systems, St. Paul, MN, USA, May

6–10, 2013 (2013) (Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems), 215–22. doi:10.5555/2484920
23. Wang Z, Yin Y, An B. "Computing Optimal Monitoring Strategy for Detecting Terrorist Plots," in Proc AAAI Conference on Artificial Intelligence, Phoenix, Arizona, USA, February 12–17, 2016 (2016) (CA, USA: AAAI), 30.
24. G L, Nemhauser L, WolseyM A. *An Analysis of Approximations for Maximizing Submodular Set Functions—I*. Germany: Mathematical Programming (1978).
25. Holme P, Kim BJ, Yoon CN, Han SK. Attack Vulnerability of Complex Networks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2002) 65:056109. doi:10.1103/PhysRevE.65.056109
26. Tsai J, Yin Z, Kwak JY, Kempe D, Tambe M. *Urban Security: Game-Theoretic Resource Allocation in Networked Physical domainsTwenty-Fourth Aaai Conference on Artificial Intelligence* (2011).
27. Motter AE, Lai YC. Cascade-based Attacks on Complex Networks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2002) 66:065102. doi:10.1103/PhysRevE.66.065102
28. Zhao L, Park K, Lai YC. Attack Vulnerability of Scale-free Networks Due to Cascading Breakdown. *Phys Rev E Stat Nonlin Soft Matter Phys* (2004) 70: 035101. doi:10.1103/PhysRevE.70.035101
29. Holmgren AJ. Using Graph Models to Analyze the Vulnerability of Electric Power Networks. *Risk Anal* (2006) 26:955–69. doi:10.1111/j.1539-6924.2006.00791.x
30. Nguyen DT, Shen Y, Thai MT. Detecting Critical Nodes in Interdependent Power Networks for Vulnerability Assessment. *IEEE Trans Smart Grid* (2013) 4:151–9. doi:10.1109/tsg.2012.2229398
31. Duan B, Liu J, Zhou M, Ma L. A Comparative Analysis of Network Robustness against Different Link Attacks. *Physica A: Stat Mech its Appl* (2016) 448: 144–53. doi:10.1016/j.physa.2015.12.045
32. Nguyen Q, Pham HD, Cassi D, Bellingeri M. Conditional Attack Strategy for Real-World Complex Networks. *Physica A: Stat Mech its Appl* (2019) 530: 121561. doi:10.1016/j.physa.2019.121561
33. Deng Y, Wu J, Tan YJ. Optimal Attack Strategy of Complex Networks Based on Tabu Search. *Physica A: Stat Mech its Appl* (2016) 442:74–81. doi:10.1016/j.physa.2015.08.043
34. Opsahl T. *The united states Air Transportation Network* (2007). Available at: https://toreopsahl.com/datasets/#usairports (Accessed June 23, 2021).

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

REVIEW
published: 24 December 2021
doi: 10.3389/fphy.2021.795279

A Briefing Survey on Advances of Coupled Networks With Various Patterns

Gaogao Dong[1]*, *Dongli Duan*[2]* and *Yongxiang Xia*[3]*

[1]School of Mathematical Science, Jiangsu University, Zhenjiang, China, [2]School of Information and Control Engineering, Xi'an University of Architecture and Technology, Xi'an, China, [3]School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China

In real-world scenarios, networks do not exist in isolation but coupled together in different ways, including dependent, multi-support, and inter-connected patterns. And, when a coupled network suffers from structural instability or dynamic perturbations, the system with different coupling patterns shows rich phase transition behaviors. In this review, we present coupled network models with different coupling patterns developed from real scenarios in recent years for studying the system robustness. For the coupled networks with different coupling patterns, based on the network percolation theory, this paper mainly describes the influence of coupling patterns on network robustness. Moreover, for different coupling patterns, we here show readers the research background, research context, and the latest research results and applications. Furthermore, different approaches to improve system robustness with various coupling patterns and future possible research directions for coupled networks are explained and considered.

Keywords: complex network, robustness, resilience, coupled network, coupling pattern

OPEN ACCESS

Edited by:
Huijia Li,
Central University of Finance and Economics, China

Reviewed by:
Xiaoke Xu,
Dalian Nationalities University, China
Xiaoke Ma,
Xidian University, China

***Correspondence:**
Gaogao Dong
gago999@126.com
Dongli Duan
mineduan@163.com
Yongxiang Xia
xiayx@hdu.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *14 October 2021*
Accepted: *19 November 2021*
Published: *24 December 2021*

Citation:
Dong G, Duan D and Xia Y (2021) A Briefing Survey on Advances of Coupled Networks With Various Patterns. Front. Phys. 9:795279. doi: 10.3389/fphy.2021.795279

1 INTRODUCTION

With the significant improvement of the ability of high-performance computer clusters, the in-depth study of cloud storage and computing, internet of things application, and pervasive mobile internet, the amount of data about people's livelihood is increasing and available [1, 2]. These huge amounts of data show network features of extensive distribution, multi-source heterogeneous, such as social network, communication network, power network, energy network, financial network, transportation network, trade network, ecological network and climate network, etc. [3–10]. And, there exists the complex coupling relationship among these real networks, such as spatial relevance, economic connection, strategic linkage, and coexistence relationship [11, 12]. This makes various network systems form a co-generation unit, coupled network [13–16]. Multi-layer network as an important coupled network describes the relevance of real systems from the perspective of coupling between networks [17]. In a multilayered system, each layer represents a separate network system. These coupling links between different networks (layers) may have different functions to each layer and can change the basic characteristics of the individual network and the robustness of the entire coupling system. Coupled patterns with dependent and interconnected features in the real scenarios can be described as interconnected networks, networks of networks, interdependent networks, and so on.

Interdependent networks mean that failure of dependent nodes between coupled networks will cause cascading failures between the networks. Buldyrev et al. [18] initially developed a theoretical framework to understand the robustness of two interdependent networks. Based on this, Gao et al.

[19] extended two dependent networks to basic coupling dependent networks, Network of Networks (NON), to study the system structural robustness. The coupling structure between networks not only includes basic coupling modes like tree, star, and chain but also has more complex generalized topological structure [20–23]. They found that interdependent networks are more vulnerable than isolated networks. With the decreases in dependent coupling strength between networks, the percolation transition changes from the first order to the second order at the critical coupling strength [24]. And, for star-like partially dependent networks, number of dependent networks has an influence on the robustness of networks, but robustness of a loop-like system is independent of the number of coupled networks [25, 26]. Each node within the network is not only connected to its own network nodes but also has coupled relationship with nodes in other networks, and this allows seemingly harmless interference to spread like ripples through the coupled network, and ultimately lead to catastrophic consequences [17, 27].

In addition to interdependence between networks, there often exists interconnected coupling relationship in the real system. Bagrow et al. showed that interconnected networks exhibit surprising percolation properties like the decoupling of interconnected network due to random failures before the network collapses [28]. And interconnected nodes play a key role in the interconnected networks, and failures of these nodes will have a significant impact on network integrity such as Alzheimer's disease has a destructive effect on the connections between systems [29, 30]. In the case of epidemics with a high transmission rate, vaccination of interconnected nodes is more effective in controlling the spread of diseases than vaccination of high-degree nodes [31]. Otherwise, the density of interconnected links also has a significant impact on the system robustness. For example, the level of mobility between cities has been shown to affect the epidemiological transition at the meta-population level [32].

The research on dynamic networks has also attracted more and more attention. For better understanding dynamical characteristic of real networks such as web of sexual contacts, the nervous system, power grid, and metabolism system, Holme et al. proposed the concept of temporal network and defined that the links only exist intermittently to describe the dynamic changes of network structure over time [33]. Considerable research has found that this intermittency has a profound impact on dynamic resilience [34]. Recently, Gao et al. proposed an analytical framework to identify the natural control and state parameters of a multi-dimensional complex system, thereby helping to derive effective one-dimensional dynamical expression and accurately predict system resilience behaviors [35]. Furthermore, Duan et al. found that dynamical coupled network can accelerate the cascading process [36].

This makes us ask the following questions: Is the network system with different coupling patterns safe and stable? How do we prevent system failure? System structural robustness and dynamical resilience play a crucial role in reducing risk and mitigating damage [37–39]. The network structural robustness relies on their network connectivity and can be defined that the ability to retain their connectivity when a portion of their nodes or edges are removed. And, system dynamical resilience characterizes the ability of a system to adjust its activity to maintain its basic functionality in the face of internal disturbances or external environmental changes. In this review, we will focus on recent studies in robustness of coupled network with different coupling patterns to learn more about the subject for more readers.

2 ONE-TO-ONE DEPENDENCY COUPLED PATTERN

Based on dependency relationship between a power network and an Internet network were implicated in an electrical blackout that occurred in Italy, Buldyrev et al. proposed a fully interdependent network model, in which the coupling pattern means one-to-one interdependence of nodes within two networks [18]. When a node in the network is under attack or disabled, the dependent node within the other network will also fail, and cascading failure occurs in the network system. They studied the percolation behaviors in this system under random attack, which triggered a surge of coupled network robustness. Their findings highlighted that the giant component of the system shows a first-order abrupt transition phenomenon with the increase of attack strength that is different from continuous second-order phenomenon of single network. And the results also implied that the broader degree distribution makes the system more vulnerable by using the percolation theory. Since not all nodes in the network are dependent on each other in the real scenario, Parshani et al. presented a partial dependent network model, that is, only partial nodes are interdependent between two networks, as shown in **Figure 1A** [24]. Based on the same failure mechanism with a fully dependent network model, they found the phase transition behavior of network changes from a first-order phase transition to a second-order phase transition with the decrease of coupling strength q between two networks.

Some important infrastructures in the real network have high connection strength and are often considered as attack targets in the network system. Huang and Dong et al. studied the robustness of fully and partial interdependent networks under targeted attacks based on nodes degree [40, 41]. The results show that it is difficult to maintain the robustness of interdependent network by protecting high degree nodes. Xia et al. studied the robustness based on the dependencies in real power and communication networks and revealed the maximum expected payoff for an attacker is affected by the coupling pattern [42, 43].

In fact, more than two networks dependent on each other depend on each other to form a real system. This makes multiple interdependent network systems attract more attention. Furthermore, Gao et al. generalized two dependent networks to n networks (NON) with one-to-one dependency coupling pattern, including some coupled structures like tree, star, and loop which are shown in **Figure 1B–D** [25]. By developing mathematical frameworks, they numerically and analytically studied the robustness of the system. And, Duan et al. studied the robustness of dependent network by considering dynamical

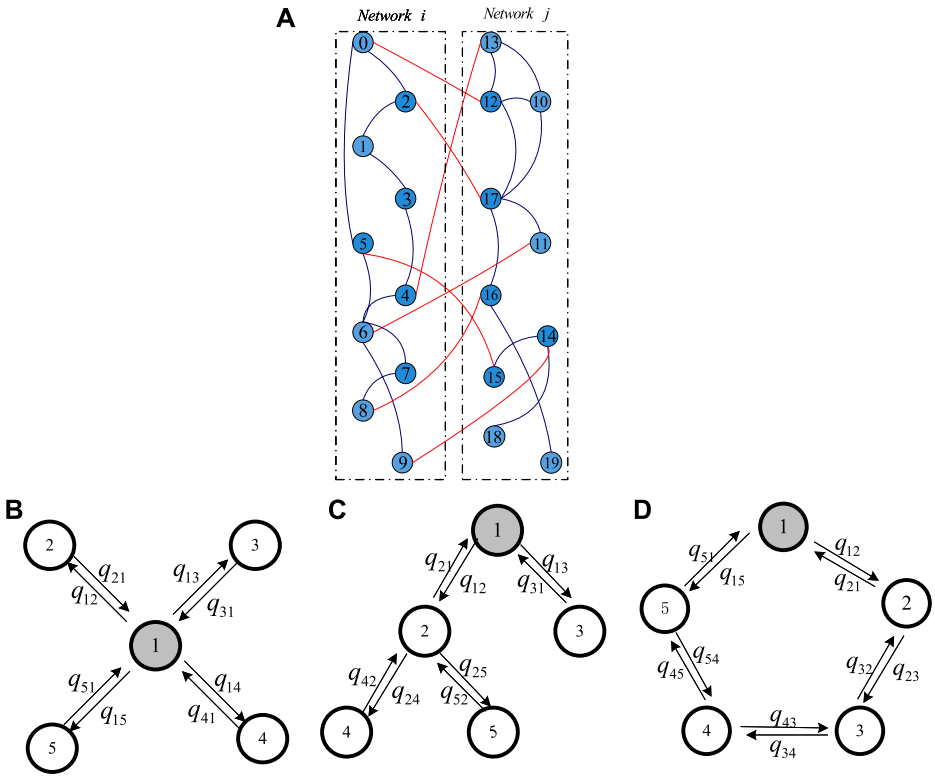


FIGURE 1 | (A) Schematic illustration of partial one-to-one dependency relationship, where only faction $q_{ij} = q_{ji} = \frac{7}{10}$ of nodes dependent on each other between sub-networks *i* and *j*, and red and black links denote inter-dependency and intra-connection links respectively. **(B–D)** Taking five sub-networks as an example, schematic illustration of Network of Networks (NON) with basic dependent structures, star **(B)**, tree **(C),** and loop **(D)**. And a q_{ij} $(i, j = 1, \ldots, 5)$ fraction of nodes in network *i* dependent on nodes within network *j*.

behaviors of nodes within networks triggered by marginal perturbations [36]. They proposed a more generalized framework based on the dynamics of dependent networks and studied the phase transition conditions of dependent networks under various failure mechanisms. They found the analytical expressions for the critical conditions of the first and second phase transitions, and the first phase transition occurred in the weakly dependent network. About directed dependency links, Liu et al. developed a framework to study the system robustness by comparing undirected dependency links. They also found that effect of in-degree and out-degree correlations within the system [44, 45]. Further studies on the impact of different attacks on the one-to-one dependent networks, such as localized attacks [46, 47], overload failures [48], and k-core failure mechanisms [49], have also yielded meaningful results. And different topologies within the network such as group [50], similarity [51, 52], correlation [53], and clustering [54–56] have significant implications for real systems.

For this coupling pattern, one-to-one dependency links is the primary factor leading to network cascading failure. These results generally revealed when connection density within networks is strengthened, and the proportion of dependent nodes within the network is reduced, it can resist attacks to a large extent and reduce the scale of cascading failure. Moreover, unlike the phase transition behavior of a single network, the phase transition behavior exhibited in the system is the first-order jump behavior. This mutation-like behavior further expands the vulnerability of network system and makes it less easy to protect. And these results also gave us on how to design more robust and resilient real networked systems.

3 COUPLED PATTERN WITH MULTIPLE-SUPPORT RELATIONSHIP

The studies of the above dependent networks are restricted by the condition that a functional node in a network depends on one and only one node in the other networks. However, in the real networks, the dependent relationship is often multiple support, as shown in **Figure 2** from Ref. [57]. For example, multiple directed-support links exist between power stations and communication base stations in power and communication networks. Shao and Dong et al. proposed a coupled network model with multiple support-dependency relationships [58, 59]. And for this case, functional nodes have at least one functional support link from other networks and belong to the giant component during the cascading failure process. Then they also provided the analytical expressions on remaining size of the giant component and critical threshold, where the size of the giant component approaches zero. And for the different coupling

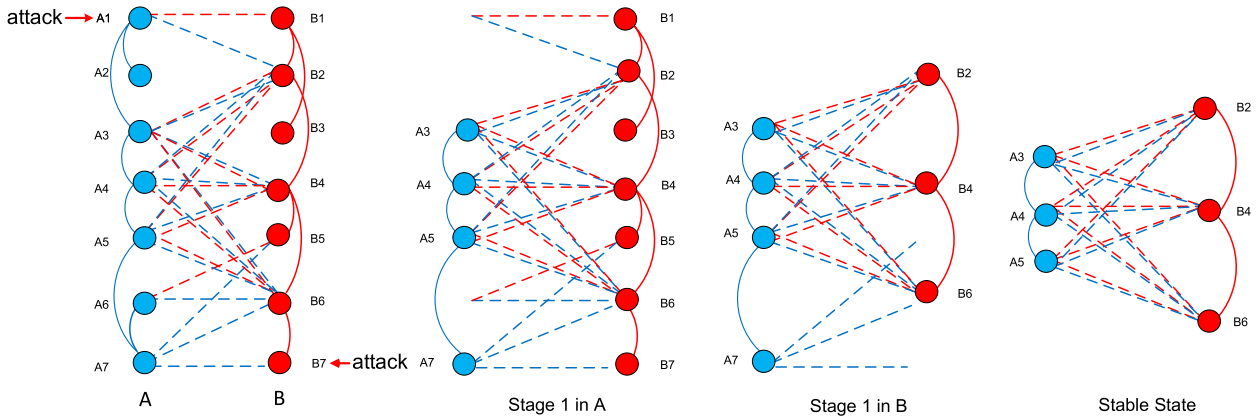


FIGURE 2 | Schematic illustration of cascading failure of two networks with multiple support relationship [57]. The curve links denote intra connectivity links within networks *A* and *B*, and red (blue) dash links are multiple support links from network *A* (*B*) to *B* (*A*). Here we assume that the functional nodes not only belong to the giant component within own network but also have at least *M* support links from other network. After suffering initial attacks, the system undergoes different stages of cascading failures and reaches a steady stable state. During the cascading failure, the functional nodes belonging to the giant component only have *M* support links is the case of the Ref. [60], and $M = 1$ is the similar to the Ref. [58].

structures, star, tree, and loop, Dong et al. developed a framework and extended the case of two networks to n networks with multiple support-dependence relationship [23]. And the findings implied that as connectivity density within network increases, the first-order transition region becomes smaller and the second-order transition region becomes larger. Recently, Zhou et al. proposed a two-layer coupled network model with multiple support-relationship and assumed that functional nodes belonging to giant component within own network have only dependent m support-link that can be survived during a cascading failure process [60]. They also studied the influence on intra-layer and inter-layer degree correlation on network robustness behaviors. The results suggest that such correlations have a significant effect on continuous phase transitions and a small effect on discontinuous phase transitions. Very recently, Dong et al. developed a theoretical framework to study the structural robustness of the coupled network with multiple effective dependency links [57]. It is defined that a functional node requires at least M support-links from the other network to function. In the model, the authors presented exact analytical expressions for the process of cascading failures, the fraction of functional nodes in the stable state, and provided a calculation method of the critical threshold. The results indicated that the system will undergo an abrupt phase transition behavior after initial failure.

Different from the one-to-one dependent network model, the multiple dependent network model describes more realistic dependency relationship in the real system. It can be observed in the real systems, such as communication and grid systems multiple-support each other [18]; social networks (e.g., Twitter) are multiple coupled because they share the same participants [61], and multi-modal transport networks are composed of different traffic systems (e.g., buses, subways) sharing the same location [62]. Similar to one-to-one interdependent network, above studies found that the system occurs a first order phase transition by defining failure mechanisms. And, the system needs more internal connection density to avoid collapse when it requires more effective support-links. These studies revealed the robustness of multiple effective dependent networks, which can help to better understand the cascading failure propagation mechanism of the real system.

4 INTERCONNECTED NETWORK

From the above analysis, one can observe that the occurrence of cascading failures largely relies on dependency relationship between networks, such as blackouts in power grids, financial crisis, etc. Since the existence of dependency attributes, small perturbations in one network are amplified throughout the dependent network system. However, the natural networks (systems) are often coupled together in the way of interconnected networks like brain and cellular networks are comparatively stable and do not crash [63]. In this kind of coupled network, the interaction between one network and another leads to the necessary expansion of the complex network paradigm, including different types of networks and different types of interactions between them. Unlike the dependency links, the links within and between interacting networks have the same attributes that underpin inter-network connectivity and maintain nodes functionality of the network system [64].

Leicht et al. developed an analytical framework from generating functions and studied the robustness of interconnected networks assuming the similar connectivity links exist within and between networks [13].

They found that when considering the interaction with other networks, the threshold to measure network connectivity becomes very small and the system becomes more robust. Furthermore, Dong et al. proposed a partial interacting network model, that means only part of nodes are interconnected with other nodes in the network and all sub-

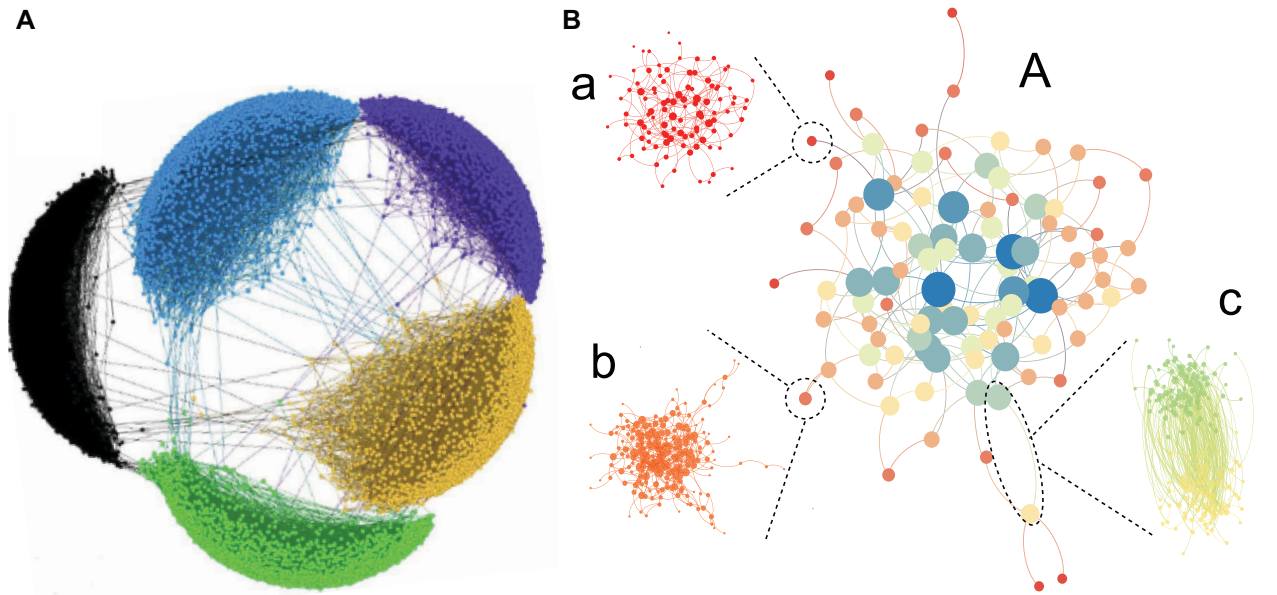


FIGURE 3 | Schematic illustration of interacting network with different topological structures. **(A)** Every sub-network is coupled to all other sub-networks from inter-connected coupling pattern in the Ref. [50]. And, different colors denote different topological structures of sub-networks. **(B)** Each sub-network has connections to other specific sub-networks not all other sub-networks from [26]. Network *A* follows a power-law degree distribution. Sub-networks *a* and *b* within network *A* follow Poisson sub-degree distribution. The links in network *A* follow the Poisson inter-degree distribution, as shown in sub-networks *c*.

networks coupled together in this way, as shown in **Figure 3A** from [65]. They found that increasing the interlinks and interconnected nodes can significantly increase the robustness of the system. Additionally, the continuous phase transition that occurs in a single network disappears, the divergence of the continuous phase transition response function is eliminated, and the system becomes more stable. And, for this kind of network model, the results imply that both analytically and numerically that influence of interlinks on the percolation phase transition is similar to an external field in a ferromagnetic-paramagnetic spin system. By defining the critical exponents δ and γ, these scaling indexes govern the external field and these exponents are consistent with Widom's identity [65, 66]. Moreover, in the real-world scenarios, tons of sub-networks interconnect with others to form a more generalized network, modular interacting network system, and any pair of sub-networks is randomly selected and coupled each other, as shown in **Figure 3B** from [26]. Furthermore, the results implied that there exists an optimal coupling structure, where the system shows the most resilient behavior to withstand failures.

For this case of coupling pattern, network failure behavior was studied by considering functional nodes in the network belong to the giant component of whole coupled networks. As a realistic network model, the interacting network model shows potential applications to epidemic and information spreading, link prediction, and recommendation algorithms. In addition, this interconnected network can also be applied to many different real systems. For example, in the climate network, each isobaric layer of the atmosphere is represented as a complex network, and different isobaric networks are connected [67], the European air transport multi-path network, in which each airline is a sub-network, and public airports can be modeled as coupling nodes [68], the epidemic spreads on interconnected social networks [69]. Due to the same attributes within and between this kind of coupled network, its phase transition behavior often occurs in a second-order phase transition. When the proportion of functional nodes belonging to the largest connected group in the network approaches zero, the critical threshold of the network can be determined. Basically, the research results of this coupled network show that increasing the connection density of network can significantly improve the system robustness.

5 DISCUSSION

In addition to the above coupling patterns, there is a mixed coupling, and dependency links together with inter-connected links between networks. In the model, researchers investigated the case of both interdependent and interconnected links coexistence, where two types of coupled links are randomly connected between two networks. And, they found an interesting phase transition phenomenon, hybrid transition, where the size of giant component both shows abrupt and continuous transition as attacking strength increases [70]. This mixed coupling pattern has not only inter-network interdependence but also includes inter-network connectivity to describe the coupling pattern of real-world scenario [71]. With the development and popularization of the Internet of Things, all things will be interconnected in the near future,

where there exists the physical structure of interdependence, and at the same time there exists the interconnected property.

6 CONCLUSION

Network robustness is becoming increasingly important as we enter age of smart technologies, such as data analysis, SMART Grid, and the Internet of Things (IOT), etc. Complex networks can realistically reflect the coupled relationship in the real scenarios and also permeate different disciplines at the same time, gradually sublimates into an important research field, network science. The research of coupled networks with various patterns is driven by the development of current science and technology; at the same time, it can simulate and guide the system, where we live, from a multi-high-dimensional perspective. In this review, we briefly introduced the advances in robustness of coupled network with various patterns. The phase transition behaviors between networks, how to mitigate failure, and possible future filed of coupled network are explained and considered. In addition, coupled networks have found important application and help us to deal with crises and hidden dangers in the real systems.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

FUNDING

This research is supported by grants from National Natural Science Foundation of China (Grant Nos. 61 973 143, 71 974 080, and 71 690 242), the National Natural Science Foundation of China (Grant No. 11 731 014), the National Key Research and Development Program of China (Grant No. 2020YFA0608601) and Young backbone teachers of Jiangsu Province.

REFERENCES

1. Barabási A-L. Scale-free Networks: a Decade and beyond. *Science* (2009) 325(5939):412–3. doi:10.1126/science.1173299
2. Shekhtman LM, Danziger MM, Havlin S. Recent Advances on Failure and Recovery in Networks of Networks. *Chaos Solitons Fractals* (2016) 90:28–36. doi:10.1016/j.chaos.2016.02.002
3. Barabási A-L, Albert R. Emergence of Scaling in Random Networks. *Science* (1999) 286(5439):509–12.
4. Caldarelli G. *Scale-free Networks: Complex Webs in Nature and Technology*. Oxford, United Kingdom: Oxford University Press (2007).
5. Girvan M, Newman MEJ. Community Structure in Social and Biological Networks. *Proc Natl Acad Sci* (2002) 99(12):7821–6. doi:10.1073/pnas.122653799
6. Dong G, Qing T, Du R, Wang C, Li R, Wang M, et al.Complex Network Approach for the Structural Optimization of Global Crude Oil Trade System. *J Clean Prod* (2020) 251:119366. doi:10.1016/j.jclepro.2019.119366
7. Pastor-Satorras R, Vázquez A, Vespignani A. Dynamical and Correlation Properties of the Internet. *Phys Rev Lett* (2001) 87(25):258701. doi:10.1103/physrevlett.87.258701
8. Dong G, Qing T, Tian L, Du R, Li J. Optimization of Crude Oil Trade Structure: A Complex Network Analysis. *Complexity* (2021) 2021:1–11. doi:10.1155/2021/3480546
9. Zhang X, Shao S, Stanley HE, Havlin S. Dynamic Motifs in Socio-Economic Networks. *EPL* (2014) 108(5):58001. doi:10.1209/0295-5075/108/58001
10. Kossinets G, Watts DJ. Empirical Analysis of an Evolving Social Network. *Science* (2006) 311(5757):88–90. doi:10.1126/science.1116869
11. Boccaletti S, Bianconi G, Criado R, Del Genio CI, Gómez-Gardeñes J, Romance M, et al.The Structure and Dynamics of Multilayer Networks. *Phys Rep* (2014) 544(1):1–122. doi:10.1016/j.physrep.2014.07.001
12. Vespignani A. The Fragility of Interdependency. *Nature* (2010) 464(7291):984–5. doi:10.1038/464984a
13. Leicht E, D'Souza RM. *Percolation on Interacting Networks*. arXiv (2009). arXiv preprint (arXiv:0907.0894).
14. De Domenico M, Solé-Ribalta A, Cozzo E, Kivelä M, Moreno Y, Porter MA, et al.Mathematical Formulation of Multilayer Networks. *Phys Rev X* (2013) 3(4):041022. doi:10.1103/physrevx.3.041022
15. Danziger MM, Bashan A, Berezin Y, Shekhtman LM, Havlin S. An Introduction to Interdependent Networks. In: International Conference on Nonlinear Dynamics of Electronic Systems, July 4–6, 2014 Albena, Bulgaria: Springer (2014). p. 189–202. doi:10.1007/978-3-319-08672-9_24
16. Radicchi F. Percolation in Real Interdependent Networks. *Nat Phys* (2015) 11(7):597–602. doi:10.1038/nphys3374
17. Kivelä M, Arenas A, Barthelemy M, Gleeson JP, Moreno Y, Porter MA. Multilayer Networks. *J Complex Netw* (2014) 2(3):203–71. doi:10.1093/comnet/cnu016
18. Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of Failures in Interdependent Networks. *Nature* (2010) 464(7291):1025–8. doi:10.1038/nature08932
19. Gao J, Buldyrev SV, Stanley HE, Havlin S. Networks Formed from Interdependent Networks. *Nat Phys* (2012) 8(1):40–8. doi:10.1038/nphys2180
20. Gao J, Buldyrev SV, Stanley HE, Xu X, Havlin S. Percolation of a General Network of Networks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2013) 88(6):062816. doi:10.1103/PhysRevE.88.062816
21. Bianconi G, Dorogovtsev SN. Multiple Percolation Transitions in a Configuration Model of a Network of Networks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2014) 89(6):062814. doi:10.1103/PhysRevE.89.062814
22. Dong G, Du R, Tian L, Liu R. Robustness of Network of Networks with Interdependent and Interconnected Links. *Physica A Stat Mech its Appl* (2015) 424:11–8. doi:10.1016/j.physa.2014.12.019
23. Dong G, Gao J, Du R, Tian L, Stanley HE, Havlin S. Robustness of Network of Networks under Targeted Attack. *Phys Rev E Stat Nonlin Soft Matter Phys* (2013) 87(5):052804. doi:10.1103/PhysRevE.87.052804
24. Parshani R, Buldyrev SV, Havlin S. Interdependent Networks: Reducing the Coupling Strength Leads to a Change from a First to Second Order Percolation Transition. *Phys Rev Lett* (2010) 105(4):048701. doi:10.1103/PhysRevLett.105.048701
25. Gao J, Buldyrev SV, Havlin S, Stanley HE. Robustness of a Network of Networks. *Phys Rev Lett* (2011) 107(19):195701. doi:10.1103/physrevlett.107.195701
26. Dong G, Wang F, Shekhtman LM, Danziger MM, Fan J, Du R, et al.Optimal Resilience of Modular Interacting Networks. *Proc Natl Acad Sci* (2021) 118(22):e1922831118. doi:10.1073/pnas.1922831118
27. Stanley HE. *Introduction to Phase Transitions and Critical Phenomena, International Series of Monographs on Physics*. Oxford, United Kingdom: Oxford University Press (1971).
28. Bagrow JP, Lehmann S, Ahn Y-Y. Robustness and Modular Structure in Networks. *Net Sci* (2015) 3(4):509–25. doi:10.1017/nws.2015.21
29. Han J-DJ, Bertin N, Hao T, Goldberg DS, Berriz GF, Zhang LV, et al.Evidence for Dynamically Organized Modularity in the Yeast Protein-Protein Interaction Network. *Nature* (2004) 430(6995):88–93. doi:10.1038/nature02555
30. van Straaten ECW, Stam CJ. Structure Out of Chaos: Functional Brain Network Analysis with Eeg, Meg, and Functional Mri. *Eur Neuropsychopharmacol* (2013) 23(1):7–18. doi:10.1016/j.euroneuro.2012.10.010

31. Stam CJ. Modern Network Science of Neurological Disorders. *Nat Rev Neurosci* (2014) 15(10):683–95. doi:10.1038/nrn3801
32. Colizza V, Vespignani A. Invasion Threshold in Heterogeneous Metapopulation Networks. *Phys Rev Lett* (2007) 99(14):148701. doi:10.1103/physrevlett.99.148701
33. Holme P, Saramäki J. Temporal Networks. *Phys Rep* (2012) 519(3):97–125. doi:10.1016/j.physrep.2012.03.001
34. Almaas E, Kovács B, Vicsek T, Oltvai ZN, Barabási A-L. Global Organization of Metabolic Fluxes in the Bacterium escherichia Coli. *Nature* (2004) 427(6977):839–43. doi:10.1038/nature02289
35. Gao J, Barzel B, Barabási A-L. Universal Resilience Patterns in Complex Networks. *Nature* (2016) 530(7590):307–12. doi:10.1038/nature16948
36. Duan D, Lv C, Si S, Wang Z, Li D, Gao J, et al.Universal Behavior of Cascading Failures in Interdependent Networks. *Proc Natl Acad Sci USA* (2019) 116(45): 22452–7. doi:10.1073/pnas.1904421116
37. Li M, Liu R-R, Lu L, Hu M-B, Xu S, Zhang Y-C. *Percolation on Complex Networks: Theory and Application*. Physics Reports (2021), Vol. 907, 1–68.
38. Liu Y, Sanhedrai H, Dong G, Shekhtman LM, Wang F, Buldyrev SV, et al.Efficient Network Immunization under Limited Knowledge. *Natl Sci Rev* (2021) 8(1):nwaa229. doi:10.1093/nsr/nwaa229
39. Liu X, Li D, Ma M, Szymanski BK, Stanley HE, Gao J. *Network Resilience*. arXiv (2020). arXiv preprint (arXiv:2007.14464).
40. Huang X, Gao J, Buldyrev SV, Havlin S, Stanley HE. Robustness of Interdependent Networks under Targeted Attack. *Phys Rev E Stat Nonlin Soft Matter Phys* (2011) 83(6):065101. doi:10.1103/PhysRevE.83.065101
41. Dong G, Gao J, Tian L, Du R, He Y. Percolation of Partially Interdependent Networks under Targeted Attack. *Phys Rev E Stat Nonlin Soft Matter Phys* (2012) 85(1):016112. doi:10.1103/PhysRevE.85.016112
42. Jiang J, Xia Y, Xu S, Shen H-L, Wu J. An Asymmetric Interdependent Networks Model for Cyber-Physical Systems. *Chaos* (2020) 30(5):053135. doi:10.1063/1.5139254
43. Xu S, Xia Y, Shen H-L. Analysis of Malware-Induced Cyber Attacks in Cyber-Physical Power Systems. *IEEE Trans Circuits Syst* (2020) 67(12):3482–6. doi:10.1109/tcsii.2020.2999875
44. Liu X, Stanley HE, Gao J. Breakdown of Interdependent Directed Networks. *Proc Natl Acad Sci USA* (2016) 113(5):1138–43. doi:10.1073/pnas.1523412113
45. Liu X, Pan L, Stanley HE, Gao J. Multiple Phase Transitions in Networks of Directed Networks. *Phys Rev E* (2019) 99(1):012312. doi:10.1103/PhysRevE.99.012312
46. Berezin Y, Bashan A, Danziger MM, Li D, Havlin S. Localized Attacks on Spatially Embedded Networks with Dependencies. *Sci Rep* (2015) 5(1):8934–5. doi:10.1038/srep08934
47. Yuan X, Shao S, Stanley HE, Havlin S. How Breadth of Degree Distribution Influences Network Robustness: Comparing Localized and Random Attacks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2015) 92(3):032122. doi:10.1103/PhysRevE.92.032122
48. Wang F, Tian L, Du R, Dong G. The Robustness of Interdependent Weighted Networks. *Physica A: Stat Mech its Appl* (2018) 508:675–80. doi:10.1016/j.physa.2018.05.110
49. Yuan X, Dai Y, Stanley HE, Havlin S. K-Core Percolation on Complex Networks: Comparing Random, Localized, and Targeted Attacks. *Phys Rev E* (2016) 93(6):062302. doi:10.1103/PhysRevE.93.062302
50. Shekhtman LM, Shai S, Havlin S. Resilience of Networks Formed of Interdependent Modular Networks. *New J Phys* (2015) 17(12):123007. doi:10.1088/1367-2630/17/12/123007
51. Parshani R, Rozenblat C, Ietri D, Ducruet C, Havlin S. Inter-similarity between Coupled Networks. *EPL* (2011) 92(6):68002. doi:10.1209/0295-5075/92/68002
52. Hu Y, Zhou D, Zhang R, Han Z, Rozenblat C, Havlin S. Percolation of Interdependent Networks with Intersimilarity. *Phys Rev E Stat Nonlin Soft Matter Phys* (2013) 88(5):052805. doi:10.1103/PhysRevE.88.052805
53. Valdez LD, Macri PA, Stanley HE, Braunstein LA. Triple point in Correlated Interdependent Networks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2013) 88(5):050803. doi:10.1103/PhysRevE.88.050803
54. Dong G, Xiao H, Wang F, Du R, Shao S, Tian L, et al.Localized Attack on Networks with Clustering. *New J Phys* (2019) 21(1):013014. doi:10.1088/1367-2630/aaf773
55. Fan W, Gaogao D, Ruijin D, Lixin T. Robustness of Multiple Interdependent Networks under Shell Attack. In: 2017 36th Chinese Control Conference (CCC), Dalian, China, July 26–28, 2017. IEEE (2017). p. 1447–50. doi:10.23919/chicc.2017.8027554
56. Dong G, Du R, Hao H, Tian L. Modified Localized Attack on Complex Network. *EPL* (2016) 113(2):28002. doi:10.1209/0295-5075/113/28002
57. Dong G, Yao Q, Wang F, Du R, Vilela ALM, Eugene Stanley H. Percolation on Coupled Networks with Multiple Effective Dependency Links. *Chaos* (2021) 31(3):033152. doi:10.1063/5.0046564
58. Shao J, Buldyrev SV, Havlin S, Stanley HE. Cascade of Failures in Coupled Network Systems with Multiple Support-Dependence Relations. *Phys Rev E Stat Nonlin Soft Matter Phys* (2011) 83(3):036116. doi:10.1103/PhysRevE.83.036116
59. Dong G, Tian L, Du R, Fu M, Stanley HE. Analysis of Percolation Behaviors of Clustered Networks with Partial Support-Dependence Relations. *Physica A: Stat Mech its Appl* (2014) 394:370–8. doi:10.1016/j.physa.2013.09.055
60. Zhang H, Zhou J, Zou Y, Tang M, Xiao G, Stanley HE. Asymmetric Interdependent Networks with Multiple-Dependence Relation. *Phys Rev E* (2020) 101(2):022314. doi:10.1103/PhysRevE.101.022314
61. Szell M, Lambiotte R, Thurner S. Multirelational Organization of Large-Scale Social Networks in an Online World. *Proc Natl Acad Sci* (2010) 107(31): 13636–41. doi:10.1073/pnas.1004008107
62. De Domenico M, Sole-Ribalta A, Gomez S, Arenas A. Navigability of Interconnected Networks under Random Failures. *Proc Natl Acad Sci* (2014) 111(23):8351–6. doi:10.1073/pnas.1318469111
63. Reis SDS, Hu Y, Babino A, Andrade Jr JS, Jr, Canals S, Sigman M, et al.Avoiding Catastrophic Failure in Correlated Networks of Networks. *Nat Phys* (2014) 10(10):762–7. doi:10.1038/nphys3081
64. Goswami B, Shekatkar SM, Rheinwalt A, Ambika G, Kurths J. A Random Interacting Network Model for Complex Networks. *Sci Rep* (2015) 5(1): 18183–10. doi:10.1038/srep18183
65. Dong G, Fan J, Shekhtman LM, Shai S, Du R, Tian L, et al.Resilience of Networks with Community Structure Behaves as if under an External Field. *Proc Natl Acad Sci USA* (2018) 115(27):6911–5. doi:10.1073/pnas.1801588115
66. Fan J, Dong G, Shekhtman LM, Zhou D, Meng J, Chen X, et al.Structural Resilience of Spatial Networks with Inter-links Behaving as an External Field. *New J Phys* (2018) 20(9):093003. doi:10.1088/1367-2630/aadceb
67. Donges JF, Schultz HCH, Marwan N, Zou Y, Kurths J. Investigating the Topology of Interacting Networks. *Eur Phys J B* (2011) 84(4):635–51. doi:10.1140/epjb/e2011-10795-8
68. Cardillo A, Gómez-Gardeñes J, Zanin M, Romance M, Papo D, Del Pozo F, et al.Emergence of Network Features from Multiplexity. *Sci Rep* (2013) 3(1): 1344–6. doi:10.1038/srep01344
69. Dickison M, Havlin S, Stanley HE. Epidemics on Interconnected Networks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2012) 85(6):066109. doi:10.1103/PhysRevE.85.066109
70. Hu Y, Ksherim B, Cohen R, Havlin S. Percolation in Interdependent and Interconnected Networks: Abrupt Change from Second- to First-Order Transitions. *Phys Rev E Stat Nonlin Soft Matter Phys* (2011) 84(6):066116. doi:10.1103/PhysRevE.84.066116
71. Dong G, Du R, Tian L, Liu R. Percolation on Interacting Networks with Feedback-Dependency Links. *Chaos* (2015) 25(1):013101. doi:10.1063/1.4905202

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 03 January 2022
doi: 10.3389/fphy.2021.790218

Study on Power Grid Partition and Attack Strategies Based on Complex Networks

Yanli Zou and Haoqian Li*

School of Electronic Engineering, Guangxi Normal University, Guilin, China

Based on the community discovery method in complex network theory, a power grid partition method considering generator nodes and network weightings is proposed. Firstly, the weighted network model of a power system is established, an improved Fast-Newman hierarchical algorithm and a weighted modular Q function index are introduced, and the partitioning algorithm process is practically improved combined with the characteristics of the actual power grid. Then, the partition results of several IEEE test systems with the improved algorithm and with the Fast-Newman algorithm are compared to demonstrate its effectiveness and correctness. Subsequently, on the basis of subnet partition, two kinds of network attack strategies are proposed. One is attacking the maximum degree node of each subnet, and the other is attacking the maximum betweenness node of each subnet. Meanwhile, considering the two traditional intentional attack strategies, that is, attacking the maximum degree nodes or attacking the maximum betweenness nodes of the whole network, the cascading fault survivability of different types of networks under four attack strategies is simulated and analyzed. It was found that the proposed two attack strategies based on subnet partition are better than the two traditional intentional attack strategies.

Keywords: complex network, power grid, subnet partition, attack strategy, cascading failure

OPEN ACCESS

Edited by:
Yongxiang Xia,
Hangzhou Dianzi University, China

Reviewed by:
Yilun Shang,
Northumbria University,
United Kingdom
Zhixi Wu,
Lanzhou University, China
Zhihai Rong,
University of Electronic Science and Technology of China, China

****Correspondence:***
Yanli Zou
zouyanli72@163.com

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *06 October 2021*
Accepted: *23 November 2021*
Published: *03 January 2022*

Citation:
Zou Y and Li H (2022) Study on Power Grid Partition and Attack Strategies Based on Complex Networks. Front. Phys. 9:790218. doi: 10.3389/fphy.2021.790218

1 INTRODUCTION

With the construction of ultra-high voltage grids, smart grids, and clean energy-based energy Internet, the gradual interconnection of large grids has taken shape and continues to develop and improve on this basis. At the same time, as the scale of a power system expands, the reliability analysis and calculation of the power system becomes more and more complex and difficult [1, 2]. In recent years, researchers have tried to use the complex network theory to model and analyze the power grid and made good progress [3, 4]. One of the most important properties of complex networks is community structure, which refers to the close connection of nodes within a community and the sparse connection among the communities [4]. The application of this property can provide reference for power grid planning [5, 6].

In order to ensure the safe and stable operation and management of regional power grids, it is very important to carry out network planning in a reasonable and feasible way. In order to realize the online monitoring of grid operation status and fast dispatch of decision-making, power workers generally divide a grid into several sub-regions and manage each sub-region separately, which effectively improves the processing speed and reduces the calculation amount [7]. Analysis of power grid status and formulation of reasonable dispatching strategies are crucial to the management of a

power grid. Usually, a network is divided based on the working experience of the power workers or the administrative area where the nodes are located [8], which obviously does not accurately reflect the state correlation between the components of the grid and cannot adapt to the changing operational state of the grid. The literature [9] proposed the concept of modularity, then modularity became the evaluation standard of community division, and the optimization of modular Q-function became the mainstream of research [10–14]. In [11], modularity Q was used as an index to evaluate the partition results, but it could not reflect the electrical and physical characteristics of a power grid, so it could not evaluate the partition results of power grids well. The literature [12] put forward the concept of power supply modularity combined with power supply correlation strength and improved the Fast-Newman algorithm to automatically identify the community structure of a power grid. In [13], two different types of genetic algorithms were improved and analyzed to solve the problem of community detection in a power system. The results show that genetic algorithm is a fast and effective method to deal with community detection in a large-scale power grid. The literature [15] proposed a new community division method based on resistance distance and similarity, where the distance function between nodes was defined by similarity, and the distance between communities was calculated by the distance between nodes. A power grid was divided into several communities according to whether the nearest neighbor nodes were in the same community.

At present, most of the community detection methods focus on the unweighted networks whose edge denotes whether there is a connection between nodes, regardless of the strength of the connection. However, in the real world, a real network is always complex, and the interaction strength between nodes is different. The unweighted network is not enough to reflect the relationship of objects in real life [16], so the study on weighted networks has a practical significance. The literature [17] overcame the resolution limitation of the traditional community detection method based on modularization by adding a weight term in the modularization formula for the purpose of detecting community which is small enough compared with the whole network. In [18], four weighted network models were established by using power flow and line impedance as the weights of edges, respectively. Then, the examples were simulated with four different models to verify the role of community structure in power grids. However, it was not verified and analyzed in combination with the actual application scenario of the power grid partition. The literature [19] proposed the index of node similarity, which was used to assign nodes with the greatest similarity to the same community. However, the community detection method of the model is mainly based on the pure topological structure of an undirected and unweighted network, without considering the function of a community. Therefore, it cannot fully reflect the electrical characteristics of a power grid.

According to the management of a power grid, each community should at least contain one generator node to ensure the supply of power. Otherwise, it will not work normally after isolation. In order to ensure the normal work of each subnet after power grid partition, this paper proposes an improved Fast-Newman algorithm based on the Fast-Newman algorithm. This improved algorithm considers generators and the weight of a network, overcoming the shortcomings of traditional partition methods which only focus on topology or only focus on electrical characteristics. Furthermore, it was noticed that previous studies on network attack strategies mainly applied random attack or deliberate attack to attack the node with the largest degree value or the node with the largest betweenness in a network. These attack strategies may not make full use of the network structure information, look too simple, and lack effective data mining in the early stage [20–22].Therefore, on the basis of subnet partition, this paper proposes a new network attack strategy. The cascading failure invulnerability of different types of networks under several attack strategies is simulated and compared with each other. It was found that the attack effect of our attack strategy is better than that of traditional attack strategies.

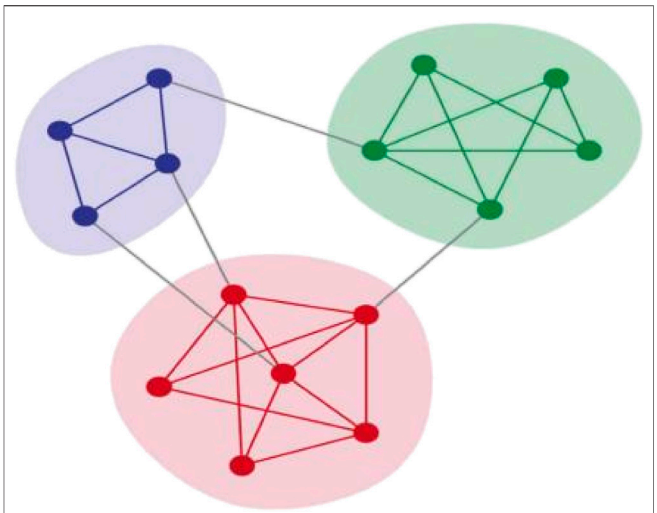


FIGURE 1 | Diagram of community structure.

2 BASIC CONCEPTS

2.1 Community Structure

In nature and society, things with similar characteristics are often more closely related to each other—for example, people in a tribe have more frequent connections than those who are not members of the tribe. A closely connected community means that information or rumors spread faster among them than that in a sparsely connected community, people with the same hobbies are more likely to become friends, and so on. If things and their relationships are represented as a network, then the regions (node sets) whose nodes are closely connected in the network are called communities. If there is a community in a network, it is said to have a community structure. Community partition is equivalent to grouping nodes in a network. Community structure is very common in real networks. It is important to find the basic community structure in a network, for a single community

behaves like a node of the network, which is beneficial to network study. On the one hand, identifying these substructures in a network can provide insights into how network functions and topologies affect each other. On the other hand, communities usually have attributes that are completely different from the average attributes of the network. By only focusing on the average properties, one will usually miss many important and interesting functions within the network. Generally speaking, the nodes in a community are densely connected, while connections among communities are relatively sparse. Detecting communities in a network can help us find the objects with the same function in the system, study the relationship among different communities, infer the missing attributes in the nodes, and make a reasonable prediction of the undiscovered relationship between nodes so as to better understand the underlying structure of the network and the information contained in it. Community discovery has been successfully applied in many areas of real life, such as anti-terrorism detection, behavior prediction, recommendation system, and so on [23, 24]. Community detection in a network is one of the hotspots in modern network science. **Figure 1** is a graph of community structure, where different communities are distinguished by different colors. It can be seen that there are three communities in the network, and the density of connections in each community is relatively higher than that among communities. In other words, community structure is a dense subgraph with distinct boundaries in the network.

2.2 Weighted Power Grid Model

When modeling a power grid, the generators and load buses are usually regarded as nodes, the lines between nodes are regarded as edges, and double circuit or multi-circuit lines are usually combined into one edge. The complex network theory uses node set V, edge set E, and edge weight set W to describe a complex network. For different types of networks and different research purposes, the definition of weight is also diversified, and the weighting method can usually be divided into two categories: similarity weights and dissimilarity weights. The similarity weight indicates the degree of correlation between two nodes; the closer the relationship between nodes, the larger the weight, and vice versa. The dissimilarity weights have an opposite meaning; the smaller the correlation between nodes, the greater the weight. According to the needs of study, when analyzing a power system, we use the above-mentioned two weighting methods to model a power grid. This paper considers three types of models of a power grid and carry out a comparative analysis of detection community. The first one is an unweighted network model, where the weight of each line is uniformly set to 1. The second one is a weighted network model, where the line reactance value X_{ij} is taken as the weight of the edge, which belongs to the dissimilarity weights. The third one is a weighted network model where the line conductance value $Y_{ij} = 1/X_{ij}$ is taken as the weight of the edge, which belongs to similarity weight. The weight setting in the models is shown in **Eq. 1**, where the data comes from Matpower 6.0 [25].

$$\begin{cases} W_{ij} = 1 \\ W_{ij} = X_{ij} \\ W_{ij} = Y_{ij} \end{cases} \tag{1}$$

2.3 Q-Function Model Based on Weighted Network

The literature [26] proposed the concept of modularity to measure the rationality of subnet division of unweighted networks. The literature [18] extended the definition of modularity to weighted networks. The modularity Q function under weighted networks is defined as follows:

$$Q^w = \sum_s \left(e_w^{ss} - \left(a_{ss}^w\right)^2\right) \tag{2}$$

where $e_w^{ss} = 1/2T \sum_{ij} w_{ij}\delta(c_i, s)\delta(c_j, s)$ is the proportion of the sum of the weights of the edges connecting the internal nodes of the community s to the total weights, c_i denotes the subnet where node i locates, $a_{ss}^w = 1/2T \sum_i T_i\delta(c_i, s)$ is the proportion of the sum of the weights of all the nodes in the community s to the total weights, T_i is the weight of node i which equals to the sum of the weights of the edges directly connected to node i, and T is the total weights of all the edges of the network. $Q^w \in [0, 1]$, for random network with equal weights; $Q^w = 0$, values other than 0 indicate deviations from randomness. The larger the proportion of the sum of the weights of the edges connecting the internal nodes of the communities to the total weights, the larger is Q^w.

3 AN IMPROVED ALGORITHM OF POWER GRID PARTITION BASED ON COMMUNITY DISCOVERY

Combined with the physical and topological characteristics of a power grid, the Fast-Newman aggregation algorithm [26] is improved to ensure that each subnet includes at least one generator node after division and to improve the accuracy of subnet division. The steps of the improved algorithm proposed in this paper are as follows:

1) According to the real network architecture, the weighted network model of a power system is established, and various data of nodes and edges in the power grid are obtained from Matpower 6.0. The edge weights of the network are defined according to **Eq. 1**.
2) Introduce the modularity Q function index, improve it according to the edge weight, and define the modularity function Q^w of the power grid with the weighted model according to **Eq. 2**.
3) Initialization—each generator node in the network is divided as a subnet to form an initial subnet structure, without considering the load nodes. The modularity Q_0^w of the network is calculated according to **Eq. 2**.
4) Each node i in the network is incorporated into one of the adjacent subnets and calculates the increment ΔQ^w of the whole network modularity brought by each combination.

TABLE 1 | Modularity Q value of each system under four different methods.

IEEE standard network	Fast-Newman	The weight is 1	The weight is impedance	The weight is admittance
IEEE14	0.4037	0.4013	0.3774	0.4728
IEEE30	0.5434	0.4851	0.5260	0.5588
IEEE39	0.6212	0.6262	0.6584	0.6870
IEEE118	0.7123	0.7281	0.7370	0.8011
IEEE2383	0.8957	0.8937	0.9259	0.9837

Node i is eventually incorporated into the adjacent subnet that makes the value of ΔQ^{w} maximum. $\Delta Q^{w} = Q^{w'} - Q^{w}$, where $Q^{w'}$ is calculated after the node i is joined into an adjacent subnet, and Q^{w} is calculated before the node i is joined.

5) The network obtained in step 4 is compressed, and each subnet is condensed into a node. The sum of the weights of the nodes in the original subnet is assigned to the agglomerated new node, and all the connected edges between the two subnets are agglomerated into one edge. The weight of the agglomerated edges between the subnets is the sum of the weights of all the connected edges in the original subnets, so a new compressed network is obtained.
6) Repeat step 4 until the change of a belonging subnet of any node cannot increase the ΔQ^{w} value, Q^{w} value will not change, and nodes will not be moved. Find out the partition result corresponding to the maximum modularity value Q^{w} in the process of merging, which is the optimal subnet partition result.

The above-mentioned algorithm can be summarized into two stages. Steps 1–4 are to find the optimal solution of Q value based on the existing network, and steps 5–6 are the subnet combination of the division results obtained in the above-mentioned steps to obtain the updated network. After all the steps are completed, it is a round. Then, the algorithm will automatically enter the next round until the Q value no longer changes. Finally, the subnet division corresponding to the Q value is the final subnet division result. The overall time complexity of the algorithm is $O(m(m+N))$, where m is the number of edges and N is the number of nodes. Compared with the original division method, the improved algorithm not only ensures that each subnet after division has a generator to supply power to the loads but also comprehensively considers the topology and electrical characteristics of a power system, making the division more realistic.

4 EXPERIMENTAL ANALYSIS

Based on the Fast-Newman agglomeration algorithm, this paper proposes an improved power grid subnet division method which considers generator nodes and weighted network models. According to the three network weighting methods defined in **Eq. 1**, IEEE14, IEEE30, IEEE39, IEEE118, and IEEE2383 standard test networks are divided using our improved algorithm. The modularity Q values with using the three weighting methods are calculated and compared with the Fast-Newman algorithm.

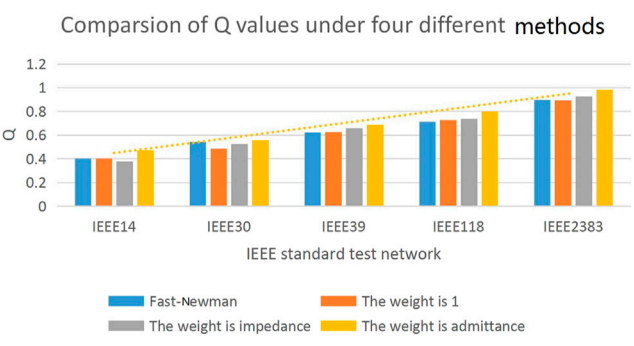


FIGURE 2 | Comparison histogram of the Q value of each network in the four different division methods.

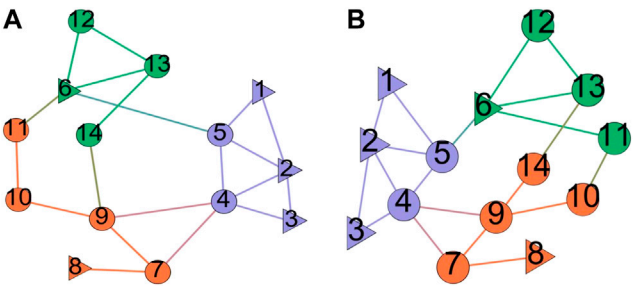


FIGURE 3 | The community structure of IEEE14 network in two division modes. **(A)** Fast-Newman. **(B)** Improved algorithm with admittance weight.

Table 1 shows the data table of the modularity Q value of each system under the four different cases, and **Figure 2** shows the comparison histogram of the Q value of each network.

In the simulation, the weight refers to the weight of a connected edge, and we define the four division methods as follows: (1) Fast-Newman algorithm, (2) unweighted network (with the weight being 1), (3) impedance weight, and (4) admittance weight. The yellow dashed line in **Figure 2** is the trend line of the modularity Q value under the fourth division method. It can be seen that, with the increase of network size, Q values are improved in different degrees under the four division methods, which indicates that this kind of algorithm is suitable for the division of large and complex networks. The larger the Q value is, the better the effect of subnet division is. **Figure 2** shows that the modularity function Q of different networks is maximum under the fourth weighting method. Next, we mainly conduct a

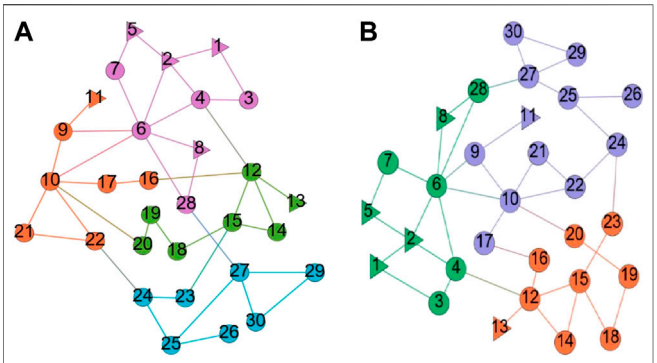


FIGURE 4 | The community structure of IEEE30 network in two division modes. **(A)** Fast-Newman. **(B)** Improved algorithm with admittance weight.

comparative analysis and discussion on the division results of the first and fourth types. The subnet division results are shown in **Figure 3**, **Figure 4**, **and Figure 5**.

Figure 3, **Figure 4**, **and Figure 5** show the community structures of IEEE14, IEEE30, and IEEE39 standard networks in the two division modes. We use different colors to distinguish the divided subnets. The triangle symbol denotes the generator node, and the circular symbol denotes the load node. The IEEE14 standard network is divided into three communities in the two methods, the IEEE30 standard network is divided into four and three communities in the two methods, and the IEEE39 standard network is divided into seven communities in the two methods. It was found that, in the IEEE14 standard network, at least one generator is reserved in each subnet under the two division results, while in the IEEE30 and IEEE39 networks, only the fourth division method ensures that each divided subnet has at least one generator. In the Fast-Newman division method, it appears that there is no generator in one subnet of the IEEE30 and IEEE39 networks (see the blue marker subnet in IEEE 30 and the dark green marker subnet in IEEE 39), which is often defective in an actual power system operation.

When a transmission line in a power grid is damaged or removed, if the usual emergency control measures could not prevent the propagation of the fault, we can take active splitting measures to split the power grid into multiple "islands" according to the result of the pre-division so as to prevent the large-scale spread of the fault. After the splitting of a power grid, the key to the normal operation of each sub-network is the generator. The Fast-Newman aggregation algorithm cannot guarantee that every subnet has at least one generator after dividing the power grid. However, the improved Fast-Newman algorithm can do this work. It takes generators into account in the initialization step of the algorithm and to combine the electrical and topological characteristics of the network so that it can find a more realistic community division of the power grid. Since each subnet has one or more generators, we can take a series of stability measures for the subnets after grid splitting, such as boost or load shedding, to control the propagation of cascading faults to the greatest extent. In addition, considering both the division results and Q-values, we can see that the division result of the admittance model is the most reasonable and the community structure is the most obvious in the four models, which indicates that the community structure of the grids is prevalent and the weight of admittance has a facilitating effect on the community division in the proposed IEEE standard networks.

5 CASCADING FAILURE ATTACK STRATEGY BASED ON SUBNET DIVISION

Network invulnerability refers to the ability of a system to maintain its normal operation when some nodes or links in it are damaged by random failure or deliberate destruction. The stronger the network invulnerability, the better its robustness. The study in the previous two sections shows that most of the actual power grids have a community structure. Using this nature of the power grids to do network partition can facilitate the control and management of the power grids. Furthermore, we can apply the community-based attack strategy to the network invulnerability research, which is rare in the network attack strategy research. How to use network topology and functional information to obtain the best attack effect at least cost remains to be further studied.

In the study of cascading failures in a network, the most used model is "capacity–load" model, and the most commonly used

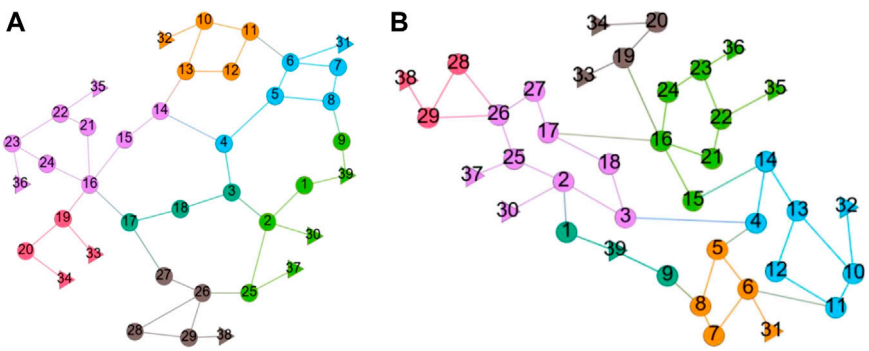


FIGURE 5 | The community structure of IEEE39 network in two division modes. **(A)** Fast-Newman. **(B)** Improved algorithm with admittance weight.

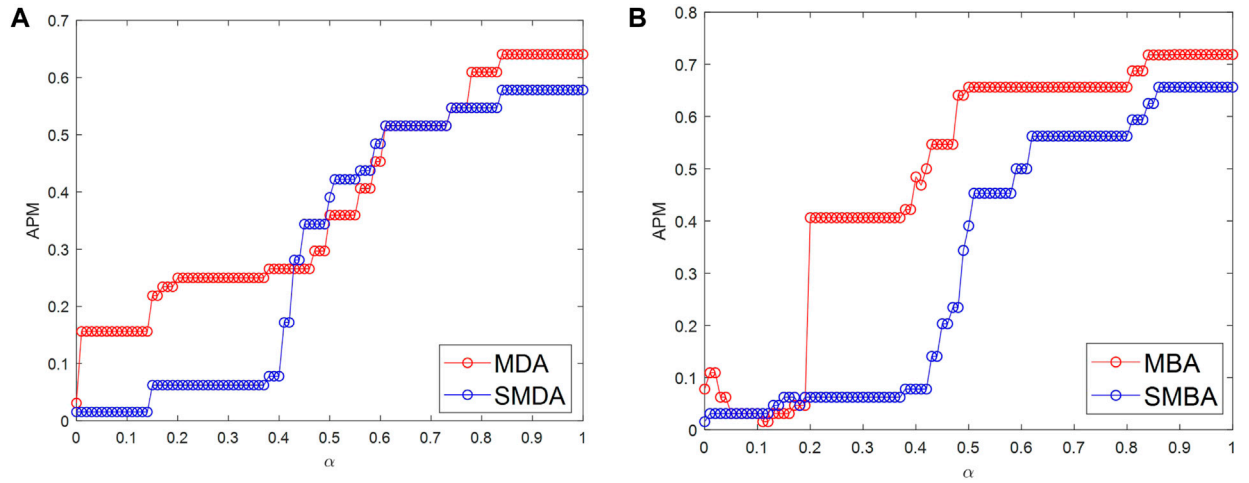


FIGURE 6 | Robustness comparison of IEEE118 network under different attack strategies. **(A)** Attack strategy based on degree. **(B)** Attack strategy based on betweenness.

attack strategies are random attack strategy, which attack random chosen nodes, and deliberate attack strategy, which attack the nodes with the largest degree value or the largest betweenness in a network. However, the model and these attack strategies may not make full use of the network structure and functional information. This paper proposes a new attack strategy with consideration of the community structure of a power grid. The cascading fault of a power grid is simulated with applying the DC power flow model [27], which can better reflect the electrical characteristics of the power grid. With the DC power flow model, the current loading of a transmission line is defined as the current through it, and its capacity is $1 + \alpha$ times of its initial value $I_{ij}(0)$. Power loading of a node is defined as $v_i * I_{oi}$, where I_{oi} is the sum of currents flowing out of node i, and its capacity is $1 + \beta$ times of its initial value. The capacity of each node is set to be large enough to avoid tripping during a cascading failure process. We vary the tolerance ratio of the transmission lines α while assessing the robustness of a power grid.

Based on the previous subnet division, this section will study degree-based and betweenness-based attack strategies, respectively. Each attack strategy includes global attack and community attack—for example, in the fourth division method of **Section 4**, IEEE39 standard network is divided into seven communities. Then, we will attack the nodes with the largest degree or betweenness in each community at the same time. Similarly, sorting the nodes in descending order of degree or betweenness, attack the first seven nodes with the largest degree or the largest betweenness value in the whole network, and observe the network invulnerability effect under the four attack strategies. The methods of attacking maximum degree nodes in the whole network and attacking maximum betweenness nodes in the whole network is called the MDA method and the MBA method, respectively. The method of attacking the maximum degree node of each subnet is called SMDA method, and the method of attacking the maximum betweenness node of each subnet is called SMBA method. In particular, the external connection of the subnet is removed when calculating the maximum degree node and the maximum betweenness node of the subnet. The simulation experiments on IEEE 39, IEEE 118, and IEEE 2383 standard test networks are carried out, respectively. The number of attacked nodes in each network is equal to the number of communities of that network. The average remaining power percentage (APM) defined in [28] is used to quantify the robustness of the power grid, where $\mathrm{APM} = 1/M \sum P_m/P$, P_m is the maintained generation power of the generators after cascade failure, and P is the generation power of the generators before cascading failure. M is the number of times the experiment was repeated. After the cascade failure stops, the larger the APM, the better the robustness of the network. The simulation results are shown in **Figure 6 and Figure 7**.

Using the improved algorithm, IEEE 39, IEEE 118, and IEEE2383 are divided into 7 subnets, 11 subnets, and 86 subnets, respectively, which equal to the attacked nodes in each network. **Figure 6** and **Figure 7** show the network robustness comparison of IEEE39, IEEE118, and IEEE2383 standard networks under different attack strategies.

It can be seen that, between the degree-based attack or the betweenness-based attack, the attack effect of the attack strategy based on the subnet partition method proposed in this paper generally is better than that based on the global degree or betweenness.

Figure 7A is the robustness comparison of the IEEE39 standard network under four attack strategies, and **Figure 7B** is the robustness comparison of the IEEE2383 standard network under the four attack strategies. In the four attack strategies, the network shows a different invulnerability. The scale of cascading failures is the smallest when the nodes with the largest betweenness of the whole network were attacked, and the scale of network cascade failures is the largest when the nodes with the largest betweenness of the communities were attacked. The other two attack effects from strong to weak are attacking the largest

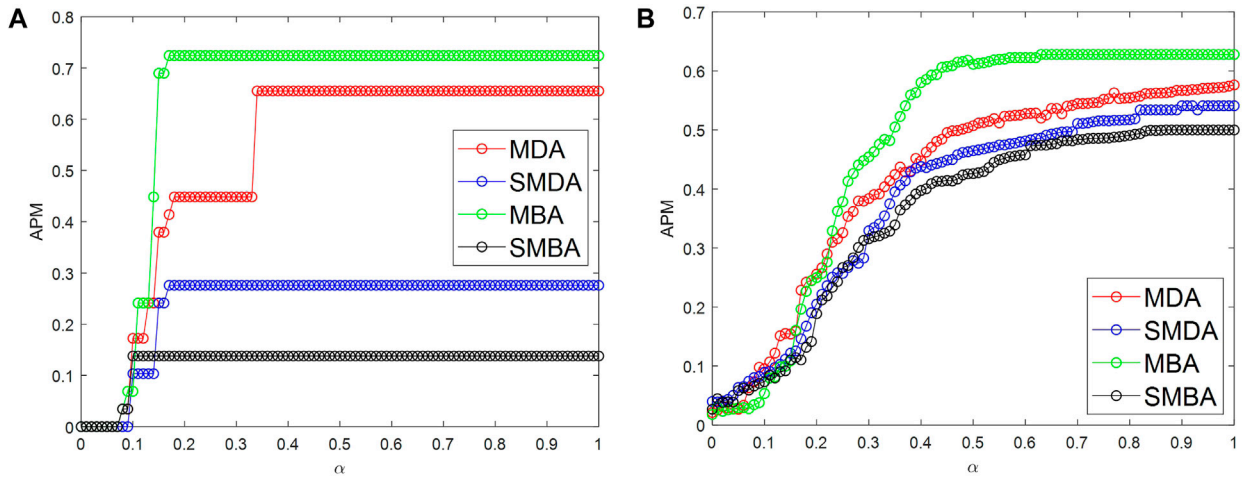


FIGURE 7 | Robustness comparison diagram of the network under four attack strategies. **(A)** IEEE 39. **(B)** IEEE2383.

TABLE 2 | The differences of attacked nodes under four attack strategies.

Network type	f_a (%)	f_b (%)
IEEE39	57	0
IEEE118	54.5	36.3
IEEE2383	45.3	16.3

degree nodes in the communities and attacking the largest degree nodes in the networks. To analyze the differences of attacked nodes under four attack strategies, the n maximum degree nodes in the network (n is the number of communities) are denoted as set N_a, and the n maximum degree nodes in each communities are denoted as set N_b, then $f_a = \mathrm{card}(N_a \cap N_b)/\mathrm{card}(N_a)$ is the ratio of the number of nodes that belong to $N_a \cap N_b$ to the number of nodes N_a. In a similar way, the n largest betweenness nodes in the network are denoted as set N_c, and the n largest betweenness nodes in each communities are denoted as set N_d, $f_b = \mathrm{card}(N_c \cap N_d)/\mathrm{card}(N_c)$ is the ratio of the number of nodes that belong to $N_c \cap N_d$ to the number of nodes N_c. The calculated results of the three networks are shown in **Table 2**.

It can be seen from **Table 2** that the value of f_a is far greater than that of f_b in the three networks, which means that most of the nodes with the largest degree in the community are the nodes with the largest degree of the whole network. However, the nodes with the largest betweenness in the communities usually are not those nodes with the largest betweenness of the whole network. Therefore, the attack effects of MBA and SMBA are the most different.

6 CONCLUSION

Based on community discovery in complex network theory, this paper proposes a power grid partitioning method considering generator nodes and connection weight. Firstly, the weighted network model of a power system is established. Then, the improved Fast-Newman hierarchy algorithm and a weighted modular Q function index are introduced, and the improvement of the partition process is carried out according to the characteristics of the actual power grid. Finally, the improved algorithm is compared with Fast-Newman algorithm to demonstrate its effectiveness and correctness. The sub-network partition method proposed in this paper comprehensively considers the electrical characteristics and topological characteristics of a power system. It ensures that each sub-network has at least one generator node after network partition, which can provide power supply for the loads of the sub-network after the breakdown of the power grid. It has a certain guiding significance for power grid partition.

In addition, several cascading fault attack strategies are studied based on the results of the subnet partition. The cascading fault scales are compared in several IEEE standard test networks for attacking those nodes with the largest degree or the largest betweenness of each subnet and for attacking the same number nodes with the largest degree or the largest betweenness of the whole network. The study shows that the attack strategy with attacking the largest betweenness node of each subnet is the best one. It means that subnet partition has a significant value on the identification of the key nodes of a power grid. Attacking the maximum betweenness node of each subnet has very serious attack consequences.

This paper only considers that each subnet contains generator nodes when partitioning a power grid and does not consider the power balance of power generation and power consumption in each subnet. In further research, the power of generators and loads can be taken into account when partitioning a power grid so that the difference between power generation and power consumption in each subnet is as small as possible. In this way, when a subnet needs to be disconnected from the main power grid for a serious fault, generator tripping and load shedding can be minimized.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. This data can be found here: https://github.com/MATPOWER/matpower.

AUTHOR CONTRIBUTIONS

YZ and HL performed the analysis. HL validated the analysis and drafted the manuscript. YZ reviewed the manuscript. YZ designed the research. All authors have read and approved the content of the manuscript.

FUNDING

We acknowledge support from the National Natural Science Foundation of China (grants 12162005 and 11562003) and the Guangxi Innovation Driven Development Project Guike AA21077015.

SUPPLEMENTARY MATERIAL

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fphy.2021.790218/full#supplementary-material

REFERENCES

1. Jia Y, Xu Z. A Direct Solution to Biobjective Partitioning Problem in Electric Power Networks. *IEEE Trans Power Syst* (2017) 32(3):2481–3. doi:10.1109/TPWRS.2016.2607638
2. Karimipour H, Dinavahi V. Parallel Domain Decomposition Based Distributed State Estimation for Large-Scale Power Systems. *IEEE Trans Ind Applicat* (2015) 52(2):1. doi:10.1109/TIA.2015.2483703
3. Chu C-C, Iu HH-C. Complex Networks Theory for Modern Smart Grid Applications: A Survey. *IEEE J Emerg Sel Top Circuits Syst.* (2017) 7(2):177–91. doi:10.1109/JETCAS.2017.2692243
4. Dao VL, Bothorel C, Lenca P. Community Structure: A Comparative Evaluation of Community Detection Methods. *Net Sci* (2020) 8(1):1–41. doi:10.1017/nws.2019.59
5. Mehrjerdi H, Lefebvre S, Saad M, Asber D. A Decentralized Control of Partitioned Power Networks for Voltage Regulation and Prevention against Disturbance Propagation. *IEEE Trans Power Syst* (2013) 28(2):1461–9. doi:10.1109/TPWRS.2012.2225154
6. Li Z, Lou Y, Liu J, Liu S, Yang F, Fu Y. Optimal Partition of Power Distribution Network Service Areas Based on Improved K-Means Algorithm. In: International Conference on Power System Technology; 2014 Oct 20-22; Chengdu, China. IEEE (2014).
7. Pahwa S, Youssef M, Schumm P, Scoglio C, Schulz N. Optimal Intentional Islanding to Enhance the Robustness of Power Grid Networks. *Physica A: Stat Mech its Appl* (2013) 392(17):3741–54. doi:10.1016/j.physa.2013.03.029
8. Wang T, Li Y, Gu X, Jinghua J. Identification of the Key Transmission Sections Considering Optimization of Geographical Partition Boundary for Power Grids. *Trans China Electrotechnical Soc* (2014) 29(4):220–8. doi:10.19595/j.cnki.1000-6753.tces.2014.04.029
9. Newman MEJ, Girvan M. Finding and Evaluating Community Structure in Networks. *Phys Rev E* (2004) 69(2):026113. doi:10.1103/PhysRevE.69.026113
10. Agarwal G, Kempe D. Modularity-maximizing Graph Communities via Mathematical Programming. *Eur Phys J B* (2008) 66(3):409–18. doi:10.1140/epjb/e2008-00425-1
11. Li Z, Zhang S, Wang R-S, Zhang X-S, Chen L. Quantitative Function for Community Detection. *Phys Rev E* (2008) 77(3):036109. doi:10.1103/PhysRevE.77.036109
12. Wei G. Power Grid Oriented Community and its Detection Method. *Comp Appl Softw* (2021) 38(04):88–94. doi:10.3969/j.Issn.1000-386x.2021.04.015
13. Guerrero M, Montoya FG, Baños R, Alcayde A, Gil C. Community Detection in National-Scale High Voltage Transmission Networks Using Genetic Algorithms. *Adv Eng Inform* (2018) 38:232–41. doi:10.1016/j.aei.2018.07.001
14. Newman MEJ. Finding Community Structure in Networks Using the Eigenvectors of Matrices. *Phys Rev E* (2006) 74:036104. doi:10.1103/PhysRevE.74.036104
15. Lu P, Yu Z, Guo Y. A Novel Algorithm for Community Detection Based on Resistance Distance and Similarity. *Mod Phys Lett B* (2021) 35(09):2150164. doi:10.1142/s0217984921501645
16. Li S, Jiang L, Wu X, Han W, Zhao D, Wang Z. A Weighted Network Community Detection Algorithm Based on Deep Learning. *Appl Maths Comput* (2021) 401(7):126012. doi:10.1016/j.amc.2021.126012
17. Haq NF, Moradi M, Wang ZJ. Community Structure Detection from Networks with Weighted Modularity. *Pattern Recognition Lett* (2019) 122:14–22. doi:10.1016/j.patrec.2019.02.005
18. Pan G, Wang X, Peng X, Wu X-M. Study of Power Grid Partition Identification Method Based on Community Structure Detection. *Power Syst Prot Control* (2013) 41(13):122–7.
19. Chen Z, Xie Z, Zhang Q. Community Detection Based on Local Topological Information and its Application in Power Grid. *Neurocomputing* (2015) 170:384–92. doi:10.1016/j.neucom.2015.04.093
20. Xia Y, Fan J, Hill D. Cascading Failure in Watts-Strogatz Small-World Networks. *Physica A: Stat Mech its Appl* (2010) 389(6):1281–5. doi:10.1016/j.physa.2009.11.037
21. Yang G, Qi X, Liu L. Research on Network Robustness Based on Different Deliberate Attack Methods. *Physica A: Stat Mech its Appl* (2020) 545:123588. doi:10.1016/j.physa.2019.123588
22. Li H, Du J, Peng X, Ding C. Research on Cascading Invulnerability of Community Structure Networks under Intentional-Attack. *J Comp Appl* (2014) 34(4):935–8. doi:10.11772/j.issn.1001-9081.2014.04.0935
23. Pizzuti C. Evolutionary Computation for Community Detection in Networks: A Review. *IEEE Trans Evol Computat* (2018) 22(3):464–83. doi:10.1109/TEVC.2017.2737600
24. Shang Y. Generalized K-Core Percolation in Networks with Community Structure. *SIAM J Appl Math* (2020) 80(3):1272–89. doi:10.1137/19M1290607
25. Zimmerman RD, Murillo-Sanchez CE, Thomas RJ, MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education. *IEEE Trans Power Syst* (2011) 26(1):12–9. doi:10.1109/TPWRS.2010.2051168
26. Newman MEJ. Fast Algorithm for Detecting Community Structure in Networks. *Phys Rev E* (2004) 69(6):066133. doi:10.1103/PhysRevE.69.066133
27. Zhang X, Tse CK. Assessment of Robustness of Power Systems from a Network Perspective. *IEEE J Emerging Selected Top Circuits Syst* (2015) 5(3):456–64. doi:10.1109/JETCAS.2015.2462152
28. Wu J, Zhang X, Ma S, Rong Z, Tse CK. Bifurcation in Transmission Networks under Variation of Link Capacity. *Int J Bifurcation Chaos* (2018) 28(07):1850093. doi:10.1142/S0218127418500931

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article or claim that may be made by its manufacturer is not guaranteed or endorsed by the publisher.

frontiers in Physics

ORIGINAL RESEARCH
published: 18 January 2022
doi: 10.3389/fphy.2021.806259

Spreading to Localized Targets in Signed Social Networks

*Jiaqi Song, Zhidan Feng and Xingqin Qi**

School of Mathematics and Statistics, Shandong University, Weihai, China

Inspired by lots of applications like viral marketing of products and transmitting information in a network, ranking the spreading ability of nodes in the network has been widely studied. At present, the above problem is mostly studied on unsigned networks which only contain positive relationships (e.g., friend or trust) between users. In real-world networks, there usually exist both positive relationships and negative relationships (e.g., foe or distrust) between users. Based on this, we aim to find the influential spreaders in a signed network which meet the requirement of real scene. Moreover, when the spreading only aims to affect a specific group of nodes instead of all nodes, such as promoting cigarette, a new problem called localized targets spreading problem was come up with. Localized targets spreading problem has been studied on unsigned networks, but it is still open for signed networks. Thus, in this paper, we propose a new method, called local influence matrix (LIM) method, which aims to find the seed nodes set with maximum positive influence on a specific group of targets but with minimum influence on the non-target nodes in signed social networks. Simulation results show that our method performs well on real networks.

Keywords: influence diffusion, signed social networks, IC model, centrality, localized targets

Edited by:
Gaogao Dong,
Jiangsu University, China

Reviewed by:
Hai-Feng Zhang,
Anhui University, China
Yinghong Ma,
Shandong Normal University, China

****Correspondence:***
Xingqin Qi
qixingqin@sdu.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *31 October 2021*
Accepted: *29 November 2021*
Published: *18 January 2022*

Citation:
Song J, Feng Z and Qi X (2022) Spreading to Localized Targets in Signed Social Networks. Front. Phys. 9:806259. doi: 10.3389/fphy.2021.806259

1 INTRODUCTION

In recent years, a variety of attention has been paid to investigating the spreading ability of nodes in complex networks. Effectively identifying influential nodes is of great significance in reality, for instance, and helping to design appropriate marketing strategies. There are numerous studies having been done on this issue and a series of methods have been proposed, such as degree centrality (DC) [1], betweenness centrality (BC) [2] and k-shell decomposition (KS) [3] etc. In addition to these famous methods, many researchers proposed other novel methods [4, 5]. Recently Guilbeault and Centola derived a new measure called complex centrality (CC) [6] depending on a "complex" path instead of a "simple path."

In previous research, people often concentrate on finding the most influential nodes for the *entire* network. However, in our daily life, there are some situations where we'd like to find the most influential nodes for *localized targets*, i.e. aiming to infect not all the nodes but only a small number of localized nodes. The problem of localized targets was firstly proposed by Sun et al. [7]. Actually, the target spreading problem has many real applications. For example, in advertising based on online social networks (e.g., Facebook and Twitter), cigarette advertisement should be promoted as much as possible among adults and but should avoid being promoted among teenagers. However, some traditional centrality methods can not meet this requirement. For example, when some information needs to be passed to the target nodes in the yellow circle in **Figure 1**, most degree-related methods are hard to achieve the goal. In **Figure 1**, the network's maximum out-degree node is far away from the target nodes. So if the information is passed from the node with maximum out-degree to the targets, the seed node is very likely to lose its spreading ability during the propagation process. So the

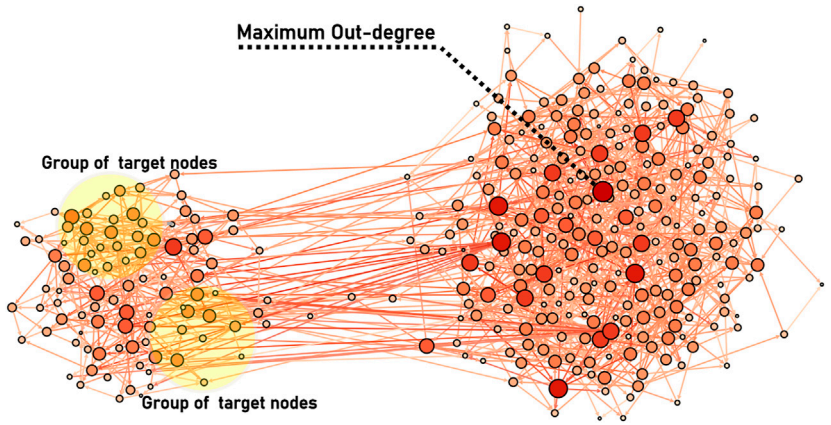


FIGURE 1 | Illustration of the problem of spreading towards localized targets in complex networks. The network is an artificial network (350 nodes and 1,129 links) with two communities. The color (from dark red to white) of the nodes represents their respective degrees. Nodes in the yellow circle are the targets that need to be activated. The maximum out-degree node whose color is darkest is marked.

following problem comes up naturally: how to identify the most influential nodes in a network which can activate the given localized targets as often as possible while activating the non-target nodes as little as possible?

The pioneer method proposed by Sun et al. [7] is suitable for the unsigned networks, and their method only pays attention to the first objective (*i.e.*, activate the given localized targets as often as possible), but ignores the second objective (*i.e.*, avoid activating the non-target nodes). On the other hand, in some online social systems (e.g., Slashdot, Bitcoinalpha), users are allowed to mark positive signs or negative signs on the relationships with others. Compared with unsigned networks, the signed networks describe the real social systems more accurately and reasonably. There are also a few methods of identifying the influential nodes in a signed network. But to our best knowledge, there is still not any study attempting to identify the most influential nodes towards given target nodes in a signed network. In this paper, we thus propose a local influence matrix method (LIM) to solve this problem by computing the local paths from target nodes to other nodes. After applying this method on some generated networks and real networks, we test its efficiency. We also compare it with some traditional methods which are extended simply to deal with this particular case, and verify this new method's better performance.

2 MODELLING SIGNED SOCIAL NETWORKS

In this paper, we model a signed social network as a directed, weighted, and signed graph $G(V, E, P, R)$, where V is the set of nodes that correspond to users in the social network with $|V| = N$. Let E be the set of edges, and the attitude (positive, negative, or neutral) of each edge is stored at the matrix R with $R(u, v) \in \{1, 0, -1\}$. Let P be a non-negative diffusion probability matrix, where $P(u, v)$ shows the diffusion probability from user u to user v. For example, if $P(u, v)$ is equal to 0.2, it means that the probability that user u will successfully deliver message to user v is 0.2.

Here we use the example in **Figure 2** to illustrate the signed social networks. **Figure 2A** shows an example of a signed social network which introduces the relationship between the three users (Jerry, Tuffy, and Tom). **Figure 2B** demonstrates the graph model of the signed social network of **Figure 2A**. Three nodes v, u, and w are corresponding to user Jerry, Tuffy, and Tom respectively. Note that the direction of edges in **Figure 2A** are opposite to those in **Figure 2B**. The reason is as follows. For instance, Jerry likes Tuffy in **Figure 2B**, so he'd like to be influenced by Tuffy, in other words, if Tuffy likes some products, Jerry is easily influenced by Tuffy and likes these products. In **Figure 2**, Jerry likes Tuffy, so $R(u, v) = +1$; Jerry dislikes Tom, so $R(u, v) = -1$; and there is no relationship between Tom and Tuffy, so $R(u, v) = 0$. **Figure 2B** only shows the signs on the edges but not the weights on the edges. In **Figure 2B**, 0.1 and 0.2 represent the weights of two edges. The probability of v being successfully affected by u or w is 0.1 or 0.2.

The probability of information being accepted depends on the matrix P. If $P(v, u)$ is equal to 0.2, it means that u will accept the information from v with the probability of 0.2. And the attitude of u towards information depends on matrix R. If u accepts v's information and $R(v, u)$ is equal to 1, u will support v's information. On the contrary, if $R(v, u)$ is equal to -1, u will oppose v's information. As a result, we define a matrix $A = R^*P$ with its element $A(u, v) = R(u, v) \cdot P(u, v)$, to consider the extent of positive influence or negative influence. For example, in **Figure 2B**, $A(w, v)$ is -0.2.

Matrix P can be generated by three methods, which will be discussed in Experiments Section.

3 THE LOCAL INFLUENCE MATRIX METHOD

Usually the target nodes that need to be infected or activated are localized, which means they are within a certain distance from each other. To identify the most influential nodes in a signed

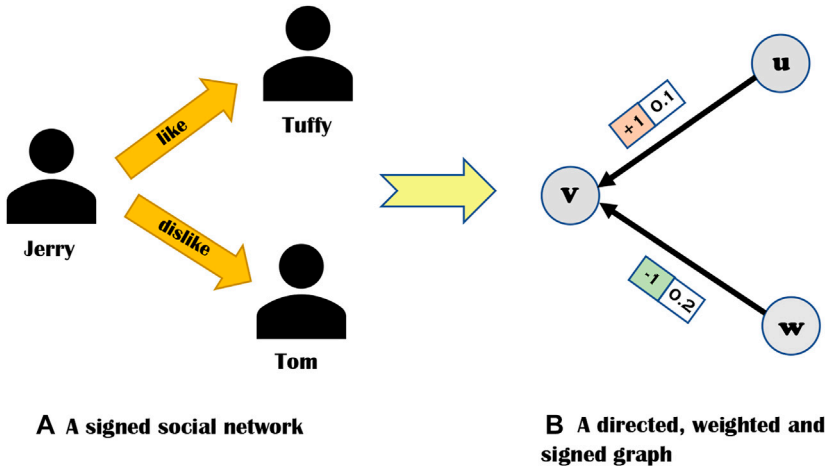


FIGURE 2 | An example of modeling a signed social network. **(A)** A signed social network **(B)** A directed, weighted, and signed graph

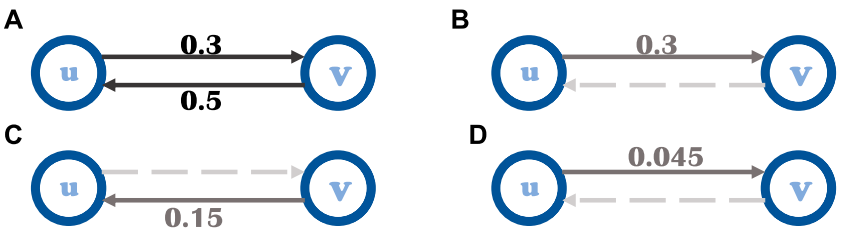


FIGURE 3 | Special situation in spreading process. **(A)** There are two opposite sides between node *u* and *v*. The probability of *u* successfully spreading information to *v* is 0.3. And the probability from *v* to *u* is 0.5. **(B)** The probability from *u* to *v* is 0.3. **(C)** The probability from *u* to *v* to *u* is 0.15. **(D)** The probability of *u* to *v* passing through *u*-*v*-*u*-*v* is 0.045.

network which can *positively activate* the given localized targets as often as possible while activating the non-target nodes as little as possible, we present the following Local Influence Matrix method (abbreviated as LIM). The basic idea is to compute all positive and negative paths within k steps from $V \setminus T$ to the target nodes T, which shows the probability of a node in $V \setminus T$ activating the node in T, and we will use them later to measure the infecting ability of the nodes in $V \setminus T$.

As mentioned above, let A be the $N \times N$ adjacency matrix of the input signed network, where $a_{i,j} \in [-1, 1]$ means the probability that node i infects j with the same (or different) status if $a_{i,j} > 0$ (or $a_{i,j} < 0$). Note that $(A^k)_{i,j}$ means the probability that node i infects j at k steps. The elements on the main diagonal of the matrix A^k represent cycles (which means a node will be activated twice in the same path and is not reasonable), we should exclude them by setting the main diagonal to zero in each step. Let $\bar{A}^k$ be the new matrix, and define

$$A^{k+1} = \bar{A}^k \times A \tag{1}$$

and then set the main diagonal of A^{k+1} to zero again and repeat the above process.

Then the *infected probability matrix* within k steps between any pair of nodes of V can be calculated as:

$$S = \sum_{l=0}^{k} \bar{A}^{l+1}, \tag{2}$$

Note that if $k > 3$, $(A^k)_{i,j}$ is relatively smaller, thus in the following we restrict $k = 3$. **Figure 3** gives a simple example to explain the reason why the matrices' diagonal elements are set to zero. In **Figure 3**, there are two opposite arcs between node u and v whose diffusion probability is 0.3 and 0.5 respectively. One way that u infects v is by the arc (u, v) with a probability of 0.3 in **Figure 3B**. If we do not let the diagonal elements of A^2 become zeros, then the following path $u \to v \to u \to v$ with a probability of 0.045 will be calculated in A^3.

Then we divide the matrix S into the following two matrices S_P and S_N.

$$S_P(u, v) = \begin{cases} S(u, v) & S(u, v) > 0 \\ 0 & S(u, v) \le 0 \end{cases} \tag{3}$$

and

$$S_N(u, v) = \begin{cases} 0 & S(u, v) \ge 0 \\ -S(u, v) & S(u, v) < 0 \end{cases} \tag{4}$$

$S_P(u, v)$ (or $S_N(u, v)$) measures the possibility that node u activates v positively (or negatively) if the original attitude/status

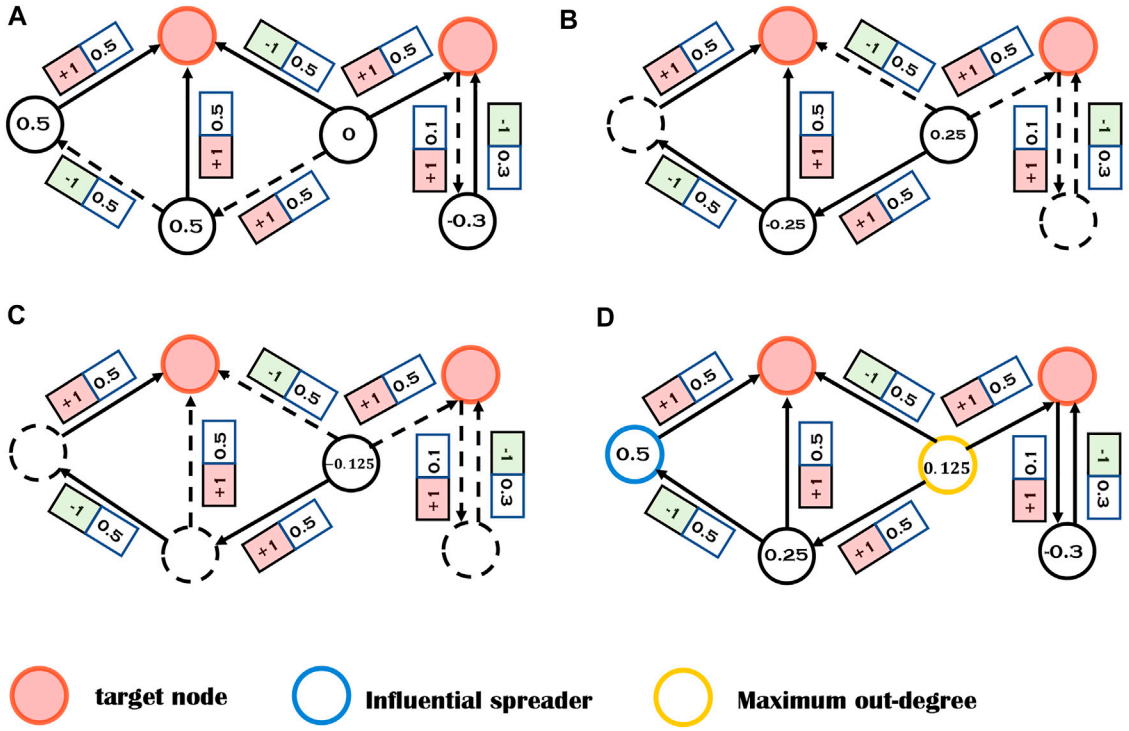


FIGURE 4 | Illustrations of the local influence matrix (LIM) algorithm ($\alpha = 1$, $\beta = 1$, $\gamma = 0$). The red nodes are target nodes and others are non-target nodes. **(A)** The nodes with numbers are directly connected with target nodes. All irrelevant nodes and edges are marked in dashed lines. The numbers on the nodes can be calculated by $A \cdot f$. **(B)** The nodes with numbers can reach target nodes in exactly two steps. All possible paths with length two are considered and the numbers on nodes can be calculated by $\bar{A}^2 \cdot f$. **(C)** The nodes with numbers can reach target nodes in exactly three steps. All possible paths with length three are considered and the numbers on nodes can be calculated by $\bar{A}^3 \cdot f$. **(D)** The numbers on the nodes represent the LIM score when $\alpha = 1$, $\beta = 1$, and $\gamma = 0$. The blue and orange nodes have maximum LIM, out-degree values respectively.

of u is positive. Recall that our problem is to identify the most influential nodes in a signed network which can positively activate the given localized targets as often as possible while activating the non-target nodes as little as possible. At first, we would like to select nodes which could positively activate target nodes as often as possible and negatively activate target nodes as little as possible. Meanwhile, it is better to minimize the impact on other non-target nodes, whether it is positively influenced or negatively influenced. The positive influence from non-target nodes to target nodes can be expressed by $S_P \cdot f$, where f is a $N \times 1$ vector in which the positions corresponding to target nodes are 1, and 0 otherwise. Likewise, $S_N \cdot f$ shows the negative influence from non-target nodes to target nodes, which is also a positive vector. In addition, $S_P \cdot f'$ and $S_N \cdot f'$ respectively represent the positive and negative influence from non-target nodes to other non-target nodes where f' is also a $N \times 1$ vector indicating non-target nodes position. To adjust the preference of these three indicators, α, β and γ are introduced as the weights of these three indicators.

Based on the above requirements, we proposed a formula to measure the influence of nodes from $V \setminus T$ to target set T as follows:

$$S_{LIM} = (\alpha S_P - \beta S_N) \cdot f - \gamma (S_P + S_N) \cdot f', \tag{5}$$

The LIM process is illustrated with a toy network in **Figure 4**, where α, β, and γ are set to be 1, 1, and 0 respectively. One can see that the most highly ranked node by LIM is different from the node with maximum out-degree.

4 EXPERIMENTS

4.1 Experimental Setup

4.1.1 Datasets

To validate the LIM method, we will apply it to two real signed networks: Slashdot [8] and Bitcoinalpha [9, 10].

- Slashdot. This is a signed and directed network in which users can rate each other as a friend or a foe. We use its biggest subgraph with 10,966 users and 44,356 relationships.
- Bitcoinalpha. Bitcoinalpha used here is a directed, signed network with 3,783 nodes and 24,186 links. Original data has weight on each arc, but here we use its underlying graph only and generate the weights by the following three models.

4.1.2 Diffusion Probability Generation

If one unweighted signed network is given, researchers [8, 11, 12] usually use the following three models to generate the influence probabilities on arcs.

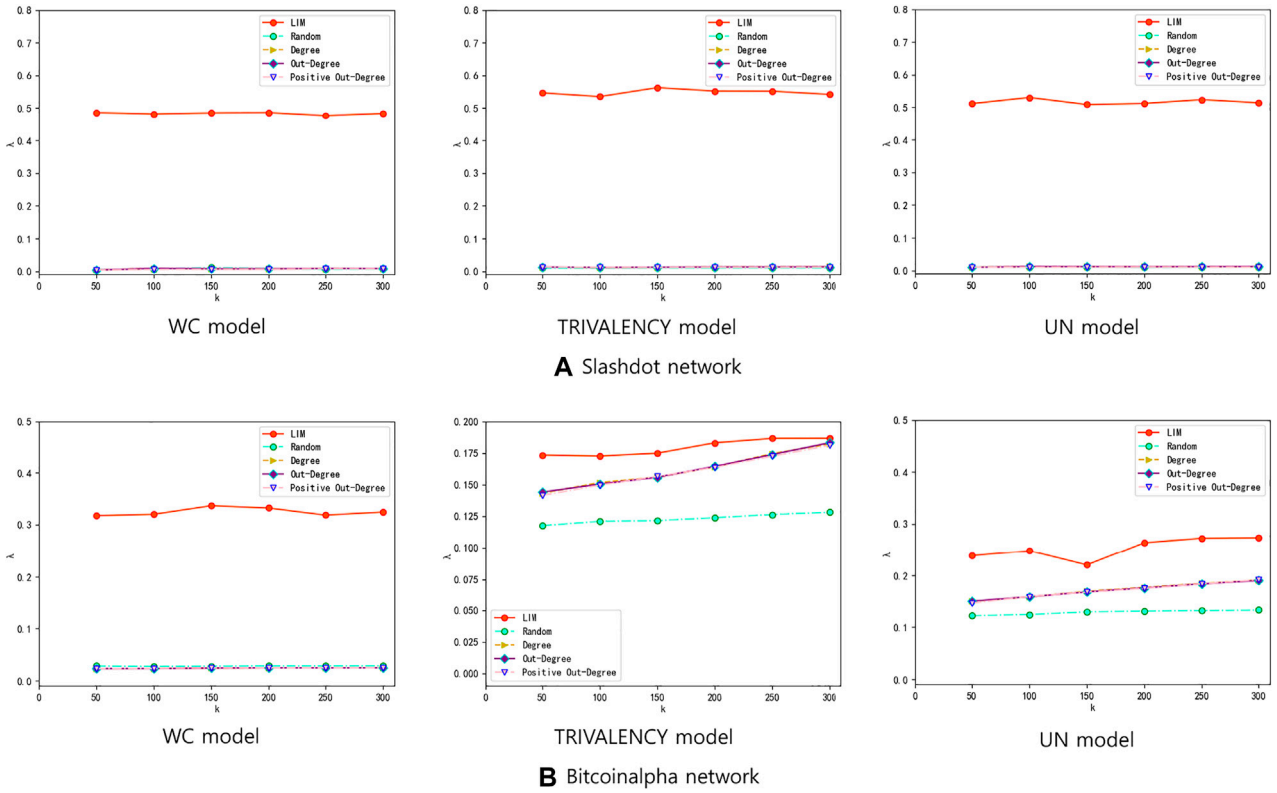


FIGURE 5 | Result Comparisons between LIM method and some degree-based centrality methods when applying on **(A)** Slashdot network **(B)** Bitcoinalpha network. The experiments are conducted on **(A)** Slashdot network **(B)** Bitcoinalpha network. Three diffusion probability methods are considered, i.e. WC model, TRIVALENCY model, and UN model. For UN model, the probability value we set is 0.03. In each experiment, parameter k means that k seeds are selected to activate other nodes, and λ means the proportion of positively activated target nodes among all activated nodes. The targets we set are a center node with small coreness and nodes within two steps from it. **(A)** On the Slashdot network, node 2,921 is the center node. **(B)** On the Bitcoinalpha network, the center node we set in targets is node 7,062. Ranking methods include Degree (yellow triangles), Out-Degree (purple diamonds), Positive Out-Degree (pink triangles), Random (green circles), and LIM (red circle) methods. The results in each figure are obtained by averaging over 2,000 independent realizations.

- Weighted Cascade (WC) model. In this model, $P(u, v)$ for an edge (u, v) is $1/d^{-}(v)$, where $d^{-}(v)$ is the in-degree of v.
- TRIVALENCY model. On each edge (u, v), this model randomly selects a value from 0.1, 0.01, and 0.001 as a diffusion probability.
- Uniformly (UN) model. The diffusion probability of all the edges are assigned the same value. We will test a relatively small value of 0.03 and a relatively large value of 0.5, respectively.

4.1.3 Localized Targets' Selection

Note that a localized target node set T should be given beforehand when testing this new method LIM on a data set. We use the following strategy to generate T. We first randomly pick up a node v with a smaller coreness centrality [3], then add those nodes within two steps from v into the target set. Note that in this paper target nodes are not allowed as seed.

4.1.4 Independent Cascade With Sign Model

The standard Independent Cascade (IC) model [12] used for unsigned networks is extended to the signed case in the following, which is called IC-S Model. Each node v has three states $s(v)$ in IC-S model, including active positive, active negative, and inactive. For a node u, active positive status means that u is active with positive attitude. A node u with inactive status means that u is not active yet.

At time t, each newly activated node u (*i.e.*, the node which is activated at time $t-1$) has only one chance to activate each of its currently inactive neighbors w. If node w is activated by u, its status $s(w)$ is determined by the status of u and the relationship between them, *i. e*, $s(w) = R(u, w) \times s(u)$. If $s(w) > 0$, then the status of w is active positive, and active negative otherwise. If w is not activated successfully by u, w can also be activated by its other neighbors.

4.1.5 Comparison Methods

To show this new method's performance, besides the *random selection method* baseline, we also use the following methods to compare with.

- Degree centrality. The degree of node i can be defined as $k(i) = \sum_{j \in G}(|a_{ij}| + |a_{ji}|)$ where a_{ij} is the entry of matrix A mentioned above.

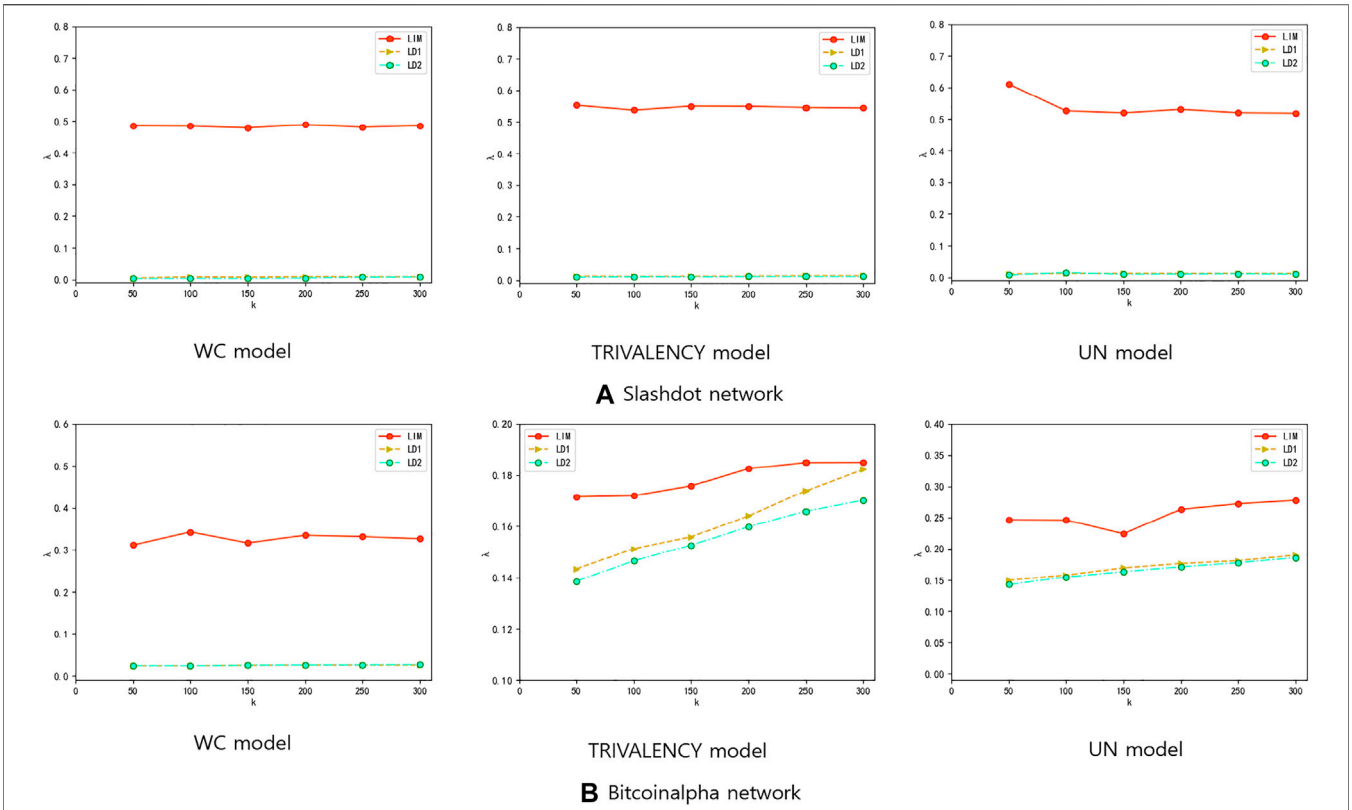


FIGURE 6 | Result Comparisons between LIM and LD1 and LD2 when applying on **(A)** Slashdot data set **(B)** Bitcoinalpha data set. The experiments are conducted on **(A)** Slashdot network **(B)** Bitcoinalpha network. Three diffusion probability methods are considered, i.e., WC model, TRIVALENCY model, and UN model. For the UN model, the probability value we set is 0.03. In each experiment, parameter k means that k seeds are selected to activate other nodes. And λ means the proportion of positively activated target nodes among all activated nodes. Ranking methods include Local Degree 1 (yellow triangles), Local Degree 2 (green circles), and LIM (red circle) methods. The results in each figure are obtained by averaging over 2,000 independent realizations.

- Out-Degree centrality. The out-degree of node i can be defined as $o(i) = \sum_{j \in G} |a_{ij}|$, where a_{ij} is also the entry of matrix A. The out-degree of the node represents the number of the out neighbors of the node, which reflects the direct influence from this node to others.
- Positive Out-Degree centrality. The positive out-degree of the node i is defined as $o^+(i) = \sum_{j \in G} a_{ij}^+$. Here a_{ij}^+ means that edges whose $a_{ij} > 0$. The positive out-degree of the node represents the direct positive influence from the node to others.
- Local Degree 1. Mathematically, the first type local degree LD1 of node i is given by:

$$ld_i^1 = \begin{cases} \sum_{j \in V} a_{ij}^+ & i \in \Omega \\ 0 & i \notin \Omega \end{cases} \tag{6}$$

where Ω is the node set within the distance $l = 3$ from the target nodes.

- Local Degree 2. The second type local degree LD2 of node i is given by:

$$ld_i^2 = \begin{cases} \sum_{j \in \Omega} a_{ij}^+ & i \in \Omega \\ 0 & i \notin \Omega \end{cases} \tag{7}$$

Note that the two type local degree methods are used to rank the node set Ω which are within the distance $l = 3$ from the target nodes. The difference between them is that LD1 counts the our-positive neighbor in the whole network while LD2 counts the out-positive neighbor only in Ω.

4.2 Experiment Results

In this section, we present our experiment results of the positive influence spreading performance of different methods on Slashdot and Bitcoinalpha. We also define the positive influence spreading performance as the proportion of the target nodes that are positively infected to the total infected nodes under the IC-S model.

Figure 5A,B shows the performance of four comparison methods (Random, Degree, Out-Degree, and Positive Out-Degree) under three types of propagation probabilities model (WC model, TRIVALENCY model, and UN model) on Slashdot data set (or Bitcoinalpha data set). The size of seed nodes k is set ranging from 50 to 300. For the UN model, we set the diffusion probability to 0.03. When constructing the target set T, we treat node 2,921 whose coreness is 2 as the center, and take the nodes within two steps from it as the target nodes. The top k nodes under the five ranking methods are selected to be the seeds, whose infecting ability are then tested by the IC-S model. After 2,000 iterations on the IC-S

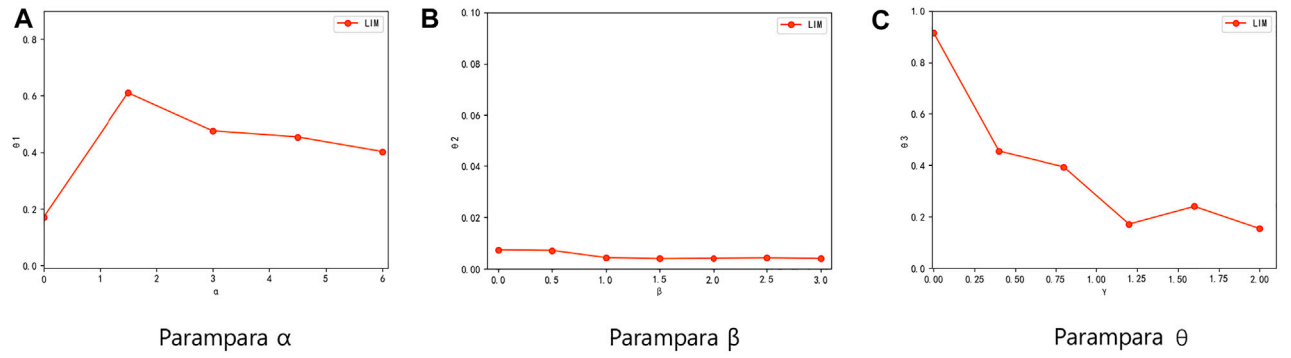


FIGURE 7 | Results of parameter testing. The experiment is carried out on Slashdot. The first and third experiments use WC models and select 30 seeds, while the second one is done under the UN model which set the diffusion probability to 0.5 and selects 100 seeds. The center node of the target nodes is set to node 2,921. **(A)** Results of parameter α. θ_1 means the proportion of positively activated target nodes among all activated nodes. Each point in this figure represents the θ_1 value with a different α value. **(B)** Results of parameter β. θ_2 means the proportion of negatively activated target nodes among all activated nodes. Each point in this figure represents the θ_2 value with different β value. **(C)** Results of parameter γ. θ_3 means the proportion of positively and negative activated non-target nodes among all activated nodes. Each point in this figure represents the θ_3 value with different γ value.

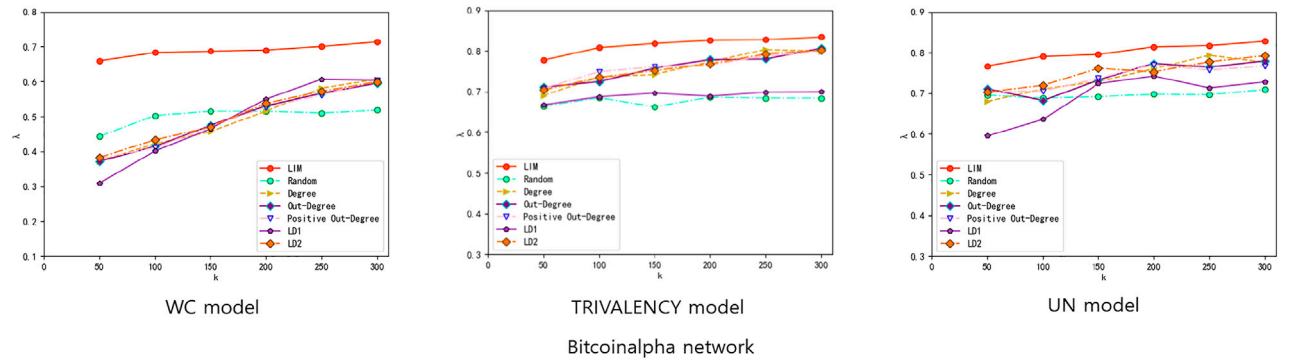


FIGURE 8 | Results of targets set transformation. The experiment is done on Bitcoinalpha. The experiment selects 150 seeds under three models. And the center node of the targets is node 1 which has the highest coreness. Same as the above experiments, the LIM method compares with other 6 methods.

model, the average positive influence spreading performances can be obtained. As shown in both **Figure 5A,B**, the LIM method outperforms the other four methods as the size of the seed nodes changes with all three types of different propagation probability.

The reason why the LIM method performs better at the beginning is that the λ we calculate is a proportion, not the number of nodes. Because of the difference of the size of seed nodes, the number of the target nodes that are positively activated and the number of the nodes finally activated are different. So even if λ_1 is bigger than λ_2, the number of the target nodes that are positively infected in experiment 1 may be smaller than that of experiment 2. Besides, the experiments on Bitcoinalpha under TRIVALENCY mode and UN model do not perform as well as in the WC model. This is mainly because that there is a lot of overlap between the nodes selected by LIM method and the nodes selected by other methods. For example, if we select 150 nodes to be seed nodes, more than 80 nodes are repeatedly selected by both the LIM method and Degree method under either of the two models.

We also compare the method LIM with the two local degree methods (LD1, LD2) on these two data sets under three types of propagation probabilities model, see **Figure 6A,B** This also shows that the LIM method performs well.

Furthermore, in order to validate the effects of the three parameters α, β, and γ, we change each of these three parameters separately and observe the changes in spreading ability. During all three experiments, the parameter that needs to be tested is changed while the other two parameters are kept as 1. **Figure 7A** shows the effect of α when applying on Slashdot under the WC model, here 30 seeds are selected. θ_1 represents the proportion of positively activated target nodes among all activated nodes. We can see that as the value of α increases, θ_1 increases significantly and then stabilizes. The significant increasing in θ_1 shows that a bigger parameter α can help to select those nodes which can positively activate targets as seeds. Similarly, **Figure 7B** shows the effect of parameter β applying on Slashdot under the UN model with the diffusion probability of 0.5, and 100 seeds are selected. θ_2 represents the proportion of negatively activated target nodes among all activated nodes. It can be seen that θ_2 has a slight downward trend but is not more obvious, this is because in most real social networks, there are

more positive edges than negative edges. The downward trend in **Figure 7B** sufficiently shows that the setting of a bigger parameter β effectively prevent negatively activating target nodes. **Figure 7C** shows the effect of parameter γ applying on Slashdot under WC model, and 30 seeds are selected. θ_3 represents the proportion of positively and negative activated non-target nodes among all activated nodes. The value of θ_3 decreases from 0.9 to nearly 0.2 as γ increases, which shows that the setting of a bigger parameter γ is also useful to prevent activating non-target nodes.

5 DISCUSSION

Identifying the influential spreaders is a very important problem both in theory and in practice. Though a number of methods have been proposed, most of them aim to infect most nodes across entire networks. However, in some real systems which intend to infect a small group of nodes, the traditional centrality methods are found to be not accurate enough to find the influential nodes to target. We extend this problem from unsigned networks to signed networks, and thus propose a local influence matrix method to rank the spreading ability of the nodes towards the targets. The simulation results indicate that our method outperforms the traditional centrality methods. Furthermore, by adjusting the parameters we set, the new method is found to be able to reduce the impact on non-target nodes.

Regarding the choice of the center node of the targets in the experiments, we would like to choose a node with smaller coreness. That is because the node with high coreness is more closely connected with other nodes, which easily causes too many targets to be selected. For example, there are 3,783 nodes on Bitcoinalpha and more than 2,000 nodes are selected as targets, if the node with highest coreness is chosen as center node. This is inconsistent with the scenario for local targets we set in advance. For example, if we choose node 1 of the Bitcoinalphain which has the highest coreness as the center of the targets, the results comparing the LIM method with the other 6 methods show that the LIM method still performs better but not much better than others, see **Figure 8**. This also shows that this new LIM method will work better when the target is localized.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

XQ proposed the idea. JS and XQ wrote the paper. ZF programmed.

FUNDING

This work is supported by the National Natural Science Foundation of China (CN) with No. 11971271; Natural Science Foundation of Shandong Province with No. ZR2019MA008.

REFERENCES

1. Bonacich P. Factoring and Weighting Approaches to Status Scores and Clique Identification. *J Math Sociol* (1972) 2:113–20. doi:10.1080/0022250x.1972.9989806
2. Freeman LC. A Set of Measures of Centrality Based on Betweenness. *Sociometry* (1977) 40:35–41. doi:10.2307/3033543
3. Kitsak M, Gallos LK, Havlin S, Liljeros F, Muchnik L, Stanley HE, et al. Identification of Influential Spreaders in Complex Networks. *Nat Phys* (2010) 6:888–93. doi:10.1038/nphys1746
4. Luan Y, Bao Z, Zhang H. Identifying Influential Spreaders in Complex Networks by Considering the Impact of the Number of Shortest Paths. *J Syst Sci Complex* (2021) 11:22194. doi:10.1007/s11424-021-0111-7
5. Ma L-l., Ma C, Zhang H-F, Wang B-H. Identifying Influential Spreaders in Complex Networks Based on Gravity Formula. *Physica A: Stat Mech its Appl* (2016) 451:205–12. doi:10.1016/j.physa.2015.12.162
6. Guilbeault D, Centola D. Topological Measures for Identifying and Predicting the Spread of Complex Contagions. *Nat Commun* (2021) 12:4430. doi:10.1038/s41467-021-24704-6
7. Sun Y, Ma L, Zeng A, Wang W-X. Spreading to Localized Targets in Complex Networks. *Sci Rep* (2016) 6:38865. doi:10.1038/srep38865
8. Li D, Xu Z-M, Chakraborty N, Gupta A, Sycara K, Li S, et al. Polarity Related Influence Maximization in Signed Social Networks. *PLoS ONE* (2014) 9: e102199. doi:10.1371/journal.pone.0102199
9. Kumar S, Spezzano F, Subrahmanian V, Faloutsos C. Edge Weight Prediction in Weighted Signed Networks. In: Proceedings of the data Mining (ICDM), 2016 IEEE 16th International Conference on (IEEE); December 2016; Barcelona, Spain. p. 221–30.
10. Kumar S, Hooi B, Makhija D, Kumar M, Faloutsos C, Subrahmanian V. Rev2: Fraudulent User Prediction in Rating Platforms. In: Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining (ACM); February 2018; New York, NY, USA. p. 333–41.
11. Chen W, Wang C, Wang Y. Scalable Influence Maximization for Prevalent Viral Marketing in Large-Scale Social Networksryan. In: Proceedings of the 16th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD'2010); July 2010; Washington DC, U.S.A. p. 1029–38.
12. Kempe D, Kleinberg J, Tardos E. Maximizing the Spread of Influence through a Social Network. *Theor Comput* (2003) 11, 137–46. doi:10.1145/956750.956769

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

frontiers in Physics

ORIGINAL RESEARCH
published: 20 January 2022
doi: 10.3389/fphy.2021.822915

Multilayer-Aggregation Functional Network for Identifying Brain Fatigue and Diseases

Wen-Kuo Cui[1,2†], *Xin-Rui Qi*[3†], *Yu Sun*[4] *and Gang Yan*[1,2,5*]

[1]School of Physics Science and Engineering, Tongji University, Shanghai, China, [2]Frontiers Science Center for Intelligent Autonomous Systems, Tongji University, Shanghai, China, [3]Center for Translational Neurodegeneration and Regenerative Therapy, Shanghai Tenth People's Hospital, Tongji University School of Medicine, Shanghai, China, [4]The Key Laboratory for Biomedical Engineering of Ministry of Education of China, Department of Biomedical Engineering, Zhejiang University, and with the Zhejiang Lab, Hangzhou, China, [5]Center for Excellence in Brain Science and Intelligence Technology, Chinese Academy of Sciences, Shanghai, China

Recent years have witnessed increasing interest of applying network science methodologies to analyze brain activity data. Owing to the noninvasiveness, low cost and high sampling rate, electroencephalogram (EEG) recordings have been widely used as a proxy for probing the internal states of human brains. Previous correlation-based functional networks (CFN) mainly focused on the covariance or coherence between readings from electrodes attached to different regions, largely overlooking local temporal properties of these electrical activities. Here, we propose a method to construct multilayer-aggregation functional network (MAFN) which is able to capture both temporal and topological characteristics from EEG data. We extract features from these MAFNs and incorporate them into each of 12 classification algorithms, aiming to detect mental fatigue and two brain diseases, schizophrenia and epilepsy. The results demonstrate that MAFNs consistently outperform CFN and dynamic version of CFN. In comparison to functional networks based on weighted phase lag index (wPLI), MAFNs also achieve higher or comparable accuracy in most classifiers. Moreover, the nodal features of MAFNs allow us to identify the important positions of EEG electrodes for different brain states or diseases. These findings together offer not only a framework for classifying normal and abnormal brain activities but also a general method for constructing more informative functional networks from multiple time series data.

Keywords: electroencephalogram, functional network, mental fatigue, schizophrenia, epilepsy

OPEN ACCESS

Edited by:
Gaogao Dong,
Jiangsu University, China

Reviewed by:
Xiaoke Xu,
Dalian Nationalities University, China
Zhihai 'Rong,
University of Electronic Science and Technology of China, China

***Correspondence:**
Gang Yan
gyan@tongji.edu.cn

†These authors have contributed equally to this work

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *26 November 2021*
Accepted: *23 December 2021*
Published: *20 January 2022*

Citation:
Cui W-K, Qi X-R, Sun Y and Yan G (2022) Multilayer-Aggregation Functional Network for Identifying Brain Fatigue and Diseases. Front. Phys. 9:822915. doi: 10.3389/fphy.2021.822915

1 INTRODUCTION

Human brain is one of the most delicate and complex systems, responsible for maintaining the internal regulation of human body and perception, and responding to external stimuli. To understand the working mechanism of brain function and to detect brain states and diseases, such as mental fatigue [1], epilepsy [2], sleep disorders [3], schizophrenia [4], depression [5] and Alzheimer's disease (AD) [6], several noninvasive technologies have been invented and widely used, such as functional magnetic resonance imaging (fMRI) [7], electroencephalogram (EEG) [8], computed tomography (CT) [9], and so on. Constructing functional networks from the brain activities recorded with these technologies has attracted more and more attentions [10–12]. In functional networks, nodes represent brain regions or voxels and edges are supposed to capture the

functional interactions between different nodes. Increasing evidence showed that functional networks change with cognitive activities, emotion, and the development of brain diseases and so on [13, 14]. Hence, functional networks can be applied to reveal different brain states or to detect brain illnesses whose neuropathology are not yet clear. For example, previous studies have found that, among others, the modules of the brain's functional network become more isolated, and the connections within the modules become stronger when people age [15]. Functional networks of patients with schizophrenia, compared with healthy people, and exhibit abnormalities in multiple global indicators (global clustering coefficient, small-world-ness, etc.) [16].

Among the technologies mentioned above, EEG has the advantages of high time resolution, and convenient data collection and low cost. Hence, extracting information from EEG recordings has been a very active field which aims to understand intentions and emotions [17, 18], to diagnose neuropsychiatric disorders (mental illness and brain diseases) [5, 19, 20], and to develop new brain-computer interface (BCI) technologies [21–23]. In these applications EEG based functional networks have also been widely used. For example Ref. 24, constructed functional networks of fatigued brains via source localization of cortical activities in 26 predefined regions of interest, and found that the characteristic path length increased, offering support for the presence of a reshaped global topology in cortical connectivity networks under fatigue state Ref. 25; explored the emotion associated functional networks among different subjects and extracted three topological properties from these networks as classification features. Their results showed that there are indeed common connectivity patterns associated with different emotions, and also demonstrated that topological features have considerable advantages over conventional power spectral density Ref. 26; constructed functional networks from EEG readings in resting state and memory task state, and found that healthy people under memory task state showed small-world characteristics in different frequency bands Ref. 27; studied cortical functional networks of subjects after sport-related mild traumatic brain injury (MTBI) and found that MTBI induces an increase in short-distance connectivity and a decrease in long-distance connectivity.

However, previously established EEG-based functional networks mainly focused on the correlation or coherence between different channels, i.e., building the connections between the electrical activity of different brain regions [28, 29]. Such constructions can enable network science methodologies to probe the interactions between regions, but largely overlook intrinsic local temporal properties of EEG signals. The fact prompts us to explore an important and interesting question: How to map the readings of multiple EEG channels into a functional network that can capture both topological and temporal characteristics of these signals? Here, to address this need, we propose an approach to construct MAFNs from multiple time series. We first build an undirected network from each time series by utilizing the idea originally from the network science field [30, 31]. Such networks can reveal the temporal regularities in each signal. We then aggregate these networks into a weighted one based on the topological similarity of different layers, which thus can also capture the connections between different channels. To demonstrate the effectiveness of our approach, we incorporate MAFNs with various supervised and unsupervised classifiers and apply them to identify three typical neuropsychiatric disorders including mental fatigue, schizophrenia and epilepsy.

To demonstrate the effectiveness of our approach, we incorporate MAFNs into 12 supervised and unsupervised classifiers and apply them in three typical tasks, identifying mental fatigue, diagnosing schizophrenia, and detecting epilepsy. The results show that in comparison to correlation-based functional networks (CFNs) and dynamic (sliding window) version of CFNs (DCFNs), MAFNs exhibit significantly higher accuracy. In addition, as the scalp-level network is affected by the volume conduction problem (each channel receives information from many brain sources), functional networks based on weighted phase lag index (wPLI) [32] are also constructed for comparison. MAFNs also achieve comparable performance, with higher accuracy in 9 out of 12 classifiers.

The main contributions of the present work can be summarized as follows.

(i) We establish a multilayer-aggregation approach for constructing functional networks from multiple time series, which is able to capture both temporal and topological characteristics of these signals;
(ii) We incorporate the constructed functional networks into 12 classifiers and apply them in three typical EEG applications, systematically demonstrating the effectiveness of our approach;
(iii) The higher accuracy of MAFN in extracting temporal and topological characteristics and identifying fatigue, schizophrenia, and epilepsy from EEG data allow it to be a potential method for understanding neural circuits associated with behaviors and diagnosing the neuropsychiatric disorders using EEG recordings.

The rest of the paper is structured as follows. **Section 2** describes the construction approach of MAFN and the classification framework based on such networks. **Section 3** shows the comparison results between traditional methods (CFN, DCFN, and wPLI) and MAFN in three EEG datasets (fatigue, schizophrenia, and epilepsy). Discussion and Conclusion are given in **Section 4**.

2 METHODS

This section includes three parts: construction of multilayer-aggregation functional networks (MAFNs) feature extraction and selection from MAFNs and MAFN-based classification framework.

2.1 Construction of MAFNs

The effectiveness of functional networks in distinguishing brain states is heavily dependent on construction methods, i.e., the

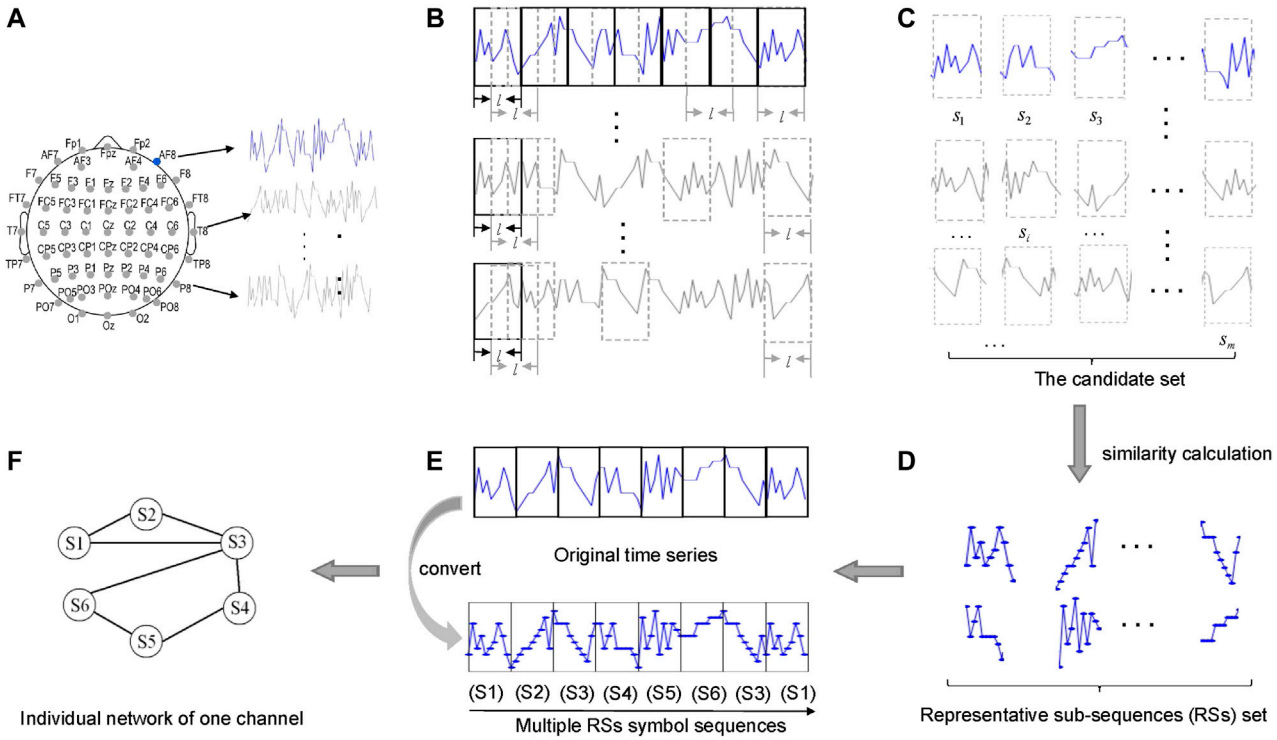


FIGURE 1 | Construction of an individual network layer for each channel. **(A)** EEG channel locations and its recorded time series. **(B)** Segmentation process of time series. **(C)** Candidate set of sub-sequences. **(D)** The representative sub-sequences (RSs) set. **(E)** The process of replacement. **(F)** The individual network (layer) for one channel.

more informative the more applicable. However, how to reconstruct a scalp-level network or source connectivity network able to represent the intrinsic connections between regions from coarse-grained and usually noisy readings is a nontrivial problem. According to the time series recordings, researchers have proposed several functional connectivity indexes to construct functional networks. Correlation-based functional networks (CFNs) and dynamic (sliding-window) version of CFN (DCFNs), as well as weighted phase lag index (wPLI) succeeded in a wide range of applications, given the fact that human brain is indeed composed of a few billion of interconnected neurons. A weighted matrix is obtained according to different functional connectivity indexes, and then binarized to obtain an unweighted and undirected network that represents the relationship between different regions. At a coarse-grained level, the human cerebral cortex can be roughly divided into several different regions, which are actually dependent on each other, and function cooperatively [33]. The dependence between regions is so strong that it can be captured by nice correlations of the activities between regions. In addition, brain activities also show temporal patterns, which means that one region is activated following the other. Thus, it is expected that construction of functional networks with better informativeness should take into account not only topological but also temporal properties. To satisfy this need, we propose a two-phase approach to create the MAFNs from EEG readings. Furthermore, according to different calculation indexes of each stage, three kinds of are constructed, based on dynamic time warping [34] (MAFN-dtw), symbolic mutual information [35, 36] (MAFN-smi), and hub depressed index [37] (MAFN-HDI) respectively.

First, to reveal temporal regularities an idea from network science (see [30, 31]) is adopted for building a network from a single time series. As illustrated in **Figure 1**, we use a sliding window to split all EEG time series (**Figure 1B**) into m sub-sequences (**Figure 1C**), and then identify from these m sub-sequences the representative sub-sequences (RSs) through the idea similar to clustering: 1) Calculate the similarity (measured by dynamic time warping (DTW) [34] or symbolic mutual information (SMI) [35, 36]) between each pair of sub-sequences, and for each sub-sequence we select its k most similar (other) sub-sequences; 2) In the mk selected sub-sequences, some are repeated. Hence we pick the top k ones who occur most frequently. 3) In these k sub-sequences, we identified n sub-sequences that are most dissimilar to each other. Therefore, the cardinality of the final set of RSs equals n. In this work we set $n = 40$. Through the procedure, the RSs we identified are most dissimilar to each other, yet are most similar to other original sub-sequences. That is, the RSs can indeed considered as motifs occurring in EEG time series (**Figure 1D**). Finally, we convert each single time series into a symbol sequences by replacing each original sub-sequence

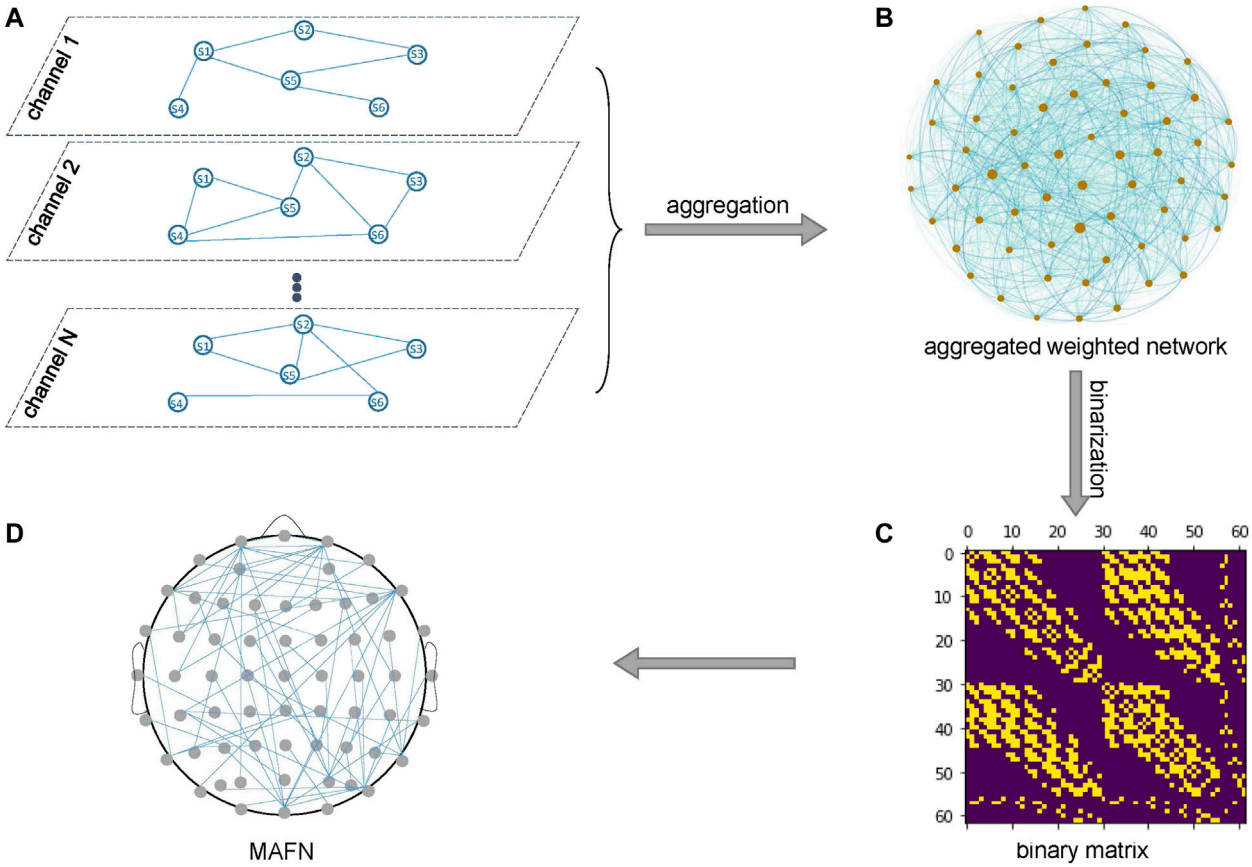


FIGURE 2 | Aggregation of the layers of all channels. **(A)** The individual layers of *N* channels and **(B)** an aggregated weighted network of these layers. **(C)** The binary matrix for the MAFN in **(D)**.

with its most similar RS (**Figure 1E**), which can be further transformed to a network (**Figure 1F**). Each node represents a RS, and two nodes are connected by a link if the two RSs in the original time series are temporally proximal to each other. Therefore, through the above procedure each channel is represented by a network (or called layer hereafter).

Second, as illustrated in **Figure 2**, the individual layers of all channels are merged into an MAFN by aggregation. Such an aggregation process captures the dependence between different channels (layers). Here we use Jaccard coefficient or Hub Depressed Index (HDI) [37]) to calculate the local *structural* similarity of node i between any pair of layers X and Y. For a node i, let $k_i(X)$ represents the degree of i in layer X and $\Gamma_i(X)$ represents the neighbor node set of node i in layer X. Jaccard coefficient and HDI between two layers are defined as

$$\mu_{XY}^{i} = \frac{|\Gamma_i(X) \cap \Gamma_i(Y)|}{|\Gamma_i(X) \cup \Gamma_i(Y)|} \tag{1}$$

and

$$\mu_{XY}^{i} = \frac{|\Gamma_i(X) \cap \Gamma_i(Y)|}{\max\{k_i(X), k_i(Y)\}} \tag{2}$$

respectively. Then the global similarity between layer X and layer Y is quantified by

$$Sim_{XY} = \frac{1}{n}\sum_{i=1}^{n} \mu_{XY}^{i} \tag{3}$$

where n is the number of nodes (*i.e.,* RSs).

So far, through the two steps above we obtain a weighted network of these layers (**Figure 2B**), where the weight of a link represents the similarity of two corresponding layers. We expect that the similarity indicates the strength of dependence between the two channels. Finally, we binarize the weighted network to a (0, 1)-matrix (**Figure 2C**) that corresponds to a MAFN shown in **Figure 2D**. Because the threshold of binarization affects the number of links and also the topological properties of the MAFN, as discussed in the next subsection we extract the features of networks with different levels of sparsity, from 12 to 34% with step size 2%, and input all these features into each classifier in our numerical experiments.

2.2 Feature Extraction From MAFNs

Network science offers several important metrics to mathematically characterize the topology of networks [38–42].

TABLE 1 | Features of functional networks.

Feature type	Feature name	Symbols
Global	Global clustering coefficient	C
	Average path length	L
	Small-world-ness	σ
	Modularity	Q
	Global efficiency	E_g
	Rich-club-ness	R_{cl}
	Average degree	$\langle k \rangle$
	Link density	ρ
	Assortativity	r
	Average Nodal efficiency	$\langle E \rangle$
Local	Node degree	k_i
	Nodal efficiency	E_i
	Nodal Betweenness	B_i
	Closeness centrality	C_{ci}
	Nodal clustering coefficient	C_i

The changes of these metrics can be used as indicators to distinguish brain functional networks for different brain states from various perspectives [43, 44]. The metrics roughly fall into two categories—global and local. Global metrics capture the connection patterns among nodes as a whole. For example, the average path length reveals the dispersion of network structure hence is related to information transmission efficiency; Modularity quantifies the extent to which a network can be divided into several densely connected communities. Local metrics capture the surrounding connection patterns of a specific node or link. For example, nodal degree is simply the number of a node's neighbors; Nodal clustering coefficient describes the connnectedness among a node's neighbors; Nodal betweenness is useful for determining whether a specific link is a bottleneck for network diffusion. In order to reflect the diversity of functional network properties, here we employ 10 global and 5 local metrics, as listed in **Table 1**.

It is worth noting that the values of these metrics depend on the threshold used to binarize either the functional network has been proposed or aggregated (weighted) networks in the second phase of MAFN construction. Hence, we consider the metrics for a wide range of network sparsity that is defined as the fraction of existing links out of all possible links between nodes. Specifically, for each metric x we also calculate the area under the curve (AUC) [16, 45] that represents the metric value as a function of network sparsity, i.e.,

$$x^{AUC} = \sum_{i=1}^{q-1} [x(S_i) + x(S_{i-1})] * \triangle S \Big/ 2, \tag{4}$$

where $[S_1, S_q]$ is the range of sparsity and $\triangle S$ is the interval for discretizing the range.

In classification algorithms described in the next subsection, we use all features for the metrics listed in **Table 1**. In fact, we constructed functional networks with sparsity levels from 12 to 34% and calculated the network attributes of all these networks, *i.e.,* for each metric x all its features $\{x(S1 = 12\%), x(S2 = 14\%), \ldots, x(Sn = 34\%), x^{AUC}\}$ are inputted into the classifier. Hence, the number of total features is the sum of the local and the global feature numbers. For instance, in the task of mental fatigue identification where each subject has 62 EEG channels, the total number of features is $(62 \times 5 + 10) \times 13 = 4160$. Similarly, the total number of features for schizophrenia and epilepsy data are 4,095 and 1,690 respectively. In order to perform fair comparisons, the total number of features obtained from correlation-based functional networks is equal to those above respectively.

In addition, to increase the interpretability of the results and to screen out the sensitive indicators of the network, we conduct a difference analysis on the indicators of the functional network by using supervised algorithms. Samples are given labels, and one can obtain the statistically significant difference of each network metric and the most differentiated binarization threshold through inter-group statistics between healthy and abnormal samples. To do so, we first use the Z-score method to standardize the metrics and count the normalized mean value of each metric x under all sparsity of one network to obtain the statistically significant difference of each network metric. Then we perform t-tests of the metrics at different network sparsity levels and calculate the corresponding p-values, followed by choosing the sparsity which results in the most statistically significant metrics (significance level is set to $p < 0.05$) [46]. Such a way is able to point out the sensitive indicators, as shown in **Section 3**, for understanding the possible mechanisms underlying the brain illness. It is noteworthy that such calculations is only for interpreting the results, and in all comparison experiments we do not intentionally choose metrics or sparsity levels.

2.3 Classification Framework Based on MAFNs

After the MAFNs constructed from experimental EEG data and the features extracted from MAFNs, we put these features encoding both topological and temporal properties into classifiers. In order to extensively compare the capability of MAFNs to that of other methods, in the present study we employ 6 *supervised* classifiers, including support vector machine with radial basis kernel function (SVM-RBF), with sigmoid kernel function (SVM-SIG), and with polynomial kernel function (SVM-POL), multi-layer Perceptron (MLP), decision tree C4.5 and dense graph propagation (DGP) [47], as well as 6 *unsupervised* classifiers, including invariant information clustering (IIC) [48], one class support vector machine (OC-SVM) [49], support vector data description (SVDD) [50], k-means, hierarchical clustering divisive analysis (DIANA), density-based spatial clustering of applications with noise (DBSCAN). To assess the performance of MAFNs in these classifiers we use accuracy defined as $(TP + TN)/(TP + TN + FN + FP)$ where TP, TN, FP, and FN represent true positive, true negative, false positive, and false negative, respectively.

In supervised classifiers, the data samples were divided into training, validation and test sets with proportions of 50, 20, and 30%, respectively. For each classifier, all features of the functional networks constructed from the training set are used to train the model, and then 5-fold cross-validation is used to validate the model, obtaining the best model parameters. Next, we test the

model and got the classification accuracy in the test dataset (i.e., the remaining 30% of the original data). Finally, we repeat the above two steps 50 times by randomly splitting the samples into training, validation and test sets, and eventually obtain the arithmetic mean of these classification accuracies as *ACC*.

In contrast, unsupervised classifiers cluster the samples to different groups according to some criteria and do not have a training process. Take the k-means as an example. First, we construct networks with sparsity levels of from 12 to 34% and calculate the values of all the features of each network respectively. Then we input the features of each network sparsity into the k-means classifier. The k-means is repeated for several times, and the smallest sum of squared errors (SSE) is the final clustering result. A prediction label is assigned to each sample. Finally, we use classification accuracy to measure the clustering results (the comparison between the assigned labels and the real labels of each sample was concluded by clustering). Note that we calculate the classification results of functional networks with different levels of sparsity, whose mean value was set as *ACC*.

3 APPLICATIONS

In this section, we incorporate MAFNs with classification algorithms and apply to three typical scenarios, demonstrating the advantages and effectiveness of MAFNs compared with the previous 3 methods. Moreover, we also show how to identify the important electrodes and their locations for detecting mental fatigue and schizophrenia.

3.1 Application in Mental Fatigue Identification

Mental fatigue can cause difficulty in concentration and negative emotions, which further reduce work efficiency, and even lead to various accidents. Hence, identifying mental fatigue has attracted considerable attention in the past decade. Here, we analyze a dataset from 26 subjects with mental fatigue [21, 24]. Each subject underwent a 20-min psychomotor vigilance test (PVT), a high-signal-load way based on reaction time for evaluating the ability to sustain attention and be alert to salient signals. To study the effect of increased mental fatigue with working hours, the first and last 5-min intervals were set as the least, and most fatigued states, respectively. High-density continuous EEG recordings were acquired from 62 Ag/AgCl scalp electrodes according to the International 10–20 system (ASA-Lab, ANT B.V., and Netherlands). The typical electrode positions are illustrated in **Figure 1A**. Signals containing artifacts due to eye movements or significant muscle activity during the recordings were removed offline via an independent component analysis approach. The final EEG signals were baseline adjusted and further digitally band pass filtered in the range 0.5–40 Hz (fifth order Butterworth). The artifact-free epochs of 500 ms duration EEG segments (from 0 to 500 ms post-stimulus) were selected and grouped for further analysis. Rhythmic patterns of activity in the (8–10 Hz) range could be an appropriate physiological signal for revealing the topological differences of cortical connectivity in fatigue state as low alpha waves have specifically been implicated with decreasing alertness. Here, we apply a graph theoretical approach to analyze such changes in the lower alpha (8–10 Hz) band of EEG data.

We construct three types of MAFNs (MAFNs-dtw, MAFNs-smi, and MAFNs-HDI), using the method described in Section 2.1, for the first and last 5-min intervals respectively for each subject. To perform comparisons, for each subject we also construct three other corresponding types of functional networks (CFNs, DCFNs, and wPLIs) simply by calculating the correlations between all pairs of EEG time series and then binarizing the correlation matrix into an undirected unweighted functional network. We examine different values of binarizing threshold (12–34%) to obtain functional networks with different levels of sparsity. To distinguish the least and most fatigued states, we extract the features from the metrics listed in **Table 1** of all these sparse networks (*i.e.,* each subject has 4160 features), and then input these features into the classifiers described in **Section 2.3**. As exhibited in **Figure 3**, the MAFNs are more effective than the corresponding CFN and DCFN in all 6 supervised and 6 unsupervised classifiers. Moreover, we observe that MAFN + SVM-SIG obtains the highest accuracy in supervised learning and wPLI + IIC outperforms other unsupervised algorithms. Meanwhile, while wPLIs are more effective than correlation-based functional networks, our MAFNs still achieve higher or comparable accuracy in 9 out of 12 classifiers.

To increase the interpretability of the results we also want to reveal the sensitive indicators of the network, *i.e.,* to examine the topological properties in each layer network for the least and most fatigued brain states. As shown in **Figure 4A**, we take F3 for example which is attached to the frontal lobes of the cerebral cortex. This region plays vital roles in memory, attention, motivation, and also has the capacity to organize and plan daily tasks. For all subjects, we count the normalized mean value of each global metric Y under all sparsity of the F3 network. We find that there are indeed significant structural differences between the F3 network layer of least and most fatigued states. Specifically, compared with the least fatigued subjects, the values of C, $\langle k\rangle$, ρ, and $\langle E\rangle$ are decreased in most fatigued networks, while the values of the other 6 global metrics are increased. Such decreases and increases are all statistically significant (t-test, p-value < 0.05). To understand the impact of network sparsity on classification framework performance, we examine the statistical significance of network metrics listed in **Table 1** for different levels of sparsity. As shown in **Figure 4B**, we find that sparsity indeed remarkably affects the expressiveness of functional networks. The inter-group comparison results reveal that there exists an optimal sparsity level, i.e., an optimal binarizing threshold, for binarizing the aggregated weighted network. Here, for distinguishing the least and most fatigued subjects, the optimal sparsity is 26% at which the differences of global metrics between the two groups are all statistically significant (the gray area in **Figure 4B**).

Moreover, the features extracted from local metrics are important for recognizing the contribution of each node in

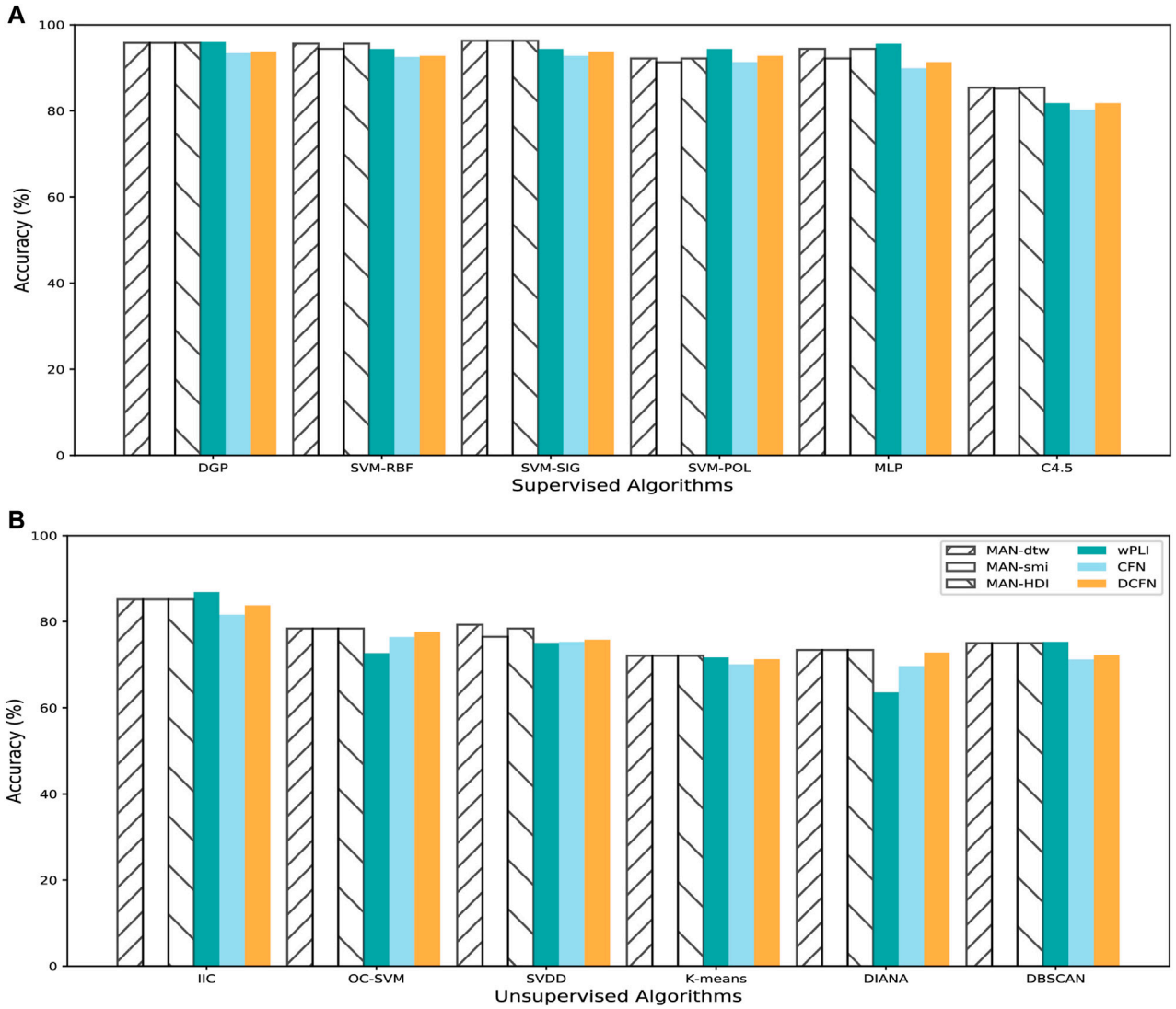


FIGURE 3 | Comparison between different methods of brain functional network construction in detecting mental fatigue with 6 supervised classifiers and 6 unsupervised classifiers. Comparison in **(A)** supervised and **(B)** unsupervised classifiers.

MAFN, *i.e.,* identifying the most relevant electrode positions for a specific task. To do so, we calculate the accuracy of the proposed classification framework by using the local metrics of only one node and descending sort the nodes according to these *ACC* values. And then put the ranking labels (1–62) as the *x*-axis. As shown in **Figure 5A**, we take the results of SVM-RBF algorithm as an example, and obtain the accuracy rate for each channel by using different network construction methods respectively. The green line is the results of MAFN-dtw + SVM-RBF, and the top1 node (electrode) is F3 which is attached to the frontal lobes of the cerebral cortex. Then we pick up the top 10 channels with the highest accuracies of the methods and the results are shown in **Figure 5C**. The process is repeated for other 5 types of network construction method. We pick up the top 10 channels with the highest accuracies of 6 methods respectively and find that the most important electrodes for fatigue detection are mainly located in the frontal and the central areas with the left electrodes more relevant than the right ones. So, it is shown that although there are differences between the results calculated from 6 network construction methods (i.e., there are differences between the top 10 highest classification accuracy channels of different methods), all 6 methods can clearly distinguish the importance of each node of the network.

3.2 Application in Schizophrenia Diagnosis

Schizophrenia is a serious and chronic mental disorder with typical positive symptoms such as delusions, hallucinations and negative symptoms such as depressed mood, which affects about 1% of people across the globe. One possible explanation for some of the symptoms of schizophrenia is that one or more problems with the corollary

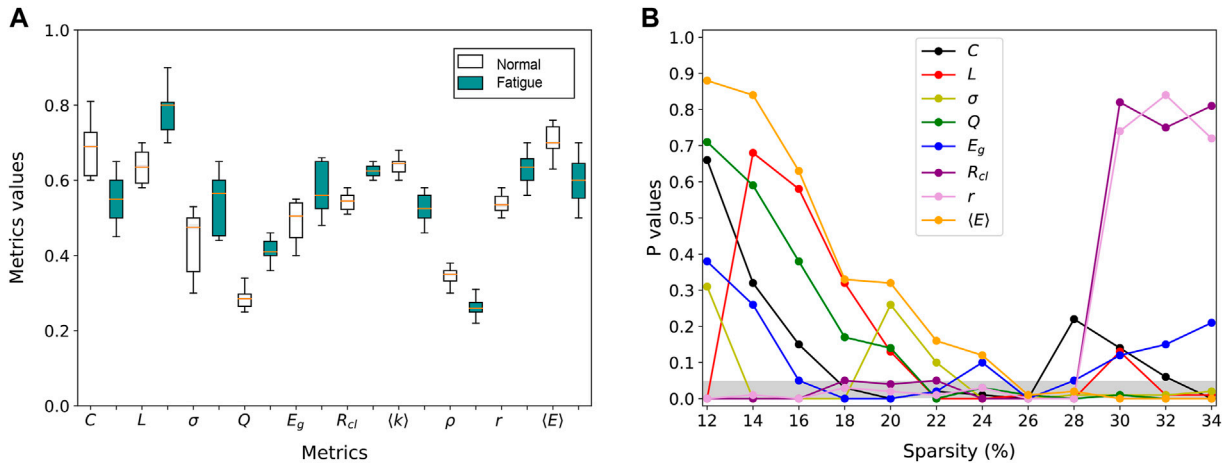


FIGURE 4 | Statistically significant difference of metrics between fatigued and healthy groups. **(A)** Inter-group differences of global metrics in the individual layer of F3 channel. **(B)** Statistical significance of the inter-group difference of global metrics as a function of network sparsity.

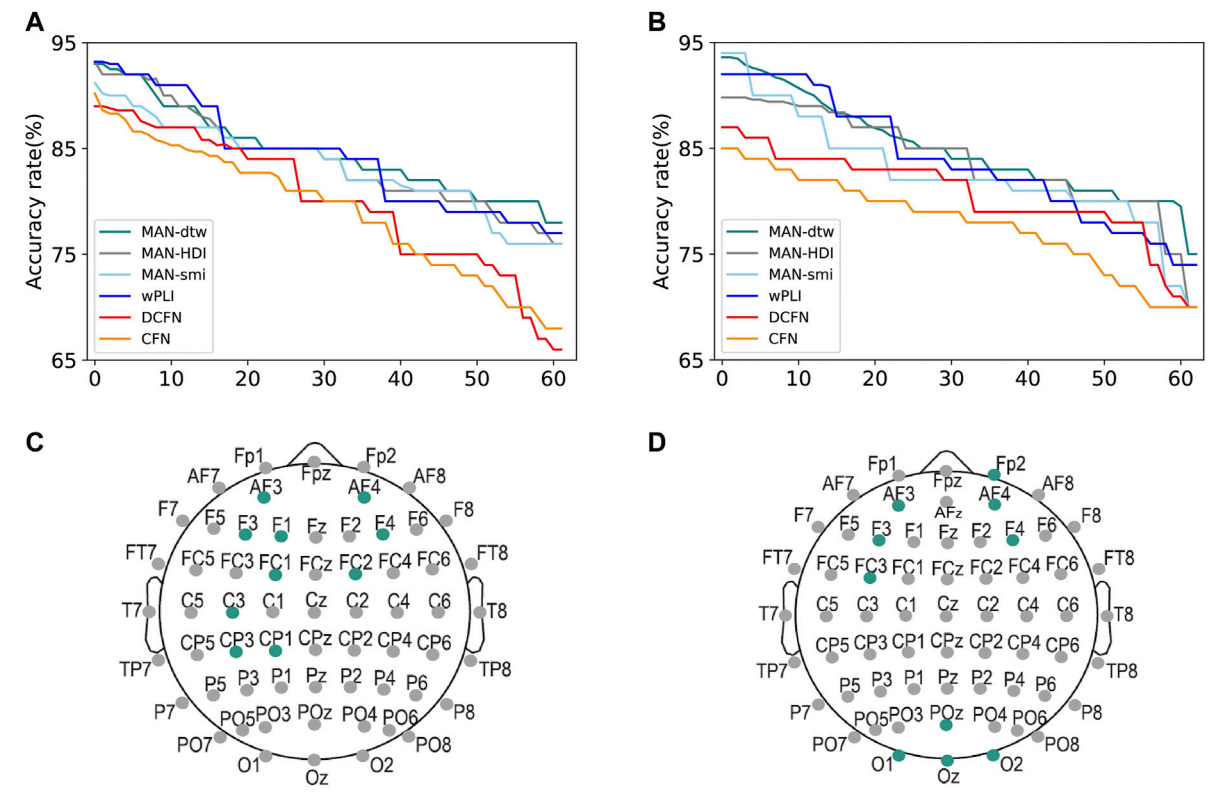


FIGURE 5 | Important channels and their locations for detecting fatigue status **(A,C)** and schizophrenia **(B,D)**. The colored points in **(C,D)** represent the corresponding positions.

discharge process in the nervous system make it difficult for patients to distinguish between internally and externally generated stimuli. Schizophrenia has made a big burden for patients and their family which prompt us to find a quick and good way for diagnosis and even early warn of the emergence of schizophrenia. In the present study we use the dataset, which is already pre-processed, from patients with

TABLE 2 | Comparison results of MAFNs and other methods for schizophrenia diagnosis.

	Networks	DGP	SVM-RBF	SVM-SIG	SVM-POL	MLP	C4.5
Supervised	MAFN-dtw	87.6	89.6	90.2	**92.4**	89.5	81.8
	MAFN-smi	86.8	87.9	89.7	90.9	88.2	81.6
	MAFN-HDI	86.5	89.6	90.2	**92.4**	87.6	82.4
	wPLI	87.5	89.6	91.2	91.2	91.2	82.1
	CFN	85.3	86.9	83.2	82.2	85.4	76.0
	DCFN	86.1	87.2	87.4	89.5	86.7	79.9
	Networks	IIC	OC-SVM	SVDD	K-means	DIANA	DBSCAN
Unsupervised	MAFN-dtw	**81.7**	76.5	70.3	73.9	74.6	72.5
	MAFN-smi	80.7	73.3	70.3	72.6	73.5	72.3
	MAFN-HDI	80.6	75.5	70.3	73.6	74.6	72.3
	wPLI	80.6	75.7	70.3	73.9	73.8	72.3
	CFN	72.1	70.8	69.2	70.2	71.4	69.1
	DCFN	78.7	72.5	69.5	71.9	72.6	71.6

The best-performing methods were highlighted (bold).

TABLE 3 | Comparison results of MAFNs and other functional methods for epilepsy detection.

	Networks	DGP	SVM-RBF	SVM-SIG	SVM-POL	MLP	C4.5
Supervised	MAFN-dtw	92.8	94.6	**95.4**	92.6	92.3	84.4
	MAFN-smi	89.6	90.9	92.7	92.9	93.2	83.2
	MAFN-HDI	92.8	93.4	93.4	93.2	89.3	80.6
	wPLI	92.5	93.3	93.3	94.1	89.2	79.9
	CFN	83.4	85.6	84.3	80.4	85.9	74.3
	DCFN	85.7	89.2	90.5	88.7	88.7	78.3
	Networks	IIC	OC-SVM	SVDD	K-means	DIANA	DBSCAN
Unsupervised	MAFN-dtw	73.3	**77.5**	73.7	72.8	70.3	71.7
	MAFN-smi	73.7	75.4	74.3	74.6	72.3	74.6
	MAFN-HDI	74.6	**77.5**	73.3	72.9	73.6	72.3
	wPLI	73.6	76.3	72.3	72.9	72.8	72.6
	CFN	72.4	70.4	69.7	70.1	69.4	71.3
	DCFN	72.8	74.5	72.2	72.3	70.7	72.0

The best-performing methods were highlighted (bold).

schizophrenia, and healthy controls in [51]. All subjects participate in a simple button-pressing task in which subjects either 1) pressed a button to immediately generated a tone, 2) passively listened to the same tone, or 3) pressed a button without generating a tone to study the corollary discharge in people with schizophrenia, and comparison controls. And 61 channel EEG data were collected from 32 healthy subjects and 49 patients with schizophrenia.

As described in **Section 2**, we construct 6 types of functional networks for each subject and incorporate them into the 12 classifiers. The results are shown in **Table 2**. It is obvious that the accuracy of classifiers involving MAFNs are consistently higher than those involving CFNs and DCFNs, demonstrating the advantage of MAFNs. The highest accuracy achieved by using MAFNs is 92.4% (MAFN-dtw + SVM-POL). Since the wPLI method can avoid the volume conductor effect, wPLIs are more effective than the corresponding 5 other methods in 2 supervised (SVM-SIG and MLP) classifiers, but MAFNs perform better in other 10 classifiers.

Furthermore, similar to the approach discussed in **Section 3.1**, we also reveal the optimal sparsity and the accuracy achieved by using the features of individual channels. The results show that when the sparsity is 30%, the global attribute of schizophrenia networks has the largest difference between groups. Finally, as exhibited in **Figure 5D**, we find that the most relevant electrodes for schizophrenia diagnosis are localized in the frontal and occipital regions.

3.3 Application in Epilepsy Detection

The third task we take to demonstrate the effectiveness of MAFNs is detecting epilepsy. The dataset contains intracranial EEG recordings obtained from patients with temporal lobe epilepsy undergoing evaluation for epilepsic surgery [52]. The 1-s EEG clips labeled "Ictal" for seizure data segments, or "Interictal" for non-seizure data segments. In the present work, 100 "Ictal" and 100 "Interictal" fragments of one subject were selected as experimental data. The 24 intracranial EEG recordings are from depth electrodes implanted along the anterior-posterior axis of the hippocampus, and from subdural electrode grids in various locations.

The results of classifiers involving MAFNs or other functional networks are displayed in **Table 3**. The highest

accuracy achieved by using MAFNs is 95.4% (MAFN-dtw + SVM-SIG). Importantly, these results indicate again that, MAFNs systematically outperform CFNs and DCFNs. Except in SVM-POL and IIC classifiers, MAFNs perform better than or comparably to wPLIs. Furthermore, we also find the optimal sparsity and the accuracy by using the features of individual channels. The results show that when the sparsity is 32%, the global attribute of epilepsy networks has the largest difference between groups.

4 DISCUSSION AND CONCLUSION

4.1 Discussion

Generally speaking, there are two types of brain networks, structural, and functional [44, 53]. The former represents chemical or electrical synapses between neurons, or fibers connecting brain regions or voxels. In these networks the connections are *physical*, meaning that they do not significantly change in a short time interval. In contrast, the later describes the *functional* interactions between neurons or regions. Such interactions can be captured by correlation/coherence or causation of activities of brain region pairs. Due to the temporal nature of brain activity, functional connectivity usually changes over time and exhibits different structural properties in different brain states. Hence, construction approach showing temporal and topological characteristics of brain activity is not only crucial for distinguishing brain states but also helpful for unveiling the systematic mechanism underlying brain functions or dysfunctions.

In this work we demonstrate the advantages of MAFN in identifying three abnormal brain states, it can also be applied to understand our healthy or diseased brain, such as detecting driving-induced fatigue, Alzheimer's disease, depression, and different emotions, etc. In addition, although we focus on MAFNs constructed from EEG recordings, our approach is also applicable to construct functional networks from other types of experimental data, and such as fMRI and fNIRS. Importantly, while scalp-level EEG data are used here, it would be interesting to extend the MAFN method to source-level connectivity [54]. Unfortunately, source reconstruction requires additional experiment data that all the three datasets in the present study lack. Moreover, directed networks (i.e., effective connectivity represents the direct or indirect causal influences of one region on another) can be more informative than undirected ones because link directionality might reveal information flow between different brain regions [55]. Therefore, exploring source-level and directed MAFNs is worth future pursuit.

5 CONCLUSION

In summary, we proposed a two-phase approach for constructing scalp-level functional networks from multiple time series by multilayer-aggregation, and incorporated such networks into a classification framework for identifying brain states and diseases based on EEG recordings. We tested the effectiveness and robustness of the approach in three data sets (fatigue, schizophrenia, and epilepsy) and the results showed that the approach is consistently more advantageous than correlation-based functional networks and also achieves comparable or higher accuracy than phase lag index based networks in most classifiers. With this approach we also revealed the important electrode positions for detecting mental fatigue and diagnosing schizophrenia.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

GY designed the research. W-KC developed the methods. W-KC and X-RQ analyzed the data and results. W-KC and GY wrote the manuscript with inputs from YS and X-RQ.

FUNDING

W-KC and GY are supported by the National Natural Science Foundation of China (Grant Nos. 11875043 and 12161141016), Supported by the Shanghai Municipal Science and Technology Major Project (2021SHZDZX0100) and the Fundamental Research Funds for the Central Universities, Shanghai Municipal Commission of Science and Technology Project (Grant No. 19511132101), and the Fundamental Research Funds for the Central Universities (Grant No. 22120190251). YS is supported by the National Natural Science Foundation of China (Grant No. 81801785) and Zhejiang Lab (Grant No. 2019KE0AD01).

ACKNOWLEDGMENTS

The authors thank Dr. Xiaolei Ru for his helpful discussion.

REFERENCES

1. Qi P, Ru H, Gao L, Zhang X, Zhou T, Tian Y, et al. Neural Mechanisms of Mental Fatigue Revisited: New Insights from the Brain Connectome. *Engineering* (2019) 5:276–86. doi:10.1016/j.eng.2018.11.025
2. Preti MG, Leonardi N, Karahanoglu FI, Grouiller F, Genetti M, Seeck M, et al. Epileptic Network Activity Revealed by Dynamic Functional Connectivity in Simultaneous EEG-fMRI. In: 2014 IEEE 11th International Symposium on Biomedical Imaging (ISBI) (2014). p. 9–12. doi:10.1109/ISBI.2014.6867796
3. Song X, Roy B, Kang DW, Aysola RS, Macey PM, Woo MA, et al. Altered Resting-State Hippocampal and Caudate Functional Networks in Patients with Obstructive Sleep Apnea. *Brain Behav* (2018) 8:e00994. doi:10.1002/brb3.994
4. Jafri MJ, Pearlson GD, Stevens M, Calhoun VD. A Method for Functional Network Connectivity Among Spatially Independent Resting-State

Components in Schizophrenia. *Neuroimage* (2008) 39:1666–81. doi:10.1016/j.neuroimage.2007.11.001
5. Zhang B, Yan G, Yang Z, Su Y, Wang J, Lei T. Brain Functional Networks Based on Resting-State EEG Data for Major Depressive Disorder Analysis and Classification. *IEEE Trans Neural Syst Rehabil Eng* (2021) 29:215–29. doi:10.1109/TNSRE.2020.3043426
6. Vecchio F, Miraglia F, Iberite F, Lacidogna G, Guglielmi V, Marra C, et al. Sustainable method for Alzheimer dementia prediction in mild cognitive impairment: Electroencephalographic connectivity and graph theory combined with apolipoprotein e. *Ann Neurol* (2018) 84:302–14. doi:10.1002/ana.25289
7. Matthews PM, Jezzard P. Functional Magnetic Resonance Imaging. *J Neurol Neurosurg Psychiatry* (2004) 75:6–12.
8. Schomer DL, Da Silva FL. *Niedermeyer's Electroencephalography: Basic Principles, Clinical Applications, and Related fields*. Lippincott Williams & Wilkins (2012).
9. Herman GT. *Fundamentals of Computerized Tomography: Image Reconstruction from Projections*. Springer Science & Business Media (2009).
10. Tóth B, Urbán G, Haden GP, Márk M, Török M, Stam CJ, et al. Large-scale Network Organization of EEG Functional Connectivity in Newborn Infants. *Hum Brain Mapp* (2017) 38:4019–33. doi:10.1002/hbm.23645
11. Hassan M, Wendling F. Electroencephalography Source Connectivity: Aiming for High Resolution of Brain Networks in Time and Space. *IEEE Signal Process Mag* (2018) 35:81–96. doi:10.1109/MSP.2017.2777518
12. Dimitrakopoulos GN, Kakkos I, Dai Z, Wang H, Sgarbas K, Thakor N, et al. Functional Connectivity Analysis of Mental Fatigue Reveals Different Network Topological Alterations between Driving and Vigilance Tasks. *IEEE Trans Neural Syst Rehabil Eng* (2018) 26:740–9. doi:10.1109/TNSRE.2018.2791936
13. Zhou C, Zemanová L, Zamora-López G, Hilgetag CC, Kurths J. Structure–function Relationship in Complex Brain Networks Expressed by Hierarchical Synchronization. *New J Phys* (2015) 9:178. doi:10.1088/1367-2630/9/6/178
14. Medaglia JD, Lynall M-E, Bassett DS. Cognitive Network Neuroscience. *J Cogn Neurosci* (2015) 27:1471–91. doi:10.1162/jocn_a_00810
15. Baum GL, Ciric R, Roalf DR, Betzel RF, Moore TM, Shinohara RT, et al. Modular Segregation of Structural Brain Networks Supports the Development of Executive Function in Youth. *Curr Biol* (2017) 27:1561–72. doi:10.1016/j.cub.2017.04.051
16. Liu Y, Liang M, Zhou Y, He Y, Hao Y, Song M, et al. Disrupted Small-World Networks in Schizophrenia. *Brain* (2008) 131:945–61. doi:10.1093/brain/awn018
17. Zhao ZW, Liu W, Lu BL. Multimodal Emotion Recognition Using a Modified Dense Co-Attention Symmetric Network. In: 2021 10th International IEEE/EMBS Conference on Neural Engineering (NER). (2021). p. 73–76. doi:10.1109/NER49283.2021.9441352
18. Song T, Zheng W, Song P, Cui Z. EEG Emotion Recognition Using Dynamical Graph Convolutional Neural Networks. *IEEE Trans Affective Comput* (2018) 11:1. doi:10.1109/TAFFC.2018.2817622
19. Jalili M, Knyazeva MG. EEG-based Functional Networks in Schizophrenia. *Comput Biol Med* (2011) 41:1178–86. doi:10.1016/j.compbiomed.2011.05.004
20. Tahaei MS, Jalili M, Knyazeva MG. Synchronizability of EEG-Based Functional Networks in Early Alzheimer's Disease. *IEEE Trans Neural Syst Rehabil Eng* (2012) 20:636–41. doi:10.1109/tnsre.2012.2202127
21. Sun Y, Lim J, Meng J, Kwok K, Thakor N, Bezerianos A. Discriminative Analysis of Brain Functional Connectivity Patterns for Mental Fatigue Classification. *Ann Biomed Eng* (2014) 42:2084–94. doi:10.1007/s10439-014-1059-8
22. Gao Z, Zhang K, Dang W, Yang Y, Wang Z, Duan H, et al. An Adaptive Optimal-Kernel Time-Frequency Representation-Based Complex Network Method for Characterizing Fatigued Behavior Using the SSVEP-Based BCI System. *Knowledge-Based Syst* (2018) 152:163–71. doi:10.1016/j.knosys.2018.04.013
23. Daly I, Nasuto SJ, Warwick K. Brain Computer Interface Control via Functional Connectivity Dynamics. *Pattern Recognition* (2012) 45:2123–36. doi:10.1016/j.patcog.2011.04.034
24. Sun Y, Lim J, Kwok K, Bezerianos A. Functional Cortical Connectivity Analysis of Mental Fatigue Unmasks Hemispheric Asymmetry and Changes in Small-World Networks. *Brain Cogn* (2014) 85:220–30. doi:10.1016/j.bandc.2013.12.011
25. Wu X, Zheng WL, Lu B. Identifying Functional Brain Connectivity Patterns for EEG-based Emotion Recognition. In: 2019 9th International IEEE/EMBS Conference on Neural Engineering (NER) (2019). IEEE (2019). p. 235–8. doi:10.1109/NER.2019.8717035
26. Micheloyannis S, Pachou E, Stam CJ, Breakspear M, Bitsios P, Vourkas M, et al. Small-world Networks and Disturbed Functional Connectivity in Schizophrenia. *Schizophrenia Res* (2006) 87:60–6. doi:10.1016/j.schres.2006.06.028
27. Cao C, Slobounov S. Alteration of Cortical Functional Connectivity as a Result of Traumatic Brain Injury Revealed by Graph Theory, ICA, and sLORETA Analyses of EEG Signals. *IEEE Trans Neural Syst Rehabil Eng* (2010) 18:11–9. doi:10.1109/TNSRE.2009.2027704
28. Gonuguntla V, Kim J-H. EEG-based Functional Connectivity Representation Using Phase Locking Value for Brain Network Based Applications. *Annu Int Conf IEEE Eng Med Biol Soc (Embc)* (20202020) 2853–6. doi:10.1109/EMBC44109.2020.9175397 *42nd*
29. Yang S, Ai N, Qiao Y, Wang L, Yu H, Xu G. Brain Functional Network Improved by Magnetic Stimulation at Acupoints during Mental Fatigue. *JBiSE* (2016) 09:65–70. doi:10.4236/jbise.2016.910b009
30. Zhang J, Small M. Complex Network from Pseudoperiodic Time Series: Topology versus Dynamics. *Phys Rev Lett* (2006) 96:238701. doi:10.1103/physrevlett.96.238701
31. Xu X, Zhang J, Small M. Superfamily Phenomena and Motifs of Networks Induced from Time Series. *Proc Natl Acad Sci U S A* (2008) 105:19601–519605. doi:10.1073/pnas.0806082105
32. Stam CJ, Nolte G, Daffertshofer A. Phase Lag index: Assessment of Functional Connectivity from Multi Channel EEG and MEG with Diminished Bias from Common Sources. *Hum Brain Mapp* (2010) 28:1178–93. doi:10.1002/hbm.20346
33. Arslan S, Ktena SI, Makropoulos A, Robinson EC, Rueckert D, Parisot S. Human Brain Mapping: A Systematic Comparison of Parcellation Methods for the Human Cerebral Cortex. *Neuroimage* (2018) 170:5–30. doi:10.1016/j.neuroimage.2017.04.014
34. Cheng Z, Yang Y, Wang W, Hu W, Zhuang Y, Song G. Time2graph: Revisiting Time Series Modeling with Dynamic Shapelets. *Aaai* (2020) 34:3617–24. doi:10.1609/aaai.v34i04.5769
35. King J-R, Sitt JD, Faugeras F, Rohaut B, El Karoui I, Cohen L, et al. Information Sharing in the Brain Indexes Consciousness in Noncommunicative Patients. *Curr Biol* (2013) 23:1914–9. doi:10.1016/j.cub.2013.07.075
36. Deng B, Cai L, Li S, Wang R, Yu H, Chen Y, et al. Multivariate Multi-Scale Weighted Permutation Entropy Analysis of EEG Complexity for Alzheimer's Disease. *Cogn Neurodyn* (2017) 11:217–31. doi:10.1007/s11571-016-9418-9
37. Zhou T, Lü L, Zhang Y-C. Predicting Missing Links via Local Information. *Eur Phys J B* (2009) 71:623–30. doi:10.1140/epjb/e2009-00335-8
38. Barabási AL. *Network Science*. Cambridge University Press (2016).
39. Chen G, Wang X, Li X. *Fundamentals of Complex Networks: Models, Structures and Dynamics*. John Wiley & Sons (2014).
40. Tang D, Du W, Shekhtman L, Wang Y, Havlin S, Cao X, et al. Predictability of Real Temporal Networks. *Natl Sci Rev* (2020) 7:929–37. doi:10.1093/nsr/nwaa015
41. Chen Z, Wu J, Xia Y, Zhang X. Robustness of Interdependent Power Grids and Communication Networks: A Complex Network Perspective. *IEEE Trans Circuits Syst* (2018) 65:115–9. doi:10.1109/tcsii.2017.2705758
42. Zhou C, Zemanová L, Zamora G, Hilgetag CC, Kurths J. Hierarchical Organization Unveiled by Functional Connectivity in Complex Brain Networks. *Phys Rev Lett* (2006) 97:238103. doi:10.1103/physrevlett.97.238103
43. Bullmore E, Sporns O. Complex Brain Networks: Graph Theoretical Analysis of Structural and Functional Systems. *Nat Rev Neurosci* (2009) 10:186–98. doi:10.1038/nrn2575
44. Bassett DS, Sporns O. Network Neuroscience. *Nat Neurosci* (2017) 20:353–64. doi:10.1038/nn.4502
45. Liang X, Wang J, Yan C, Shu N, Xu K, Gong G, et al. Effects of Different Correlation Metrics and Preprocessing Factors on Small-World Brain Functional Networks: A Resting-State Functional MRI Study. *PLoS One* (2012) 7:e32766. doi:10.1371/journal.pone.0032766

46. Cerqueira A, Fraiman D, Vargas CD, Leonardi F. A Test of Hypotheses for Random Graph Distributions Built from EEG Data. *IEEE Trans Netw Sci Eng* (2017) 4:75–82. doi:10.1109/TNSE.2017.2674026
47. Kampffmeyer M, Chen Y, Liang X, Wang H, Zhang Y, Xing EP. Rethinking Knowledge Graph Propagation for Zero-Shot Learning. *Proc IEEE Conf Comp Vis Pattern Recognition* (2019) 11487–96. doi:10.1109/cvpr.2019.01175
48. Ji X, Henriques JF, Vedaldi A. Invariant Information Clustering for Unsupervised Image Classification and Segmentation. *Proc IEEE Int Conf Comp Vis* (2019) 9865–74. doi:10.1109/iccv.2019.00996
49. Manevitz LM, Yousef M. One-class SVMs for Document Classification. *J Machine Learn Res* (2002) 2:139–54.
50. Tax DMJ, Duin RPW. Support Vector Data Description. *Machine Learn* (2004) 54:45–66. doi:10.1023/b:mach.0000008084.60811.49
51. Ford JM, Palzes VA, Roach BJ, Mathalon DH. Did I Do that? Abnormal Predictive Processes in Schizophrenia when Button Pressing to Deliver a Tone. *Schizophrenia Bull* (2014) 40:804–12. doi:10.1093/schbul/sbt072
52. Andriy T, Achintya S, Gordon L. Detection of Seizures in Intracranial EEG: Upenn and mayo Clinic's Seizure Detection challenge. In: 2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). IEEE (2015). p. 6582–5.
53. Ponten SC, Daffertshofer A, Hillebrand A, Stam CJ. The Relationship between Structural and Functional Connectivity: Graph Theoretical Analysis of an EEG Neural Mass Model. *Neuroimage* (2010) 52:985–94. doi:10.1016/j.neuroimage.2009.10.049
54. Hassan M, Wendling F. Electroencephalography Source Connectivity: Aiming for High Resolution of Brain Networks in Time and Space. *IEEE Signal Process Mag* (2018) 35:81–96. doi:10.1109/msp.2017.2777518
55. Dimitrakopoulos GN, Kakkos I, Dai Z, Wang H, Sgarbas K, Thakor N, et al. Functional Connectivity Analysis of Mental Fatigue Reveals Different Network Topological Alterations between Driving and Vigilance Tasks. *IEEE Trans Neural Syst Rehabil Eng* (2018) 26:740–9. doi:10.1109/tnsre.2018.2791936

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

frontiers in Physics

ORIGINAL RESEARCH
published: 21 January 2022
doi: 10.3389/fphy.2021.805674

A Novel Metric to Quantify the Real-Time Robustness of Complex Networks With Respect to Epidemic Models

Bo Song[1], Guo-Ping Jiang[2], Yurong Song[2], Junming Yang[1], Xu Wang[3] and Y. Jay Guo[3]*

[1]School of Modern Posts, Nanjing University of Posts and Telecommunications, Nanjing, China, [2]College of Automation, Nanjing University of Posts and Telecommunications, Nanjing, China, [3]Global Big Data Technologies Centre, University of Technology Sydney, Sydney, NSW, Australia

Spread velocity, epidemic threshold, and infection density at steady state are three non-negligible features describing the spread of epidemics. Combining these three features together, a new network robustness metric with respect to epidemics was proposed in this paper. The real-time robustness of the network was defined and analyzed. By using the susceptible–infected (SI) and susceptible–infected–susceptible (SIS) epidemic models, the robustness of different networks was analyzed based on the proposed network robustness metric. The simulation results showed that homogeneous networks present stronger robustness than do heterogeneous networks at the early stage of the epidemic, and the robustness of the heterogeneous networks becomes stronger than that of the homogeneous ones with the progress of the epidemic. Moreover, the irregularity of the degree distribution decreases the network robustness in homogeneous networks. The network becomes more vulnerable as the average degree grows in both homogeneous and heterogeneous networks.

Keywords: real-time robustness, epidemic spread, spread velocity, complex network, robustness metrics

OPEN ACCESS

Edited by:
Gaogao Dong,
Jiangsu University, China

Reviewed by:
Haiyan Wang,
Arizona State University, United States
Hongyong Zhao,
Nanjing University of Aeronautics and Astronautics, China

****Correspondence:***
Yurong Song
songyr@njupt.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *30 October 2021*
Accepted: *07 December 2021*
Published: *21 January 2022*

Citation:
Song B, Jiang G-P, Song Y, Yang J, Wang X and Guo YJ (2022) A Novel Metric to Quantify the Real-Time Robustness of Complex Networks With Respect to Epidemic Models. Front. Phys. 9:805674. doi: 10.3389/fphy.2021.805674

INTRODUCTION

Nowadays, various dynamic phenomena exist in real networks, many of which are harmful and bring great damage to real life. Especially, the threat of infectious diseases is growing increasingly due to the increasing complexity of modern social networks in all facets of human endeavor [1–5]. For example, as reported by the WHO on October 29, 2021, there have been more than 245 million confirmed cases of coronavirus disease 2019 (COVID-19) globally, including almost 5 million deaths (https://covid19.who.int/). Also, other fields like economy, politics, and culture have suffered extensive damages during the outbreak of COVID-19. Since network structures show a great impact on the propagation dynamics [6–9, 11], it is crucial to assess the robustness of different network structures with respect to the spread.

Epidemic propagation models have been recently used to analyze network robustness against virus attacks, and the robustness of different networks has been studied [10–14]. By modeling and analyzing the epidemic propagation, the descriptive features of the propagation process are often used to measure network robustness against the epidemic spread. For example, the epidemic threshold and the final infection rate at the steady state have been used to measure the robustness of the network against virus attacks individually or jointly [13]. The results of network robustness with

respect to epidemics can help in understanding and further improving network robustness against epidemics.

Although the existing measurements have been proven to be effective for network robustness when it comes to the spread of epidemics, some inherent challenges have been overlooked. Firstly, the existing measurements have mainly focused on the robustness of the network at the steady state. To our knowledge, the real-time robustness of complex networks with respect to epidemics has not been widely studied, i.e., the changes in the network robustness over time in different network structures have not been explored. Secondly, it is not accurate to measure network robustness without considering the spread velocity, which is an important factor in measuring the spread of epidemics. Therefore, the robustness of the network against epidemics can be comprehensively and accurately measured by considering the spread velocity. Furthermore, the spread velocity describes the changes in the propagation over time, which is very suitable for measuring the real-time network robustness with respect to epidemics [17].

In this paper, combining spread velocity, infection density at steady state, and the epidemic threshold, a novel metric was proposed to measure real-time robustness with respect to epidemics in complex networks. Network robustness with respect to the spread of the susceptible–infected (SI) [15] and susceptible–infected–susceptible (SIS) models [16] was analyzed based on the new metric, and some interesting results are presented in our paper. Firstly, the results confirmed that the irregularity of the degree distribution strengthens the network's vulnerability with respect to the epidemic in homogeneous networks. However, the simulation results on the real-time robustness of the different networks showed that the robustness of the Barabási–Albert (BA) scale-free network [19] is not always stronger than that of the Watts–Strogatz (WS) network [20] at any time, which was different from the results of existing studies. At the early stage of the epidemic, the BA network is more fragile than the WS network. As the infection rate worsens, the BA network becomes more robust than the WS network. Moreover, the simulation results showed that the network becomes more vulnerable to the epidemic as the average degree grows in both homogeneous and heterogeneous networks.

The rest of this paper is organized as follows. *Related Work* presents the literature review and related works. In *Network Robustness With Respect to Epidemic Models*, we analyze the necessity of proposing the new metric to measure the network robustness against diseases. In *The Novel Metric to Quantify Network Robustness*, the novel metric to quantify the network robustness with respect to the SI/SIS epidemic spread is proposed. The simulation results in different networks are presented and analyzed in *Results*, and the main conclusions and the direction for future studies are summarized in *Discussion*.

RELATED WORK

Epidemics in social networks can be theoretically described using biological epidemic models, through which the spread

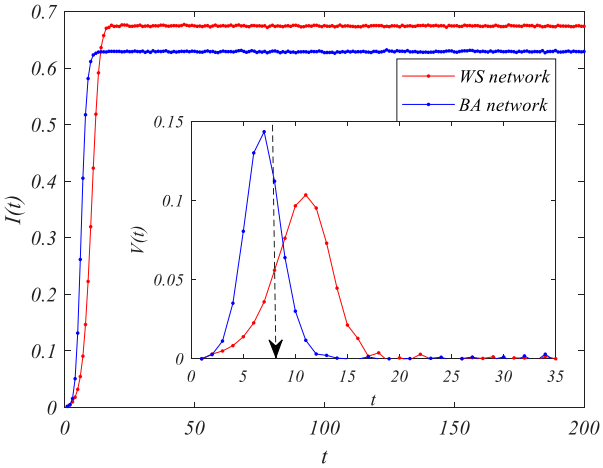


FIGURE 1 | The susceptible–infected–susceptible (SIS) epidemic spreading process in different networks, $\beta = \delta = 0.3$. $I(t)$ represents the fraction of infected nodes at time t and $V(t)$ the growth rate of infection at time t.

mechanism of viruses can be described and analyzed. For example, the SI and SIS epidemic models are often used to model the spread of epidemics [13–17]. In the SI model, the S-state nodes can pass to the infected state through contagion by the infected ones, and the rate of an S-state node being infected by a single infected neighbor is β. In the SIS model, the I-state node recovered to the S state at the rate δ in the SIS model, and the ratio between β and δ is denoted the effective infection rate τ. The time evolution of the different states of the nodes can be described using differential equations from which the relevant conclusions of epidemics can be derived.

In the complex network theory, three important features describing the epidemic spread were introduced into the epidemic models. Firstly, the epidemic threshold τ_c, as a function of the basic reproductive number R_0, was used to determine the outbreak of the epidemic [21]. When the effective infection rate τ is higher than τ_c, i.e., $R_0 > 1$, the epidemic spreads in the population, but when the effective infection rate τ is lower than τ_c, the epidemic dies out. With the outbreak of the epidemic, the states of the nodes in the network change with time, and the changing rate can be measured by the spread velocity. When the network reaches a stable state, the density of each state in the network becomes stable, and the final infection rate at the steady state can be used to measure the scale of the spread.

Therefore, the epidemic threshold, spread velocity, and the final infection rate at the steady state can comprehensively describe the propagation mechanism and can also be used as a measure of network robustness with respect to epidemics. As one of the most prominent features, the epidemic threshold is the first and commonly used measure of network robustness with respect to the epidemic spread [22, 23]. The larger the threshold, the more difficult it is to spread the virus, i.e., the more robust a network is against the virus attack [13]. Studies have found that the threshold cannot fully measure network robustness. For example, the Erdős–Rényi (ER) network [18] and the BA

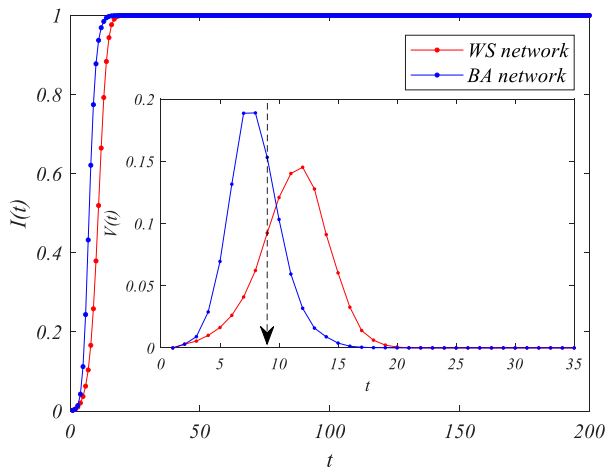


FIGURE 2 | The susceptible–infected (SI) epidemic spreading process in different networks, $\beta = 0.3$. $I(t)$ represents the fraction of infected nodes at time t and $V(t)$ the growth rate of infection at time t.

network [19] have two opposing features—the epidemic threshold and the steady-state infection rate—to measure their robustness. In [13], a new measure incorporating the fraction of infected nodes at the steady state and the epidemic threshold to assess the robustness of the complex networks with respect to the spread of epidemic has been proposed and proven to be effective in modeling epidemics with different final infection densities.

NETWORK ROBUSTNESS WITH RESPECT TO EPIDEMIC MODELS

In existing studies, the epidemic threshold and the steady-state infection rate have been bound together to measure network robustness against epidemics since it has been proven that the results are inaccurate when only one feature is considered. Besides the epidemic threshold and the steady-state infection rate, the spread velocity is another widely discussed variable that should not be ignored in the study of network robustness. For example, **Figure 1** shows the infection rate at the nodes at time t due to the SIS epidemic spreading process in the WS and BA networks, where the average degree of the two networks is the same. We can differentiate between the propagation processes in the two networks from the curve in **Figure 1**. Firstly, the final infection density in the BA network (I_{BA}) is smaller than that in the WS network (I_{WS}), i.e., $I_{WS} > I_{BA}$. Based solely on the infection scale at the steady state, we can conclude that the BA network is more robust than the WS network.

However, the performance of spread velocity is more interesting than that of the final propagation scale. In our simulation, we first described the spread velocity as the growth of the infection rate, i.e., $V(t) = I(t+1) - I(t)$. As shown in **Figure 1**, when $t < 9$, the spread velocity of the epidemic in the WS network is slower than that of the BA network, i.e., $V(t)_{BA} > V(t)_{WS}$. However, when $t \geq 9$, the spread velocity of the epidemic in the WS network is faster than that of the BA network, i.e., $V(t)_{BA} < V(t)_{WS}$. Especially, when the final infection densities at the steady state are the same, such as in the SI model shown in **Figure 2**, we can hardly conclude which network shows stronger robustness based solely on the spread velocity. Therefore, estimating the robustness of different networks based solely on the spread velocity is different, which is one of the reasons to study real-time network robustness. In addition, since the spread velocity describes the dynamics of the propagation process before attaining the steady state, it is essential in measuring real-time network robustness.

Moreover, we also measured the moment at which the steady state of the infection first arrives [$T(i\_\max)$] under different infection rates β in the BA and WS networks. **Figure 3** shows that the $T(i\_\max)$ in the WS network was larger than that in the BA network under the same β, especially when β was very small. Therefore, we can conclude that one single feature may fail to comprehensively measure the robustness of the network. Besides the epidemic threshold, the infection rate at the steady state and the spread velocity are also very important in measuring network robustness with respect to epidemics. Therefore, we proposed a novel metric with multiple features to quantify network robustness against the spread of the epidemic in this paper.

NOVEL METRIC TO QUANTIFY NETWORK ROBUSTNESS

We proposed a multi-indicator-based measurement to quantify network robustness against the epidemic by combining the epidemic threshold, the infection density at steady state, and the spread velocity. Suppose that, in the SIS epidemic model, the rate of a susceptible node being infected by a single infected neighbor is β and the infected node recovered at the rate δ in the SIS model. When $\delta = 0$, the SIS model is transformed into the SI model. In the SIS model, the effective recovery rate can be defined as $s = 1/\tau = \delta/\beta$, $s \in (0, \lambda_{\max})$. The density of the infected nodes

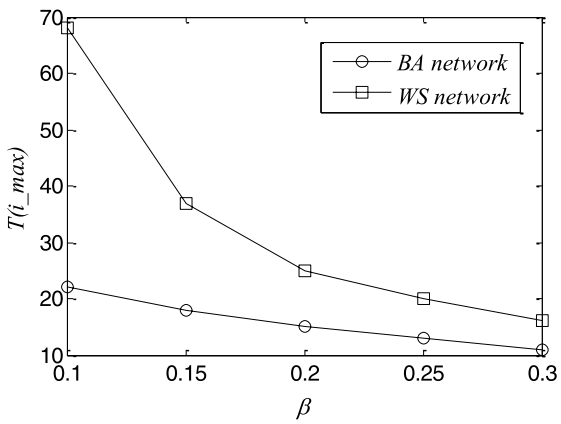


FIGURE 3 | The time of reaching the steady states of the epidemic spread under different infection rates in the Barabási–Albert (BA) and Watts–Strogatz (WS) networks.

at time t is described as $i(t)$, and the steady state of the infection under the effective infection rate τ can be written as $i_\infty(\tau)$. Considering the infection at the steady state and the spread velocity, we define $i^A(T)$ as the average infection rate of the network after time T:

$$i^A(T) = \frac{1}{T}\int_0^T i(t)dts. \tag{1}$$

The network robustness with respect to the epidemic spread can be written as

$$R_G = \int_0^{\lambda_{\max}} i^A(s)ds. \tag{2}$$

Equation 2 shows that the greater the value of R_G, the more fragile is the network, i.e., the weaker is its robustness.

The real-time robustness of network G can be written as

$$R_G(T) = \frac{1}{T}\int_0^{\lambda_{\max}}\int_0^T i(t,s)dtds. \tag{3}$$

Especially, when $T \to \infty$,

$$i^A(T) = \frac{1}{T}\int_0^T i(t)dt = \frac{1}{T}\left(\int_0^{T_s} i(t)dt + \int_{T_s}^{\infty} i_\infty dt\right) \approx i_\infty, \tag{4}$$

where T_s represents the moment when the infection reaches a steady state for the first time. Then, the network robustness can be written as

$$R_G = \int_0^{\lambda\ \max} i_\infty(s)ds, \tag{5}$$

which is the viral conductance proposed in **Eq. 13**.

Based on the SI and SIS epidemic models, we can further write the robustness of the network with respect to the spread of the SI and SIS epidemic models.

Case 1

The robustness of homogeneous networks with respect to the spread of the SI model is shown. The state of each node in the SI model is either infected or healthy, and the change in infected individuals over time can be described as

$$\frac{di}{dt} = \beta\langle k\rangle i(1-i). \tag{6}$$

By separating the variables, **Eq. 6** can be written as

$$\frac{di}{i(1-i)} = \beta\langle k\rangle dt, \tag{7}$$

Integrating both sides of **Eq. 7**, we can obtain

$$\ln\frac{1-i(t)}{i(t)} = -\beta\langle k\rangle t + c. \tag{8}$$

The density of the infected nodes at time t can be written as

$$i(t) = \frac{1}{1+\left(1/i_0 - 1\right)e^{-\beta\langle k\rangle t}}. \tag{9}$$

The final infection density of the SI model is equal to 1, i.e., $i_\infty = 1$. Based on **Eqs. 5** and **9**, the robustness of the homogeneous network G with respect to the spread of the SI epidemic can be written as

$$\begin{aligned} R_G^{SI}(T) &= \frac{1}{T}\int_0^1\int_0^T i(t,\beta)dtd\beta = \frac{1}{T}\int_0^1\int_0^T \frac{1}{1+\left(1/i_0-1\right)e^{-\beta\langle k\rangle t}}dtd\beta \\ &= \frac{1}{T}\int_0^1\int_0^T\left(1 - \frac{\left(1/i_0-1\right)e^{-\beta\langle k\rangle t}}{1+\left(1/i_0-1\right)e^{-\beta\langle k\rangle t}}\right)dtd\beta \end{aligned} \tag{10}$$

$$\begin{aligned} R_G^{SI}(T) &= \frac{1}{T}\int_0^1\int_0^T\left(1 - \frac{\left(1/i_0-1\right)e^{-\beta\langle k\rangle t}}{1+\left(1/i_0-1\right)e^{-\beta\langle k\rangle t}}\right)dtd\beta \\ &= \frac{1}{T}\int_0^1\left(\int_0^T 1dt - \int_0^T \frac{\left(1/i_0-1\right)e^{-\beta\langle k\rangle t}}{1+\left(1/i_0-1\right)e^{-\beta\langle k\rangle t}}dt\right)d\beta \\ &= \frac{1}{T}\int_0^1\left(t + \frac{1}{\beta\langle k\rangle}\ln\left(1+\left(1/i_0-1\right)e^{-\beta\langle k\rangle t}\right)\right)\Big|_{t=0}^{t=T}d\beta \\ &= \frac{1}{T}\int_0^1\left(T + \frac{1}{\beta\langle k\rangle}\ln\frac{\left(1+\left(1/i_0-1\right)e^{-\beta\langle k\rangle T}\right)}{1/i_0}\right)d\beta \\ &= 1 + \frac{1}{T}\int_0^1\left(\frac{1}{\beta\langle k\rangle}\ln\left(i_0 + (1-i_0)e^{-\beta\langle k\rangle T}\right)\right)d\beta. \end{aligned} \tag{11}$$

Case 2

The robustness of homogeneous networks with respect to the spread of the SIS model is calculated. Ignoring the degree of correlations in the nodes of the homogeneous networks, the density of the infected nodes at time t in the SIS epidemic model, i.e., $i(t)$, satisfies

$$\frac{di}{dt} = -\delta i + \beta\langle k\rangle i(1-i). \tag{12}$$

Integrating both sides of **Eq. 12**,

$$\int_0^t dt = \int_{i_0}^{i(t)} \frac{1}{-\delta i + \beta\langle k\rangle i(1-i)}di, \tag{13}$$

Then, **Eq. 13** can be rewritten as

$$t = \frac{1}{\beta\langle k\rangle - \delta}\int_{i_0}^{i(t)}\frac{1}{i}di + \frac{\beta\langle k\rangle}{\beta\langle k\rangle - \delta}\int_{i_0}^{i(t)}\frac{1}{\beta\langle k\rangle - \beta\langle k\rangle i - \delta}di, \tag{14}$$

We can obtain

$$e^{(\beta\langle k\rangle-\delta)t} = \frac{i(t)}{\beta\langle k\rangle - \beta\langle k\rangle i(t) - \delta}\Big/\frac{i_0}{\beta\langle k\rangle - \beta\langle k\rangle i_0 - \delta}, \tag{15}$$

After a simple combination, **Eq. 15** can be rewritten as

$$i(t)\left(\beta\langle k\rangle - \beta\langle k\rangle i_0 - \delta\right) = i_0 e^{(\beta\langle k\rangle-\delta)t}\left(\beta\langle k\rangle - \beta\langle k\rangle i(t) - \delta\right). \tag{16}$$

The density of the infected nodes at time t can be written as

$$i(t) = \frac{(\beta\langle k\rangle - \delta)i_0 e^{(\beta\langle k\rangle-\delta)t}}{\beta\langle k\rangle - \beta\langle k\rangle i_0 - \delta + i_0\beta\langle k\rangle e^{(\beta\langle k\rangle-\delta)t}}. \quad (17)$$

Let **Eq. 12** be equal to 0. We can obtain $-\delta i + \beta\langle k\rangle i(1-i) = 0$. When $\tau = \frac{\beta}{\delta} = \beta > \tau_c$, the infection density of the final stable state is

$$i_\infty = 1 - \frac{\delta}{\beta\langle k\rangle} = 1 - \frac{1}{\tau\langle k\rangle}. \quad (18)$$

Based on **Eqs. 5** and **17**, the robustness of the homogeneous network G with respect to the spread of the SIS epidemic can be written as

$$\begin{aligned} R_G^{SIS}(T) &= \frac{1}{T}\int_0^{\lambda_{\max}}\int_0^T i(t,s)dtds \\ &= \frac{1}{T}\int_0^{\lambda_{\max}}\int_0^T \frac{\left(\frac{\langle k\rangle}{s}-1\right)i_0 e^{\left(\frac{\langle k\rangle}{s}-1\right)t}}{\frac{\langle k\rangle}{s} - \frac{\langle k\rangle}{s}i_0 - 1 + i_0\frac{\langle k\rangle}{s}e^{\left(\frac{\langle k\rangle}{s}-1\right)t}}dtds \end{aligned} \quad (19)$$

Using simple operational processes, $R_G^{SIS}(T)$ can be rewritten as

$$\begin{aligned} R_G^{SIS}(T) &= \frac{1}{T}\int_0^{\lambda_{\max}}\int_0^T \frac{\left(\frac{\langle k\rangle}{s}-1\right)i_0 e^{\left(\frac{\langle k\rangle}{s}-1\right)t}}{\frac{\langle k\rangle}{s} - \frac{\langle k\rangle}{s}i_0 - 1 + i_0\frac{\langle k\rangle}{s}e^{\left(\frac{\langle k\rangle}{s}-1\right)t}}dtds \\ &= \int_0^{\lambda_{\max}}\frac{s}{T\langle k\rangle}\int_0^T \frac{1}{\frac{\langle k\rangle}{s} - \frac{\langle k\rangle}{s}i_0 - 1 + i_0\frac{\langle k\rangle}{s}e^{\left(\frac{\langle k\rangle}{s}-1\right)t}}d\left(\frac{\langle k\rangle}{s} - \frac{\langle k\rangle}{s}i_0 - 1 + i_0\frac{\langle k\rangle}{s}e^{\left(\frac{\langle k\rangle}{s}-1\right)t}\right)ds \\ &= \int_0^{\lambda_{\max}}\frac{s}{T\langle k\rangle}\ln\left(\frac{\langle k\rangle}{s} - \frac{\langle k\rangle}{s}i_0 - 1 + i_0\frac{\langle k\rangle}{s}e^{\left(\frac{\langle k\rangle}{s}-1\right)t}\right)\Big|_{t=0}^{t=T}ds \\ &= \int_0^{\lambda_{\max}}\frac{s}{T\langle k\rangle}\left(\ln\left(\langle k\rangle - \langle k\rangle i_0 - s + i_0\langle k\rangle e^{\left(\frac{\langle k\rangle}{s}-1\right)T}\right) - \ln(\langle k\rangle - s)\right)ds. \end{aligned} \quad (20)$$

RESULTS

Based on the new network robustness measurement we proposed, Monte Carlo simulations were performed to further explore the robustness of the different networks with respect to the spread of the epidemic. It is generally known that most of the real-world networks are characterized by a high clustering effect, a short average path length, and power law node degree distribution, i.e., small-world phenomenon and scale-free property. Therefore, WS small-world networks, BA scale-free networks, and several real-world networks were used in our simulations. All the simulation results were averaged over 500 runs.

Firstly, the BA and WS networks, with the same average degree, $\langle k\rangle = 6$, were used in our simulation to study the effect of degree distribution on the robustness of the networks. **Figure 4** shows the network robustness R_G^{SIS} at time T with respect to the spread of the SIS model. For simplicity, the recovery rate δ was set as 1. The curves in

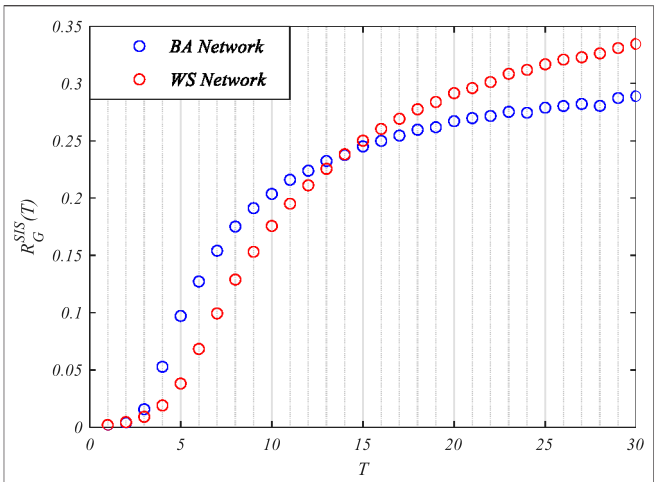


FIGURE 4 | The robustness of the Watts–Strogatz (WS) and Barabási–Albert (BA) networks with respect to the susceptible–infected–susceptible (SIS) epidemic model.

Figure 4 show that, when $T < 15$, $R_{BA}^{SIS} > R_{WS}^{SIS}$, i.e., the robustness of the WS network is stronger than that of the BA network. Due to the existence of a small fraction of hub nodes, the epidemic in the BA network is more likely to break out than that in the WS network. Therefore, at the early stage of the epidemic, the BA network is more fragile than the WS network because of the higher epidemic threshold and faster spread velocity. However, when the infection rate becomes more severe, the spread gradually slows down since most of the nodes in the BA network are of a lower degree than that of the average, and the infection scale in the WS network becomes larger than that in the BA network. Therefore, when $T \geq 15$, the WS network becomes more fragile than the BA network, i.e., $R_{BA}^{SIS} < R_{WS}^{SIS}$, as shown in **Figure 4**.

Moreover, the simulations were carried out in a group of WS small-world networks, where the irregularity/randomness of the networks increases as the value of the rewiring rate p grows following the generation algorithm of the WS network. Especially, when $p = 0$, the network is a regular graph; when $p = 1$, the network is completely random. **Figure 5** shows that, as p grows, R_G^{SIS} becomes larger; that is, the network becomes more vulnerable. Therefore, the irregularity/randomness of the network weakens the robustness of the homogeneous networks. In addition, compared with the robustness of the BA network (red circle), the homogeneous networks were more robust than the BA network at the early stage of the epidemics ($T < 8$ in **Figure 5**). Also, after $T > 15$, the BA network showed better robustness than the group of homogeneous networks. The results further extend our conclusion that, in the initial stage of propagation, the homogeneous networks showed better robustness than the heterogeneous networks. As the robustness gap grew smaller with the spread of the epidemic, and finally, the heterogeneous networks became more robust than the homogenous networks.

The above simulation results indicated that it is not adequate to simply conclude which network is more robust

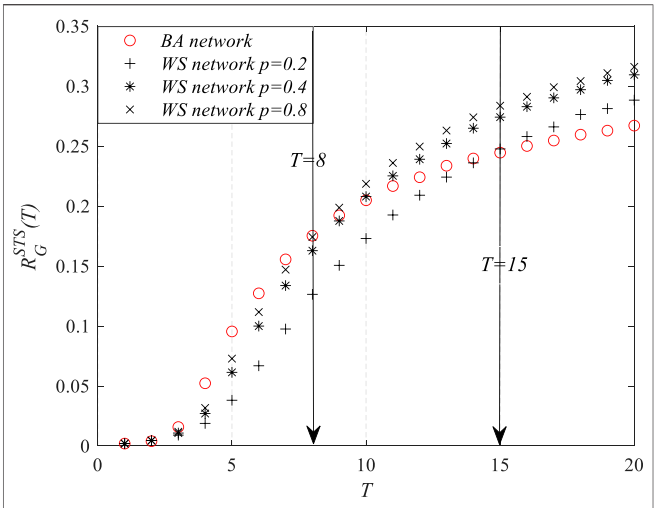


FIGURE 5 | The robustness of homogeneous networks at time T with respect to the susceptible–infected–susceptible (SIS) epidemic spread.

with respect to the epidemic. The robustness of the network changes with time, and the network does not always show a strong/weak robustness at all stages of the epidemic. During the early stage of the epidemic spread, the robustness of homogeneous networks was stronger than that of the heterogeneous networks. After the propagation reached the steady state, heterogeneous networks showed better robustness than the homogeneous networks.

To analyze the impact of the degree distribution on network robustness with respect to the epidemic, simulations were also carried out in the WS and BA networks with different average degrees, $\langle k \rangle$, as shown in **Table 1** and **Figure 6**. **Table 1** shows that, at the steady state ($T = 30$), the network became more vulnerable to virus attacks as the average degree of the network increases. The results validated the BA network as having stronger robustness than the WS network at the steady state.

Figure 6 shows the changes of network robustness as time T increased in the WS and BA networks with different average degrees, $\langle k \rangle$. The figure shows that the WS network exhibited stronger robustness than did the BA network with the same average degree at the early stage of the epidemic, and the robustness of the BA network was stronger than that of the WS network at the steady state.

We also applied the proposed metric to real-world networks where the dynamics processes can be described by epidemic models [24–27]. For example, the virus spread in e-mail networks, the information transfer in neural networks, and rumor diffusion in online social networks. In this paper, three real-world networks were used to validate our results on network models [28]: 1) e-mail network—the network of e-mail interchanges between members of the University Rovira i Virgili (Tarragona); 2) neural network—the network representing the neural network of *Caenorhabditis elegans*, which was compiled by D. Watts and S. Strogatz; and 3) Facebook network—the complete

TABLE 1 | The robustness of the Watts–Strogatz (WS) and Barabási–Albert (BA) networks with different <*k*> values at the steady state (T = 30)

	<*k*> = 4	**<*k*> = 6**	**<*k*> = 8**	**<*k*> = 10**
WS network	*0.2981*	*0.3492*	*0.3716*	*0.3842*
BA network	*0.2274*	*0.2880*	*0.3209*	*0.3488*

WS, *Watts–Strogatz;* BA, *Barabási–Albert*
(<k>) is the average degree of network.

Facebook network data (from a single-time snapshot in September 2005) of Caltech. Only intra-college links were included. The basic topological properties of these three networks are shown in **Table 2**. In order to study the impact of degree distribution on the robustness of real-world networks, new network models were created by rewiring the links in the real-world networks. After rewiring, the heterogeneity of the degree distribution of nodes was reduced, while the numbers of nodes and links remained unchanged, and the new created networks were connected graphs.

Figure 7 shows the impact of degree distribution on the robustness of real-world networks with respect to the spread of the SIS epidemic. We can see that, at the early stage of the epidemics, the robustness of the real-world networks (red circles) was worse than that of the new created network models (black circles). That is to say, the heterogeneity of the degree distributions of nodes can reduce the network robustness at the early stage of the epidemic. After the propagation reached a steady state, the robustness of the real-world networks (red circles) became stronger than that of the new created network models (black circles). The simulation results confirmed that homogeneous networks present stronger robustness than do heterogeneous networks at the early age of the epidemic, and the robustness of the heterogeneous networks becomes stronger than that of the homogeneous ones with the progress of the epidemic. In addition, we can see from **Figure 7** that the time point when the robustness of the real networks was stronger than that of the homogeneous networks was becoming earlier with the increase of the average degree (as shown in **Table 2**, the average degree was becoming larger from the e-mail network to the Facebook network, i.e., from **Figures 7A–C**).

In summary, the simulation showed different results from previous studies based on the new measures of network robustness with respect to the spread of epidemic proposed in this paper. Firstly, the robustness of the heterogeneous networks was not always better than that of the homogeneous networks. During the initial stage of propagation, the homogeneous networks showed better robustness than did the heterogeneous networks, and at the steady state, the heterogeneous networks became more robust than the homogenous networks. Furthermore, in both homogeneous and heterogeneous networks, the networks became more vulnerable as the average degree increased. In homogeneous networks, the robustness of the networks with respect to the spread of the virus decreased as p increased, i.e., the irregularity in the networks increased the vulnerability

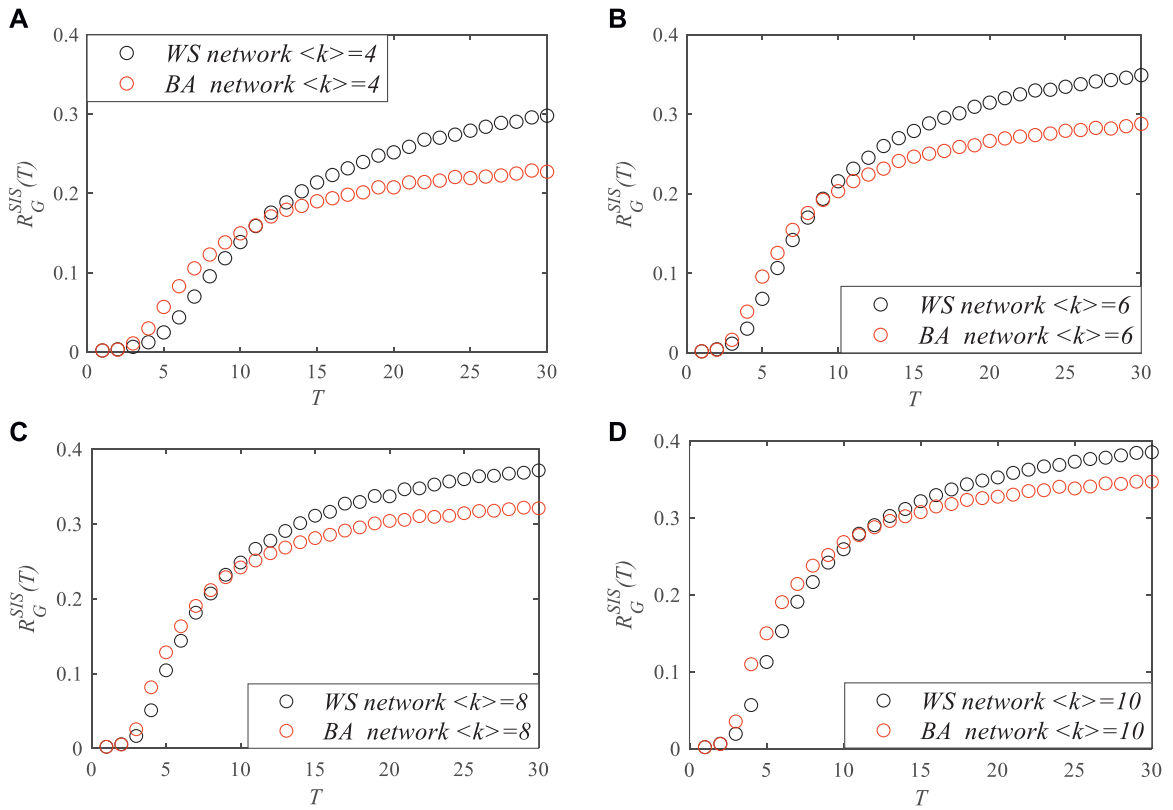


FIGURE 6 | The robustness of the Watts–Strogatz (WS) and Barabási–Albert (BA) networks with different <*k*> values at time *T* with respect to the susceptible–infected–susceptible (SIS) epidemic spread. **(A)** <*k*> = 4. **(B)** <*k*> = 6. **(C)** <*k*> = 8. **(D)** <*k*> = 10.

TABLE 2 | The real-world networks studied and their basic properties

Networks	*N*	*L*	<*k*>	*k*_max
E-mail network	1,133	5,451	9.62	71
Neural network	297	2,148	14.47	134
Facebook network	762	16,651	43.70	248

N *and* L *are the total numbers of nodes and links, respectively.* <k> *and* k_*max denote the average and the maximum degree, respectively.*

of the networks. The simulation results provided us with some ideas to enhance the network robustness with respect to the dynamic propagation processes. For example, at the beginning of the epidemic, mass gathering was harmful to improve network robustness, and after the epidemic entered a relatively stable period, avoiding small-scale clustering would help enhance the network robustness against epidemic spread.

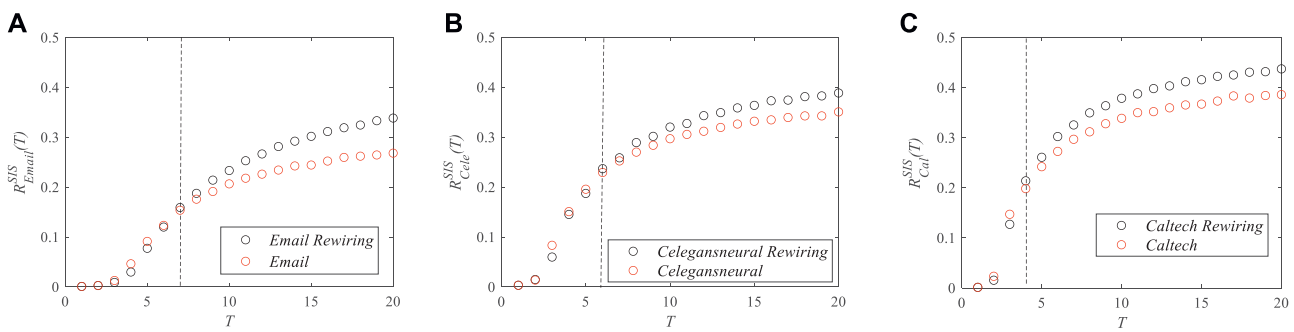


FIGURE 7 | The robustness of real-world networks at time *T* with respect to the susceptible–infected–susceptible (SIS) epidemic spread. **(A)** E-mail network. **(B)** Neural network. **(C)** Facebook network.

DISCUSSION

Considering the spread velocity, epidemic threshold, and the infection density at steady state, a novel metric to quantify network robustness with respect to epidemics was proposed in this paper. The real-time network robustness and the robustness of different networks were discussed. The simulation results showed some interesting conclusions of the impact of network structure on network robustness. The robustness of heterogeneous networks was not always stronger than that of the homogeneous networks. At the early stage of the epidemic, the homogeneous networks showed stronger robustness than did the heterogeneous networks, and at the steady state, the robustness of the heterogeneous networks was stronger than that of the homogeneous networks. In addition, the increase of irregularity and the average degree can enhance the network robustness with respect to epidemics. Our future work will explicitly focus on proposing a heuristic for computing the robustness metric for general networks. In addition, the metric proposed in our paper can be applied to network optimization to maximize network robustness with respect to different kinds of dynamic propagation processes.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material. Further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

BS was responsible for all aspects of the work. G-PJ provided the ideas for the analysis of the robustness of the real-time networks. YS and YG contributed to the analysis of the robustness of the real-time networks. JY contributed to the simulations in *Results*. XW contributed to the analysis of simulations in *Results*.

FUNDING

This work was supported by the Natural Science Foundation of Jiangsu Provence (grant no. SJ220036), the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (grant no. TJ220032), the Scientific research start-up fund of NJUPT (grant no. NY219169), and the National Natural Science Foundation of China (grant no. 61802155). This research was partially supported by School of Modern Posts at Nanjing University of Posts and Telecommunications.

ACKNOWLEDGMENTS

The authors would like to thank the participating colleges for the helpful discussion.

REFERENCES

1. Pastor-Satorras R, Vespignani A. Epidemic Dynamics and Endemic States in Complex Networks [J]. *Phys Rev E Stat Nonlin Soft Matter Phys* (2001) 63(2):066117. doi:10.1103/PhysRevE.63.066117
2. Boguñá M, Pastor-Satorras R. Epidemic Spreading in Correlated Complex Networks [J]. *Phys Rev E Stat Nonlinear Soft Matter Phys* (2002) 66(4 Pt 2): 047104.
3. Mata AS. An Overview of Epidemic Models with Phase Transitions to Absorbing States Running on Top of Complex Networks [J]. *Chaos* (2021) 31(1):012101. doi:10.1063/5.0033130
4. Zhu J, Jiang Y, Li T, Li H, Liu Q. Trend Analysis of COVID-19 Based on Network Topology Description [J]. *Front Phys* (2020) 8:517. doi:10.3389/fphy.2020.564061
5. Muoz NG, Thomson MC, Stewart-Ibarra AM, Vecchi GA, Chourio X, Nájera P, et al. Could the Recent Zika Epidemic Have Been predicted? [J]. *Front Microbiol* (2017) 8:1291. doi:10.3389/fmicb.2017.01291
6. Battiston F, Cencetti G, Iacopini I, Latora I, Lucas M, Patania A, et al. Networks bxeyond Pairwise Interactions: Structure and Dynamics [J]. *Phys Rep* (2020) 874:1–92. doi:10.1016/j.physrep.2020.05.004
7. Shang Y. Subgraph Robustness of Complex Networks under Attacks [J]. *IEEE Trans Syst Man Cybern, Syst* (2019) 49(4):821–32. doi:10.1109/tsmc.2017.2733545
8. Martin C, Niemeyer P. Influence of Measurement Errors on Networks: Estimating the Robustness of Centrality Measures [J]. *Net Sci* (2019) 7(2): 180–95. doi:10.1017/nws.2019.12
9. Hay JA, Kennedy-Shaffer L, Kanjilal S, Lennon NJ, Gabriel SB, Lipsitch M, et al. Estimating Epidemiologic Dynamics from Single Cross-Sectional Viral Load Distributions [J]. *medRxiv: preprint server Health Sci* (2020) doi:10.1126/science.abh0635
10. Wagner CE, Saad-Roy CM, Morris SE, Baker RE, Mina MJ, Farrar J, et al. Vaccine Nationalism and the Dynamics and Control of SARS-CoV-2 [J]. *Science* (2021) 373(6562):eabj7364. doi:10.1126/science.abj7364
11. Chen J, Huang Y, Zhang R, Zhu Q. Optimal Quarantining Strategy for Interdependent Epidemics Spreading over Complex networks [J], Online: arXiv:2011.14262v2 (2021).
12. Socievole A, De Rango F, Scoglio C, Van Mieghem P. Assessing Network Robustness under SIS Epidemics: The Relationship between Epidemic Threshold and Viral Conductance [J]. *Computer Networks* (2016) 103(jul.5):196–206. doi:10.1016/j.comnet.2016.04.016
13. Youssef M, Kooij R, Scoglio C. Viral Conductance: Quantifying the Robustness of Networks with Respect to Spread of Epidemics [J]. *J Comput Sci* (2011) 2(3): 286–98. doi:10.1016/j.jocs.2011.03.001
14. Song B, Wang X, Ni W, Song Y, Liu RP, Jiang G-P, et al. Reliability Analysis of Large-Scale Adaptive Weighted Networks [J]. *IEEE Trans.Inform.Forensic Secur.* (2020) 15:651–65. doi:10.1109/tifs.2019.2926193
15. Lorenzi T, Pugliese A, Sensi M, Zardini A, Evolutionary Dynamics in an SI Epidemic Model with Phenotype-Structured Susceptible Compartment [J] *J. Mathematical Biol.* (2021) 83(72).
16. Cai CR, Wu ZX, Holme P. Multistage Onset of Epidemics in Heterogeneous Networks. *Phys Rev E* (2021) 103(3):032313. doi:10.1103/PhysRevE.103.032313
17. Fineberg HV, Wilson ME. Epidemic Science in Real Time [J]. *Science* (2009) 324(5930):987. doi:10.1126/science.1176297
18. Callaway DS, Newman MEJ, Strogatz SH, Watts DJ. Network Robustness and Fragility: Percolation on Random Graphs [J]. *Phys Rev Lett* (2000) 85(25): 5468–71. doi:10.1103/physrevlett.85.5468
19. Barabasi AL, Albert R. Emergence of Scaling in Random Networks [J]. *Science* (1999) 286(5439):509–12. doi:10.1126/science.286.5439.509
20. Watts DJ, Strogatz SH. Collective Dynamics of 'small-World' Networks [J]. *Nature* (1998) 393:440–2. doi:10.1038/30918
21. Laura VC, James MS, Charles O, Asiedu-Bekoe F, Kuffour Afreh O, Fernandez K, et al. Reactive Vaccination as a Control Strategy for Pneumococcal

Meningitis Outbreaks in the African Meningitis belt: Analysis of Outbreak Data from Ghana [J]. *Vaccine* (2019) 37(37):5657–63.
22. Jamakovic A, Kooij RE, Mieghem PV, van Dam ER, Robustness of Networks against Viruses: the Role of the Spectral Radius. 'In Symposium on Communications & Vehicular Technology [C]//". IEEE (2006). doi:10.1109/SCVT.2006.334367
23. Mieghem PV, Omic J. In-homogeneous Virus Spread in Networks [J]. *Mathematics* (2013) 17(1):1–14.
24. Kumar S, Saini M, Goel M, Aggarwal N, Modeling Information Diffusion in Online Social Networks Using SEI Epidemic Model [J]. *Proced Computer Sci* (2020) 171:672–8. doi:10.1016/j.procs.2020.04.073
25. Nakarmi U, Rahnamay-Naeini M, Khamfroush H. Critical Component Analysis in Cascading Failures for Power Grids Using Community Structures in Interaction Graphs [J]. *IEEE Trans Netw Sci Eng* (2019) 1. doi:10.1109/TNSE.2019.2904008
26. Yang L-X, Yang X. A New Epidemic Model of Computer Viruses [J]. *Commun Nonlinear Sci Numer Simulation* (2014) 19(6):1935–44. doi:10.1016/j.cnsns.2013.09.038
27. Liu J, Pare PE, Nedich A, Tang CY, Beck CL, Başar T. Analysis and Control of a Continuous-Time Bi-virus Model [J]. *IEEE Trans Automatic Control* (2019) 64(12):4891–4906. doi:10.1109/TAC.2019.2898515
28. Song B, Jiang G-P, Song Y-R, Xia L-L. Rapid Identifying High-Influence Nodes in Complex Networks [J]. *Chin Phys B* (2015) 24(10):100101. doi:10.1088/1674-1056/24/10/100101

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

frontiers in Physics

ORIGINAL RESEARCH
published: 31 January 2022
doi: 10.3389/fphy.2022.821321

UAV Swarm Resilience Assessment Considering Load Balancing

Pengtao Zhang[1], *Tao Wu*[1,2], *Runhua Cao*[2], *Zi Li*[3] *and Jiwei Xu*[4]*

[1]Equipment Management and UAV Engineering College, Air Force Engineering University, Xi'an, China, [2]School of Automation, Northwestern Polytechnical University, Xi'an, China, [3]Xinjiang Institute of Engineering, Urumqi, China, [4]School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an, China

UAV swarm are often subjected to random interference or malicious attacks during the execution of their tasks, resulting in UAV failure or communication interruption. When the UAV swarm is out of interference or the repair command is executed, the performance of the UAV swarm will be restored to a certain extent. However, how to measure the changes of UAV swarm's performance during this process will be very important, and it is also crucial to determine whether the UAVs can continue to perform its mission. Based on this motivation, we propose a resilience assessment framework for UAV swarm considering load balancing after UAV swarm suffer from disturbances. We analyze the effects of different topologies and different parameters on the resilience of UAV swarm. The study found that attack intensity is the most important factor affecting UAV swarm performance. As the attack intensity increases, the performance of the UAV swarm decreases rapidly. At the same time, topology also has a very important impact on UAV swarm resilience.

Keywords: resilience, networks, UAV swarm, load balancing, malicious attacks

OPEN ACCESS

Edited by:
Dongli Duan,
Xi'an University of Architecture and Technology, China

Reviewed by:
Yilun Shang,
Northumbria University, United Kingdom
Keke Huang,
Central South University, China
Husheng Wu,
Engineering University of PAP, China

***Correspondence:**
Jiwei Xu
xu@xupt.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *24 November 2021*
Accepted: *06 January 2022*
Published: *31 January 2022*

Citation:
Zhang P, Wu T, Cao R, Li Z and Xu J (2022) UAV Swarm Resilience Assessment Considering Load Balancing. Front. Phys. 10:821321. doi: 10.3389/fphy.2022.821321

INTRODUCTION

The extensive use of unmanned aerial vehicles (UAV) improves the convenience of mission execution and reduces the cost of completing missions. Meanwhile, it allows the execution of boring and dangerous tasks without causing unnecessary risks to humans [1]. With the increasing maturity of UAV manufacturing technology and the relative reduction of manufacturing costs, more and more people are interested in using UAVs to perform various tasks. For example, power maintenance, water and soil supervision, high-voltage tower fault line inspection, construction site survey, forest patrol and fire prevention, environmental inspection, oil and gas pipeline inspection and search and rescue, UAV express, traffic monitoring, etc. [2–4]. At this stage, one of the important application trends of UAVs is UAV swarms (especially military) [5]. In the swarm, a lot of small UAVs complete the set tasks through machine-machine coordination. Once individuals are concerned, each UAV has its own mission and needs to coordinate with other UAVs. Therefore, the local organizational structure is loose. Generally, the UAV swarm needs to be affected by the environment (Threats) for perception, assessment, and response. All UAVs are required to participate in this process. Therefore, the overall organizational structure is tight. In summary, UAV swarms need to be highly resilience in terms of link connection, communication, and recovery to realize the information exchange network [6]. Therefore, the UAV swarm be regarded as an information exchange network (IE network) in this article. The IE network can be represented by a graph. UAVs are nodes in the graph, and the information exchange links between UAVs represent edges in the graph.

To date, a UAV swarm can consist of hundreds of UAVs. Although the scale of UAV swarms is increasing, there are few studies on its resilience. At this stage, the research on UAV swarms is mainly

focused on survivability [7]. The survivability is considered to be that UAV swarms have different attack strengths and different attack methods (malicious attacks, random failures). The ability of the system to complete tasks normally is used to evaluate the ability of UAV swarms to perform tasks after being attacked (interference). Specifically, some research network survivability indicators have been developed and used to measure the performance of UAV systems, including natural connectivity and maximum connected subgraphs. In the above research, the damage of UAV nodes and link interference are considered irreversible.

When UAV swarms are used to monitor military targets and harsh environments, they will encounter unpredictable difficulties in these dangerous environments, which often cause UAV nodes or links to fail. Although sometimes failed nodes and links can be repaired, the mission fails due to the inability to assess the degree of UAV recovery. Under this condition, historical fault data cannot help people improve the performance of UAV swarms. In order to improve the success rate of UAV swarm mission execution, in traditional methods, it is necessary to improve the robustness of UAV components to reduce the failure rate of nodes or increase redundant nodes or links (as described in the previous section). It will increase the cost of UAV swarms, which is undesirable. On the contrary, the UAV swarm considers that the performance recovery in the event of damage will be more executable. Resilience provides new methods for engineering and system design, and characterizes the ability of the system to resist the influence of uncertain factors and the ability to recover afterwards. Therefore, it is of great significance to introduce the resilience index into the performance measurement of the UAV swarm.

However, there are few researches on the resilience of UAV swarms. In the UAV swarm, when some UAV nodes fail due to interference, the swarm often uses load balancing methods to assign the tasks of the failed nodes to the normal nodes according to established rules (the degree of the nodes is considered in the article), which can improve the resilience and usability of UAV swarms. However, when the node is overloaded, it will reduce the efficiency of the normal node and affect the performance of the UAV swarm. Therefore, it is important to analyze the impact of load balancing on the resilience of UAV swarm. Based on the above motivation, we propose a method for measuring the resilience of UAV swarms considering load balancing, and establish a UAV swarm performance model, give a UAV swarm load distribution model, and the variation of UAV swarm resiliency under different topologies and parameters is analyzed. The research motivation of the article will be given in the first section. In the second section, we continue to introduce the current situation of resilience research. In the third section, we establish the UAV swarm resiliency evaluation model, and conducted a verification analysis in the fourth section. The conclusion will be given in the fifth section.

RELATED WORKS

Resilience comes from the related fields of materials and mechanics. Which refers to one thing to deform after being affected by outside, and to return to its original shape when the effect disappears [8]. Due to the ubiquity of the system, the concept of resilience is widely used in different disciplines. Although they own different definitions, the resilience system is generally considered the ability to resist external influences and recover quickly. Compared with similar concepts such as invulnerability, robustness, reliability [9–12], the research focuses more on the degree of change and recovery speed of the system after being affected by outside.

When resilience proposed, it has attracted lots of attention. In recent years, people consider the research on resilience one of the hot topics in the scientific research field [13–15]. We have gradually realized that various systems that humans rely on are vulnerable to various disasters and exhibit vulnerabilities. Once the system is affected, it will require a long recovery process, and it may not even be able to recover to its original state. For example, it is estimated that the virus COVID-19 has caused tens of trillions of dollars in economic losses around the world [16], and nuclear pollution caused by a leak at the nuclear power plant in Fukushima, Japan, will continue for 30 years or more [17]. So research on system resilience is particularly important. It is necessary for scholars to carry out research on system resilience design and effects. We hope that resilience research can improve the ability of various systems to withstand emergencies, so as to avoid secondary disasters. So research on resilience has attracted extensive attention from researchers in different fields, such as the resilience of transportation networks, supply systems, and supply chains.

The infrastructure system is generally resilience [18, 19] in transportation, more and more people concern the resilience of roads. For transportation, resilience is defined as “the system’s ability to maintain its proven service level or restore itself to that service level within a specified time frame” [20–22]. Current research on the resilience of transportation networks focuses on the measurement of resilience. Some researchers use the synonyms of robustness [23], redundancy [24], reliability or fragility [25], and they also use total traffic delays, economic losses, maximum post-disaster flow, and autonomous system components measure the resilience of the transportation network [26].

As an important infrastructure, the urban water supply system plays an important role to improve the quality of life and ensure the functions of economic activities. Unfortunately, many natural disasters, such as earthquakes, tsunamis, hurricanes, etc., affect urban water supply system, and then affect our life, commerce and industry and other activities. Research on resilience of water supply systems mainly focuses on resilience evaluation and recovery strategy simulation. In terms of resilience evaluation, energy and graph theory are two commonly used methods. In a water supply system, resilience can be regarded as the ratio of node energy reserves to input energy from sources, storage tanks and pumping stations [27]. This type of resilience index can basically be regarded as a reliability substitute index, like entropy and Robustness index [28–30]. Similarly, various graph metrics (such as link density, average node degree, and swarming coefficient) can be used to quantify network resilience [31, 32].

In recent years, when environmental uncertainty continues to rise, interruptions are unexpected situations that may have a negative impact on enterprises at any time. Therefore, supply chain resilience has been emphasized as an important capability [33]. In the field of supply chain, supply chain resilience generally refers to the ability of enterprises to be vigilant, quick to respond and adapt to changes brought about by supply chain interruptions. Scholars often quote "the supply chain can be restored to its original state in time or reach a new More ideal state system capabilities" to define resilience [34]. At this stage, the definition of supply chain resilience has attracted more and more scholars' attention, and discussions have been conducted from the perspective of capabilities, which mainly include flexibility, responsiveness, and resilience. There are many angles to analyze the resilience of the supply chain, mainly including flexibility, redundancy, speed, visibility, time, space, density, complexity, node importance, inventory level, number of suppliers, cost, etc. [35, 36].

So, although the definition of resilience in different systems is not uniform, overall resilience is used to measure the ability to return to its original state or ideal state when it is disturbed. Resilience systems can withstand unexpected disturbances and recover quickly. Therefore, research on resilience can be found in different disciplines (such as engineering, economics, management, etc.), meanwhile more and more attention is paid. And the existing research mostly focuses on the resilience measurement and the design of resilience system. As mentioned above, UAV swarm often suffer attacks and random failures when performing tasks, which makes some UAV nodes unable to transmit information. At this time, load balancing strategies are often used to allocate tasks to complete the established tasks [37–39]. When the function of the failed node is restored, the task will be reloaded to restore the swarm performance. In this process, the swarm performance shows a resilience process of change.

If we consider resilience of the UAV swarm at the beginning of the design, it can greatly improve the ability of the UAV swarm to perform tasks, and enhance the ability of the UAV swarm to resist the influence of uncertain factors, which is important for expanding the application range of the UAV swarm significance.

MODEL

As mentioned earlier, UAV swarm are often subject to random failures and malicious attacks during missions. There are many reasons, mainly including the random failure of the UAV itself, the influence of the natural environment (including natural climate, mountains, forests, etc.), and man-made random attacks; malicious attacks mainly come from the enemy's targeted Attacks generally refer to situations in which the enemy obtains the UAV swarm topology, such as attacks based on node degree centrality, or node betweenness centrality, and so on.

When the UAV swarm is attacked, we assume κ as the attack intensity to indicate the proportion of nodes in the UAV swarm that are attacked, and $\kappa \in [0, 1]$. the number of nodes that are attacked by the UAV swarm is $|\kappa * N|$. After the UAV node is attacked and fails, in order to realize the normal operation of the function, it is necessary to replace the failed node with the surrounding nodes, so that the UAV swarm can continue to perform the task. At the same time, the system will take measures and repair nodes with a certain probability.

Performance Model

In the UAV swarm, due to cost constraints and technical factors, each UAV node has a fixed communication capacity, that is, the amount of information that can be transmitted per unit time is fixed. Assuming the capacity of the UAV node v_i is C_i, assuming the initial communication load of the UAV node is L_i, then there is a tolerance coefficient η that satisfies the following conditions.

$$C_i = (1 + \eta)L_i, i = 1, 2, \ldots, N \tag{1}$$

Among them, N is the number of UAV nodes, and the value L_i can be determined by node degree, betweenness centrality, etc., which can be expressed as [40]:

$$L_i(0) = d_i^{(1+\beta)} \tag{2}$$

Among them, d_i is the degree of the node v_i. In order to adjust the parameter, the value used for adjustment is in accordance with the actual situation.

When the node of UAV swarm is attacked and fails, in order to maintain the normal operation of the communication network, the network of UAV swarm will distribute the load of the failed node to its neighbor nodes. Considering that the capacity of a node to accept load is proportional to the capacity of the node, the node's acceptance of new load is directly proportional to the initial load. Suppose the set of adjacent nodes v_i of a node is Γ_i. Then the new load of the node v_j is shown as:

$$\Delta L_j(t+1) = \frac{L_j(t)}{\sum_{k \in \Gamma_i} L_k(t)} L_i(t) \tag{3}$$

Among them, $L_i(t)$ is the load of the node v_i at the moment t. Load distribution requires time. Let the time required for load distribution once be a discrete time. Therefore, the load change of the node can be shown as:

$$L_j(t+1) = L_j(t) + \Delta L_j(t+1) \tag{4}$$

Among them, $\Delta L_j(t+1)$ add load for the node v_j at $t+1$. After the node load is redistributed, the load of some nodes increases, which may cause overload. There are three states of the node v_i, namely normal, overload and failure. Define the node v_i information transmission capacity of the node at the moment t, as shown below,

$$s_i(t) = \begin{cases} normal & L_i(t) \le C_i \\ overload & C_i < L_i(t) \\ failure & be\ attacked \end{cases} \tag{5}$$

Equation 5 gives the qualitative description of node state $s_i(t)$. For quantitative description, let

$$l_i = \frac{L_j(t)}{C_i} \tag{6}$$

So, **Eq. 5** can be rewritten as

$$s_i(t) = \begin{cases} 1 & l_i \le 1 \\ \frac{1}{l_i} & 1 < l_i \\ 0 & be\ attacked \end{cases} \tag{7}$$

When the UAV swarm is attacked, the node-like in the UAV swarm circulates in the three states of normal, overload and failure. Initially, all UAV nodes are in normal working condition. When the UAV node is attacked, the UAV node will fail. When some nodes in the UAV swarm fail, load distribution will be triggered, which will cause the overload or overload failure of the neighbor nodes of the failed node. However, when the failed node of the UAV is repaired, the UAV swarm will return to its normal state. Overall, the performance of the UAV swarm presents a reciprocating resilience process. Therefore, the performance function of the UAV swarm at the moment can be defined as:

$$y(t) = \frac{\sum_{i=1}^{N_t} s_i(t)}{\sum_{i=1}^{N} s_i(0)} \tag{8}$$

Among them, N_t is the number of UAVs in the swarm at the moment t, $s_i(0)$ is the performance state of the UAV nodes at the initial time.

UAV Swarm Resilience

In **Section 3.1**, we show the measurement index of UAV swarm communication performance. Performance indicators measure the ability of the UAV swarm to perform tasks. In the paper, we mainly consider the node load status and swarm load status. When the UAV swarm needs to perform tasks cooperatively, it can only be completed when sufficient information exchange. Therefore, we show the research results of Trans et al. [41] to establish the UAV swarm resilience index, which is calculated as follows:

$$R = \begin{cases} \sigma\rho\left[\delta + \zeta + 1 - \tau^{(\rho-\delta)}\right] & if\ \rho - \delta \ge 0 \\ \sigma\rho(\delta + \zeta) & otherwise \end{cases} \tag{9}$$

Among them, σ is the total performance factor (Total Performance Factor), which represents the performance that the system can maintain in the relevant time period (mainly the resilience change time period); δ is the absorption factor, which represents the ability of the system to resist interference. For example, when the system is designed for redundancy or anti-interference design at the beginning of the design, the system has a high interference absorption capacity; ρ is the recovery factor, which indicates the degree to which the system can recover when it is interfered or attacked; τ is the recovery time factor, which represents the time factor from when the system receives interference to when it recovers to a steady state. ζ is the fluctuation factor, which represents the fluctuation that may occur in the process of the system from the disturbance state to the stable state. Therefore, the resilience process of the UAV swarm is shown in **Figure 1**.

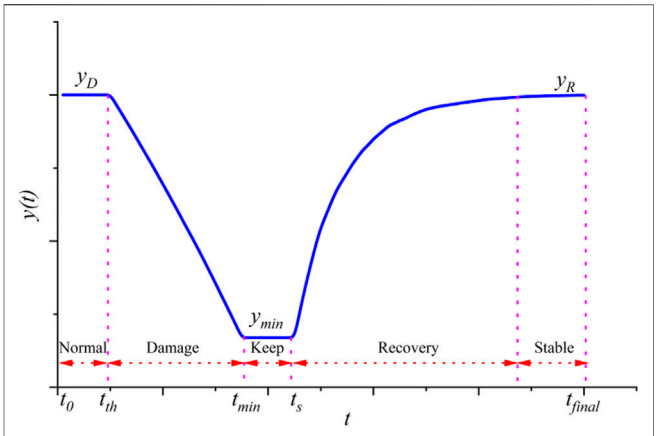


FIGURE 1 | Resilience change of UAV swarm.

$$\sigma = \frac{\sum_{t_0}^{t_{\text{final}}} y(t)}{y_D(t_{\text{final}} - t_0)}, \quad \delta = \frac{y_{\min}}{y_D}, \quad \rho = \frac{y_R}{y_D}$$
$$\tau = \frac{t_s - t_0}{t_{\text{final}} - t_0}, \ \zeta = \frac{1}{1 + \exp[-0.25(SNR_{dB} - 15)]} \tag{10}$$

Among them, $y(t)$ is defined by **Eq. 8**, y_D represents the initial performance of the UAV swarm. In the initial state, we believe that each UAV node can work normally, so $y_D = 1$. t_0 is the initial time, t_{final} is the stable time or the end time of the UAV swarm performance. In the follow-up experiment, we let $t_{\text{final}} = 100$, that is, we only observe the changes in the performance of the UAV swarm under 100-time steps.

CASE ANALYSIS

We focus on studying the resilience of UAV swarms when considering load balancing. In the third section, we propose the performance measurement index of UAV swarm when load balancing is considered, combined with the resilience index given in the literature [36], finally we realize the resilience measurement of UAV swarm.

In this section, we will discuss and analyze the resilience indicators given in the third section, focusing on the impact of network structure, network parameters, and repair rates on UAV swarm resilience. When designing the load balancing model, we use the degree of nodes as an indicator to measure the load capacity of UAVs in the UAV swarm, so we use maximum attack (delete the largest node in the current network) to simulate UAV swarms The interference received.

Then, the load is distributed according to the load balancing model proposed in **Section 3**, and the performance of the UAV swarm after each attack is calculated. In the repair process, within each discrete time t, the failed node restores its performance with probability q, and uses the inverse load distribution in Chapter 3

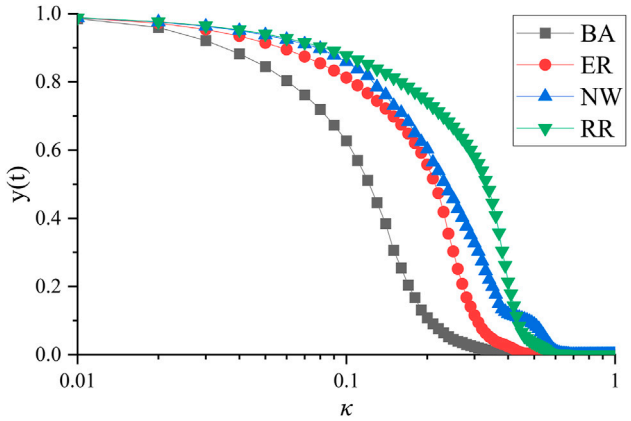


FIGURE 2 | Performance of UAV swarm under different attack intensities and topological structures. The vertical axis represents the performance of the UAV swarm, and the horizontal axis represents the logarithm of attack intensity.

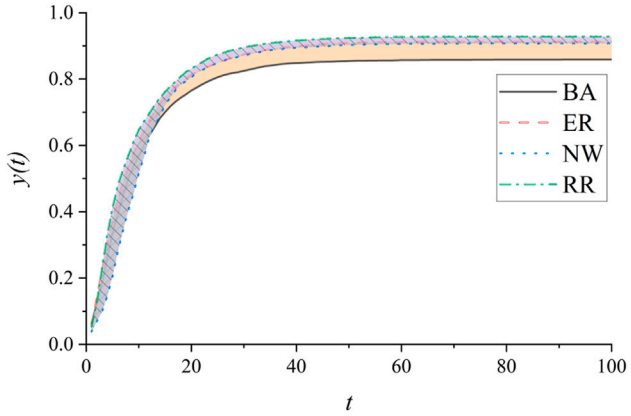


FIGURE 3 | Recovery process of UAV swarm performance under different topological structures. The ordinate is the performance of the UAV swarm, and the abscissa is discrete time T. The repair probability is 0.1, that is, at every discrete time t, the probability of damaged nodes being repaired follows a uniform distribution in the interval of (0, 1).

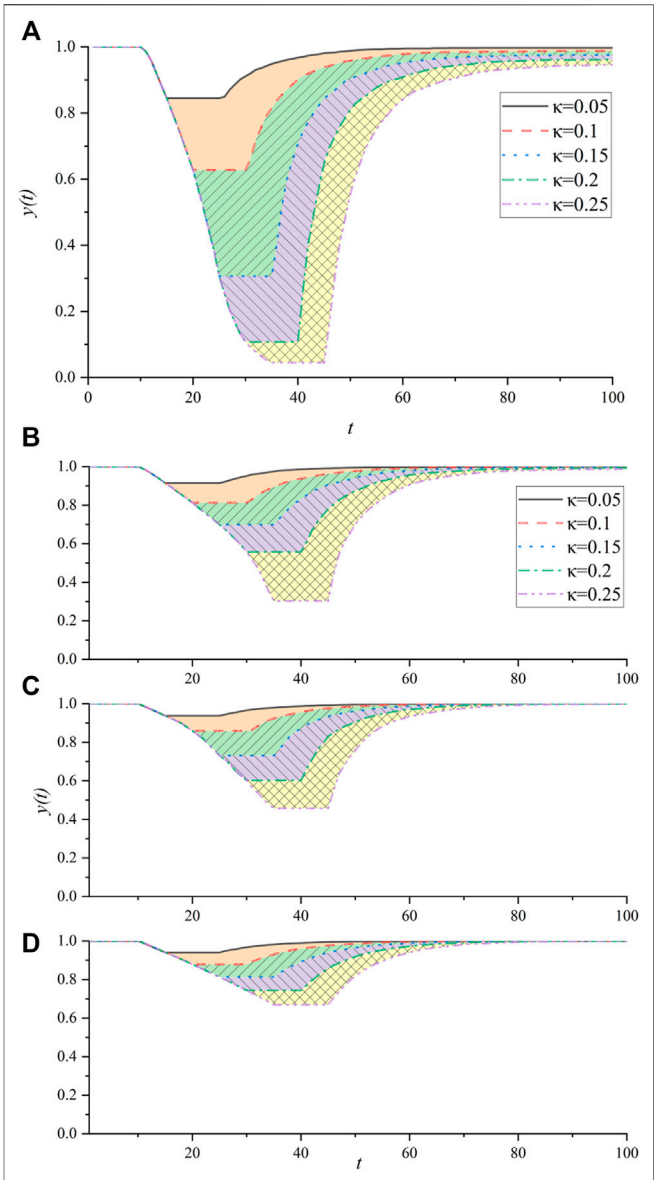


FIGURE 4 | Performance of UAV swarm under four topological structures. **(A)** BA network, **(B)** ER network, **(C)** NW network and **(D)** RR network. Each network was attacked five times with varying intensity and repaired continuously. The attack mode and repair procedure are described in **section 4.1**.

to reload the network load, and finally realize the resilience change process of the UAV swarm.

Analysis of Swarm Topology

In order to analyze the impact of different topologies on the performance of UAV swarms, we used four networks, BA network, ER random network, NW small world network and RR random rule network. For comparative analysis, each network has 100 fixed points and 200 edges. At the same time, in order to eliminate the influence of random factors in the process of generating the network, we generated a total of 200 networks and used the average to measure the performance of the network. Parameters of the four networks.

It can be seen from **Figure 2** that when the network has the same number of edges and nodes, the network topology has a significant impact on network performance. In general, when the four networks are attacked by the same intensity, the performance of the BA network has the fastest decline, the other three networks have a slower decline, and the RR network has the best performance. In terms of attack methods, we give priority to deleting the nodes with the largest degree in the current network, and networks with uneven degree distribution will collapse first. That is to say, there are Hub nodes in this type of network. When these nodes are deleted, they will directly affect the network structure, until the network collapses [42]. From the node capacity model given in Chapter 3, we can see that nodes with higher degrees are given more capacity by us, which intensifies

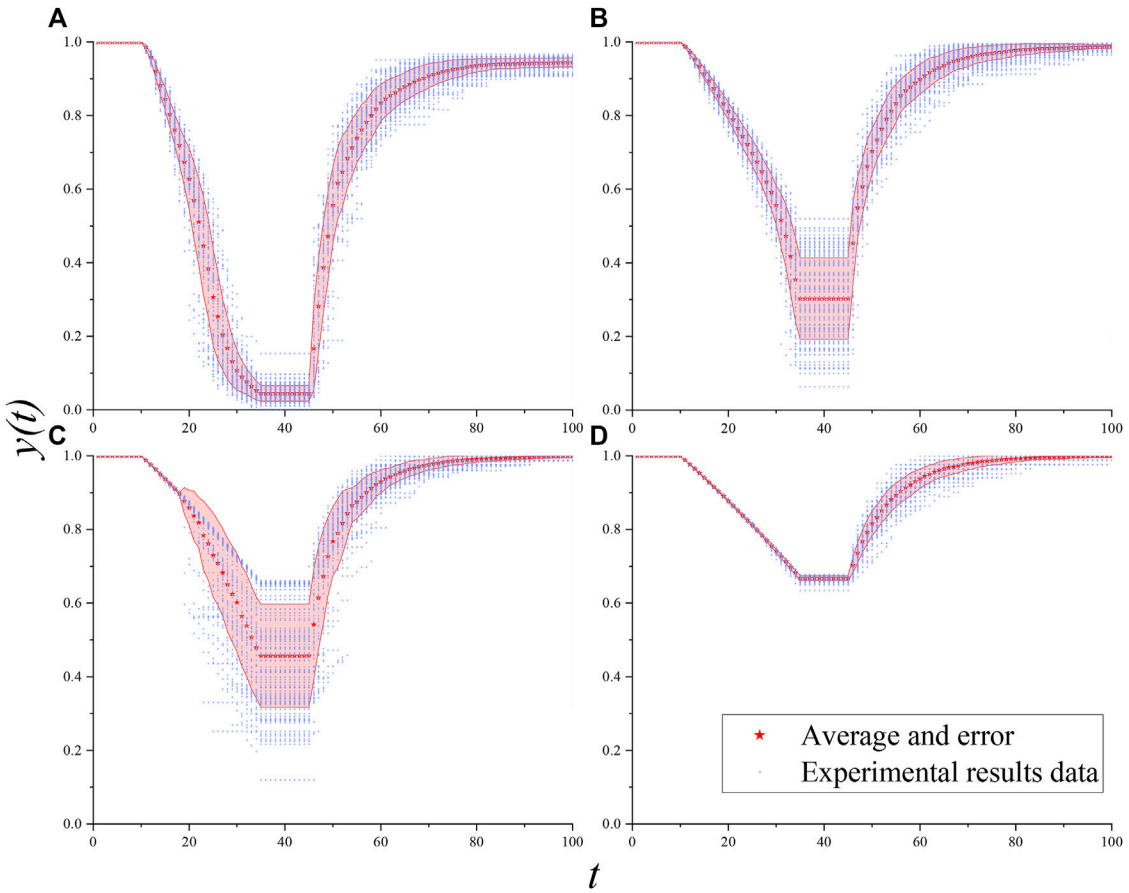


FIGURE 5 | Errors of UAV swarm resilience under different topologies. In the figure, the red pentagon is the mean of 100 experiments. The pink ribbon is the standard deviation of 100 experiments. The data for each experiment are the blue hollow tilted squares.

the heterogeneity between nodes. Therefore, under the research framework of this article, the RR network has high robustness to the maximum node degree attack.

In **Figure 3**, the performance change of the UAV swarm when the load sharing reverse process is used for repair is given. The figure shows that although the UAV nodes are all repaired, the swarm performance has not been restored to the initial state. Through research, it is found that the swarm deletes the largest nodes in the network in turn, but the order of repairing nodes is random. As a result, the UAV swarm load has non-uniformity, which ultimately leads to the worst performance with BA network characteristics.

UAV Swarm Resilience

In **Section 4.1**, when the maximum probability of attack and repair is reached, we find that the graph topology has a certain impact on the performance of the UAV swarm. In this section, we will study the resilience of UAV swarms. When studying the resilience of UAV swarms, we will use discrete time as the benchmark and proceed in the order of normal operation-attacked-state maintenance-repair-stability, where normal operation time and state maintenance time are. As can be seen from **Figure 3**, the four types of networks all show better resilience. When the network is attacked, the load capacity of the network continues to decline due to the priority deletion of nodes with greater degrees. Through the load balancing algorithm to redistribute the load of the failed node, the performance of the four networks is not degraded very quickly. However, as the number of failed nodes increases, the load of nodes that can work normally increases, causing some nodes to exceed their own load capacity and become overloaded, eventually reducing the performance of normal nodes, or even failing.

Among the four networks, the BA network exhibits stronger resilience than other networks. This shows that under malicious attacks, BA networks are susceptible to interference, that is, small disturbances will cause large fluctuations in the UAV swarm. For each network, the attack intensity will also affect the changes in network performance. That is, as the attack intensity continues to increase, the performance fluctuations of the UAV swarm will also increase.

The effect of different topologies on UAV swarm resilience is shown in **Figure 4**, and for comparison purposes only the average of 100 experiments is given. In **Figure 5** the error of the UAV swarm resilience variation for different topologies is given. Overall, the resilience of the UAV swarm under each topology shows a large fluctuation. Among them, the fluctuation of the

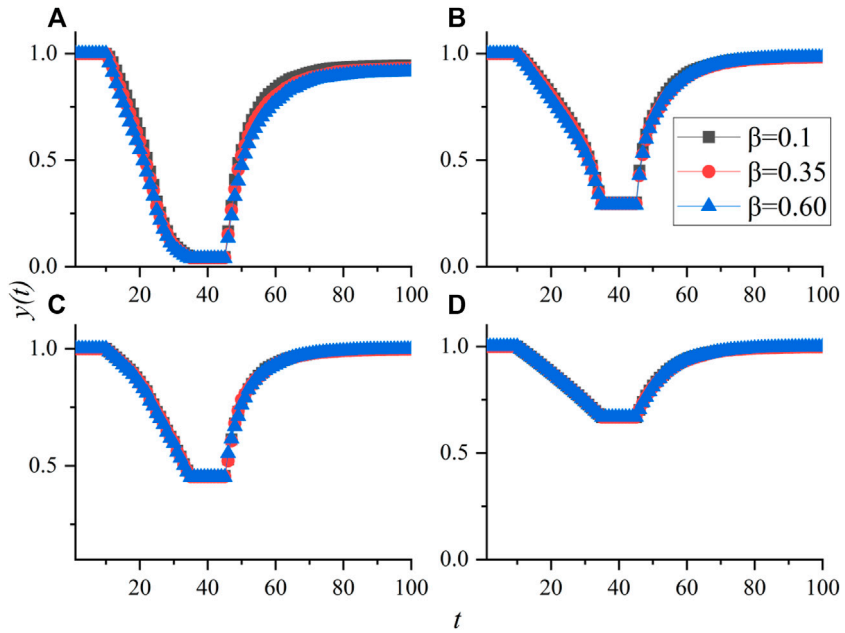


FIGURE 6 | Influence of parameter β on the resilience of the four networks. To reflect the difference, β is set to 0.1, 0.35, and 0.60, respectively. In addition, the remaining parameters η, and ρ are set to 0.1.

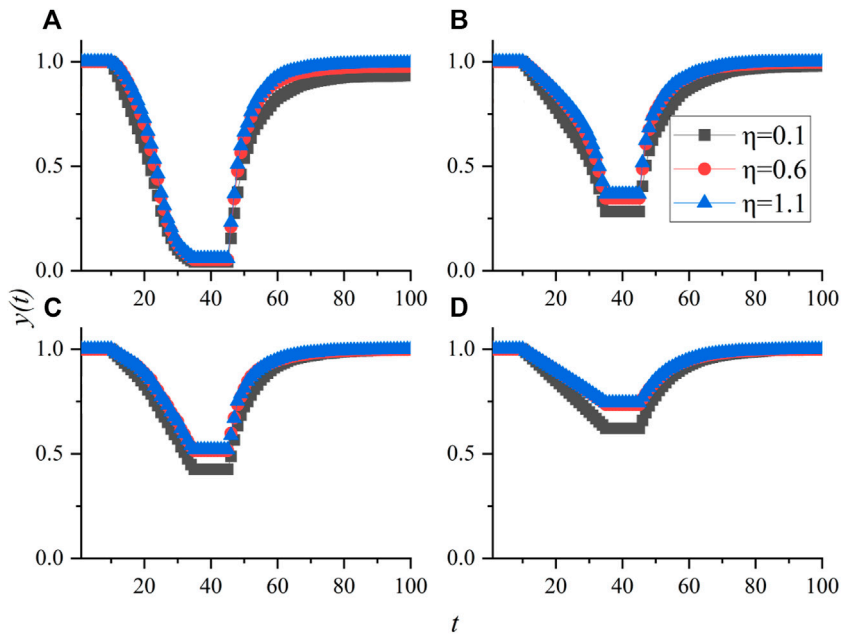


FIGURE 7 | Influence of parameter η on the resilience of the four networks. To reflect the difference, η is set to 0.1, 0.6, and 1.1, respectively. In addition, the remaining parameters β, and ρ are set to 0.1.

UAV swarm resilience is the smallest under the RR network topology (as shown in **Figure 5D**), i.e., it presents a stronger rigidity. In contrast, the NW network shows greater fluctuations, especially in increasing with the intensity of the attack (manifested in **Figure 5C** by the unevenness of the ribbon width). It is found that the reason for this phenomenon is related to the generation methods of the four networks. The RR network has the strongest regularity of degree distribution, so each generated network is highly similar and shows high similarity under the same attack strategy. NW network first

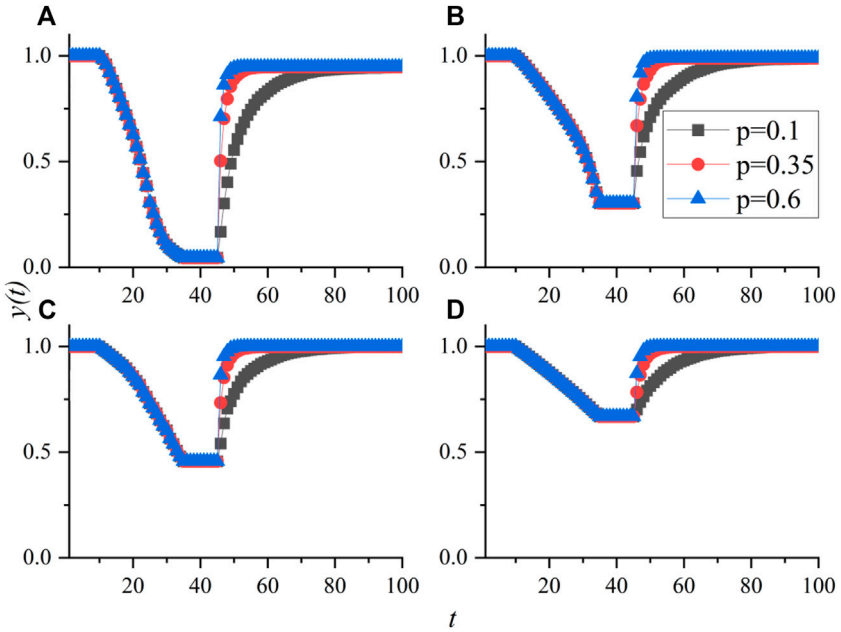


FIGURE 8 | Influence of parameter q on the resilience of the four networks. To reflect the difference, q is set to 0.1, 0.6, and 1.1, respectively. In addition, the remaining parameters β, and q are set to 0.1.

generates ring network and then connects randomly. When the attack intensity is low, the network fluctuation is small. However, when the attack intensity exceeds a limit (as shown in **Figure 5C**, 8 nodes are deleted), the network changes dramatically, resulting in dramatic differences in UAV swarm performance. By comparison, the regularity of BA network is weaker than RR network and stronger than NW network. Therefore, the error fluctuation of the BA network is between the two, i.e., the error exists but the fluctuation is not obvious (shown in **Figure 5C** as a more uniform color band). ER networks are more like a combination of BA and RR networks, i.e., like BA networks with large errors, and like NW networks with insignificant thresholds.

Parameter Influence

In **Section 4.1**, we analyzed the impact of topology on the swarm performance, and in **Section 4.2**, we analyze the impact of attack intensity on the resilience of the swarm. In this section, we will analyze the influence of four parameters on the resilience of the swarm. The experimental results are shown in **Figures 6–8**. During the experiment, for comparative analysis, we set the attack intensity constant to 0.25.

The influence of the parameters on the performance of the four types of networks is shown in **Figure 6**. We can find that the parameters β affect more on the performance of the BA network, and less on the other three networks. Especially, in **Figure 6A**, when β is 0.1, 0.35, and 0.60, the performance of the network is 0.93321, 0.97831, and 0.99412, respectively, and the corresponding network resilience is 0.359169, 0.42269, and 0.44504. Through analysis, it is found that as β increases, the difference in node capacity also increases significantly. After load balancing, more nodes will be overloaded, which will affect the performance of the swarm and cause the resilience of the swarm to fluctuate.

Figure 7 shows the impact of tolerance coefficient on network resilience. In **Eq. 1**, we define the tolerance factor, which characterizes the ability of an unmanned aerial vehicle to be overloaded. Larger tolerance factor means that the node can withstand more work without crashing, and vice versa. It can be seen in **Figure 7** that the tolerance factor can affect the performance of the four networks, but there are significant differences in the degree of impact. The tolerance factor has a small impact on the performance of the BA network and a greater impact on the RR network. Through the topology analysis of the network, it is found that the degree distribution of the BA network presents a power-law distribution, with greater differences, while the degree distributions of the other three networks are less different, especially the RR network.

The parameter η can affect much on the performance of the BA network, and little on the other three networks. Especially, in **Figure 8A**, when β = 0.1, 0.35, and 0.60, the performance of the network is 0.93321, 0.97831, and 0.99412, respectively, and the corresponding network resilience is 0.359169, 0.42269, and 0.44504. So, we find that when it increases, the difference in node capacity also increases significantly. After load balancing, more nodes will be overloaded, which will affect the performance of the swarm and cause the resilience of the swarm to fluctuate.

CONCLUSION

UAV swarm have attracted more and more attention. In the missions, the UAV itself or its communication is often subjected

to random interference or malicious attacks, which causes the UAV to fail or to interrupt the communication. When the UAV swarm is out of interference or the repair command is executed, the performance of the UAV swarm will be restored to a certain extent. However, how to measure the changes in UAV swarm's performance during this process is important, and it is also the key to determining whether the UAV can continue to perform its mission. Based on this motivation and considering the load balancing process of the UAV swarm after interference, we propose a UAV swarm resilience evaluation model that considers load balancing. In this process, the UAV node capacity model, load balancing model, overload failure model and performance resilience model are established. Finally, the resilience change process of the UAV swarm under different topological structures and parameters is analyzed. In the test process, following the characteristics of the model, we use degree attacks to test the resilience of the network. We find that attack intensity is the most important indicator that affects the performance of UAVs. With the increase of attack intensity, the performance of UAV swarm decreases rapidly, especially the performance of UAV swarm with BA network structure. Under different parameters, the performance of UAV swarm with a scale-free characteristic topology also decreases rapidly, but different parameters have different degrees of influence. Therefore, when the UAV swarm is configured with the capacity of the node degree and is attacked by the degree, the performance of the UAV degrades the fastest and the resilience changes the most.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

PZ, JX, and TW contributed to conception and design of the study. ZL organized the database. JX and RC performed the statistical analysis. PZ wrote the first draft of the manuscript. All authors contributed to manuscript revision, read, and approved the submitted version.

REFERENCES

1. Zhou X, Gao F, Fang X, Lan Z. Improved Bat Algorithm for UAV Path Planning in Three-Dimensional Space. *IEEE Access* (2021) 9:20100–16. doi:10.1109/access.2021.3054179
2. Liu D, Xu Y, Wang J, Chen J, Yao K, Wu Q, et al. Opportunistic UAV Utilization in Wireless Networks: Motivations, Applications, and Challenges. *IEEE Commun Mag* (2020) 58(5):62–8. doi:10.1109/mcom.001.1900687
3. Kouhdaragh V, Verde F, Gelli G, Abouei J. On the Application of Machine Learning to the Design of UAV-Based 5G Radio Access Networks. *Electronics* (2020) 9(4):689. doi:10.3390/electronics9040689
4. Yu X, Li C, Zhou J. A Constrained Differential Evolution Algorithm to Solve UAV Path Planning in Disaster Scenarios. *Knowledge-Based Syst* (2020) 204: 106209. doi:10.1016/j.knosys.2020.106209
5. Zhang Q, Chen J, Ji L, Feng Z, Han Z, Chen Z. Response Delay Optimization in Mobile Edge Computing Enabled UAV Swarm. *IEEE Trans Veh Technol* (2020) 69(3):3280–95. doi:10.1109/tvt.2020.2964821
6. Fu X, Pan J, Wang H, Gao X. A Formation Maintenance and Reconstruction Method of UAV Swarm Based on Distributed Control. *Aerospace Sci Tech* (2020) 104:105981. doi:10.1016/j.ast.2020.105981
7. Xu J, Deng Z, Ren X, Xu L, Liu D. Invulnerability Optimization of UAV Formation Based on Super Wires Adding Strategy. *Chaos, Solitons & Fractals* (2020) 140:110185. doi:10.1016/j.chaos.2020.110185
8. Masten AS, Reed MGJ. Resilience in Development[J]. In: *Handbook of Positive Psychology*. Oxford University Press (2002). p. 74–88.
9. Huang K, Wen H, Yang C, Gui W, Hu S. Outlier Detection for Process Monitoring in Industrial Cyber-Physical Systems, Proceeding of the IEEE Transactions on Automation Science and Engineering, June 2021 IEEE (2021). p. 1–12. doi:10.1109/TASE.2021.3087599
10. Huang K, Wu S, Li F, Yang C, Gui W Fault Diagnosis of Hydraulic Systems Based on Deep Learning Model with Multirate Data Samples, Proceeding of the IEEE Transactions on Neural Networks and Learning Systems, June 2021. IEEE (2021) p. 1–13. doi:10.1109/TNNLS.2021.3083401
11. Zhu P, Han J, Liu L, Lombardi F. Reliability Evaluation of Phased-Mission Systems Using Stochastic Computation. *IEEE Trans Rel* (2016) 65(3):1612–23. doi:10.1109/tr.2016.2570565
12. Zhu P, Han J, Guo Y, Lombardi F. Reliability and Criticality Analysis of Communication Networks by Stochastic Computation. *IEEE Netw* (2016) 30(6):70–6. doi:10.1109/mnet.2016.1500221nm
13. Keating A, Hanger-Kopp S. Practitioner Perspectives of Disaster Resilience in International Development. *Int J Disaster Risk Reduction* (2020) 42:101355. doi:10.1016/j.ijdrr.2019.101355
14. Harahap GY. Instilling Participatory Planning in Disaster Resilience Measures: Recovery of Tsunami-Affected Communities in Banda Aceh, Indonesia. *Birex Budapest Internation Research Exact Science* (2020) 2(3):394–404. doi:10.33258/birex.v2i3.1085
15. Song Z, Zhang H, Dolan C. Promoting Disaster Resilience: Operation Mechanisms and Self-Organizing Processes of Crowdsourcing. *Sustainability* (2020) 12(5):1862. doi:10.3390/su12051862
16. Dube K, Nhamo G, Chikodzi D. COVID-19 Cripples Global Restaurant and Hospitality Industry[J]. *Curr Issues Tourism* (2020) 24:1–4. doi:10.1080/13683500.2020.1773416
17. Kurihara Y, Takahata N, Yokoyama TD, Miura H, Kon Y, Takagi T, et al. Isotopic Ratios of Uranium and Caesium in Spherical Radioactive Caesium-Bearing Microparticles Derived from the Fukushima Dai-Ichi Nuclear Power Plant. *Sci Rep* (2020) 10(1):3281–10. doi:10.1038/s41598-020-59933-0
18. Karsai I, Schmickl T, Kampis G. *Resilience and Stability of Ecological and Social Systems[M]*. Springer International Publishing (2020).
19. Essuman D, Boso N, Annan J. Operational Resilience, Disruption, and Efficiency: Conceptual and Empirical Analyses. *Int J Prod Econ* (2020) 229: 107762. doi:10.1016/j.ijpe.2020.107762
20. Wan C, Yang Z, Zhang D, Yan X, Fan S. Resilience in Transportation Systems: A Systematic Review and Future Directions. *Transport Rev* (2018) 38(4): 479–98. doi:10.1080/01441647.2017.1383532
21. Liao T-Y, Hu T-Y, Ko Y-N. A Resilience Optimization Model for Transportation Networks Under Disasters. *Nat Hazards* (2018) 93(1): 469–89. doi:10.1007/s11069-018-3310-3
22. Ganin AA, Kitsak M, Marchese D, Keisler JM, Seager T, Linkov I. Resilience and Efficiency in Transportation Networks. *Sci Adv* (2017) 3(12):e1701079. doi:10.1126/sciadv.1701079
23. Tachaudomdach S, Upayokin A, Kronprasert N, Arunotayanun K. Quantifying Road-Network Robustness Toward Flood-Resilient Transportation Systems. *Sustainability* (2021) 13(6):3172. doi:10.3390/su13063172
24. Xu X, Chen A, Jansuwan S, Yang C, Ryu S. Transportation Network Redundancy: Complementary Measures and Computational Methods. *Transportation Res B: Methodological* (2018) 114:68–85. doi:10.1016/j.trb.2018.05.014

25. Gu Y, Fu X, Liu Z, Xu X, Chen A. Performance of Transportation Network Under Perturbations: Reliability, Vulnerability, and Resilience. *Transportation Res E: Logistics Transportation Rev* (2020) 133:101809. doi:10.1016/j.tre.2019.11.003
26. Sun W, Bocchini P, Davison BD. Resilience Metrics and Measurement Methods for Transportation Infrastructure: The State of the Art. *Sustainable Resilient Infrastructure* (2020) 5(3):168–99. doi:10.1080/23789689.2018.1448663
27. Creaco E, Franchini M, Todini E. The Combined Use of Resilience and Loop Diameter Uniformity as a Good Indirect Measure of Network Reliability. *Urban Water J* (2014) 13(2):167–81. doi:10.1080/1573062x.2014.949799
28. Singh VP, Oh J. A Tsallis Entropy-Based Redundancy Measure for Water Distribution Networks. *Physica A: Stat Mech its Appl* (2015) 421:360–76. doi:10.1016/j.physa.2014.11.044
29. Greco R, Di Nardo A, Santonastaso G. Resilience and Entropy as Indices of Robustness of Water Distribution Networks. *J Hydroinformatics* (2012) 14(3):761–71. doi:10.2166/hydro.2012.037
30. Shang Y. Resilient Group Consensus in Heterogeneously Robust Networks with Hybrid Dynamics. *Math Meth Appl Sci* (2021) 44(2):1456–69. doi:10.1002/mma.6844
31. Yazdani A, Otoo RA, Jeffrey P. Resilience Enhancing Expansion Strategies for Water Distribution Systems: A Network Theory Approach. *Environ Model Softw* (2011) 26(12):1574–82. doi:10.1016/j.envsoft.2011.07.016
32. Porse E, Lund J. Network Analysis and Visualizations of Water Resources Infrastructure in California: Linking Connectivity and Resilience. *J Water Resour Plann Manage* (2016) 142(1):04015041. doi:10.1061/(asce)wr.1943-5452.0000556
33. Pettit TJ, Fiksel J, Croxton KL. Ensuring Supply Chain Resilience: Development of a Conceptual Framework. *J business logistics* (2010) 31(1):1–21. doi:10.1002/j.2158-1592.2010.tb00125.x
34. Pettit TJ, Croxton KL, Fiksel J. Ensuring Supply Chain Resilience: Development and Implementation of an Assessment Tool. *J Bus Logist* (2013) 34(1):46–76. doi:10.1111/jbl.12009
35. Hosseini S, Ivanov D, Dolgui A. Review of Quantitative Methods for Supply Chain Resilience Analysis. *Transportation Res Part E: Logistics Transportation Rev* (2019) 125:285–307. doi:10.1016/j.tre.2019.03.001
36. Dubey R, Gunasekaran A, Childe SJ, Fosso Wamba S, Roubaud D, Foropon C. Empirical Investigation of Data Analytics Capability and Organizational Flexibility as Complements to Supply Chain Resilience. *Int J Prod Res* (2021) 59(1):110–28. doi:10.1080/00207543.2019.1582820
37. Finke J, Passino KM, Sparks AG. Stable Task Load Balancing Strategies for Cooperative Control of Networked Autonomous Air Vehicles. *IEEE Trans Contr Syst Technol* (2006) 14(5):789–803. doi:10.1109/tcst.2006.876902
38. Yang L, Yao H, Wang J, Jiang C, Benslimane A, Liu Y. Multi-UAV-Enabled Load-Balance Mobile-Edge Computing for IoT Networks. *IEEE Internet Things J* (2020) 7(8):6898–908. doi:10.1109/jiot.2020.2971645
39. Wu P, Xiao F, Huang H, Wang R. Load Balance and Trajectory Design in Multi-UAV Aided Large-Scale Wireless Rechargeable Networks. *IEEE Trans Veh Technol* (2020) 69(11):13756–67. doi:10.1109/tvt.2020.3026788
40. Luo XS, Zhang B. Analysis of Cascading Failure in Complex Power Networks Under the Load Local Preferential Redistribution Rule[J]. *Physica A: Stat Mech its Appl* (2012) 391(8):2771–7.
41. Tran HT, Domerçant JC, Mavris DN. A Network-Based Cost Comparison of Resilient and Robust System-Of-Systems. *Proced Comp Sci* (2016) 95:126–33. doi:10.1016/j.procs.2016.09.302
42. Wen X, Tu C, Wu M. Node Importance Evaluation in Aviation Network Based on "No Return" Node Deletion Method. *Physica A: Stat Mech its Appl* (2018) 503:546–59. doi:10.1016/j.physa.2018.02.109

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

frontiers in Physics

ORIGINAL RESEARCH
published: 31 January 2022
doi: 10.3389/fphy.2021.800860

Motif Transition Intensity: A Novel Network-Based Early Warning Indicator for Financial Crises

Ze Wang[1,2], *Siyao Liu*[3,4], *Chengyuan Han*[5], *Shupei Huang*[3,4], *Xiangyun Gao*[3,4], *Renwu Tang*[6] *and Zengru Di*[1,2]*

[1]International Academic Center of Complex Systems, Beijing Normal University at Zhuhai, Zhuhai, China, [2]School of Systems Science, Beijing Normal University, Beijing, China, [3]School of Economics and Management, China University of Geosciences, Beijing, China, [4]Key Laboratory of Carrying Capacity Assessment for Resource and Environment, Ministry of Land and Resources, Beijing, China, [5]Institute for Theoretical Physics, University of Cologne, Köln, Germany, [6]School of Government, Beijing Normal University, Beijing, China

Financial crisis, rooted in a lack of system resilience and robustness, is a particular type of critical transition that may cause grievous economic and social losses and should be warned against as early as possible. Regarding the financial system as a time-varying network, researchers have identified early warning signals from the changing dynamics of network motifs. In addition, network motifs have many different morphologies that unveil high-order correlation patterns of a financial system, whose synchronous change represents the dramatic shift in the financial system's functionality and may indicate a financial crisis; however, it is less studied. This paper proposes motif transition intensity as a novel method that quantifies the synchronous change of network motifs in detail. Applying this method to stock networks, we developed three early warning indicators. Empirically, we conducted a horse race to predict ten global crises during 1991–2020. The results show evidence that the proposed indicators are more efficient than the VIX and the other 39 network-based indicators. In a detailed analysis, the proposed indicators send sensitive and comprehensible warning signals, especially for the U.S. subprime mortgage crisis and the European sovereign debt crisis. Furthermore, the proposed method provides a new perspective to detect critical signals and may be extended to predict other crisis events in natural and social systems.

Keywords: early warning signal, critical transition, financial crisis, volatility spillover, network motif

OPEN ACCESS

Edited by:
Gaogao Dong,
Jiangsu University, China

Reviewed by:
Xiaoke Xu,
Dalian Nationalities University, China
Dror Y. Kenett,
Johns Hopkins University,
United States

***Correspondence:**
Zengru Di
zdi@bnu.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *24 October 2021*
Accepted: *10 December 2021*
Published: *31 January 2022*

Citation:
Wang Z, Liu S, Han C, Huang S, Gao X, Tang R and Di Z (2022) Motif Transition Intensity: A Novel Network-Based Early Warning Indicator for Financial Crises. Front. Phys. 9:800860. doi: 10.3389/fphy.2021.800860

INTRODUCTION

Critical transition is a ubiquitous phenomenon in social-ecological fields [1, 2]. In financial markets, critical transition appears as financial crises [3, 4]. Considering that the outbreak of financial crises accompanies catastrophic system collapses and brings grievous economic and social losses, developing a precise early warning indicator is of great significance [5, 6]. With the finding that the interconnectedness of the financial system increased dramatically before financial crises, researchers have focused on detecting early warning signals by analyzing the interactions in a financial system [7–9]. Based on network theory, all system components can be linked by their interactions to form a network; exploring global network topologies helps quantify their interconnectedness to build early warning indicators [10]. Various studies of bank, guarantee,

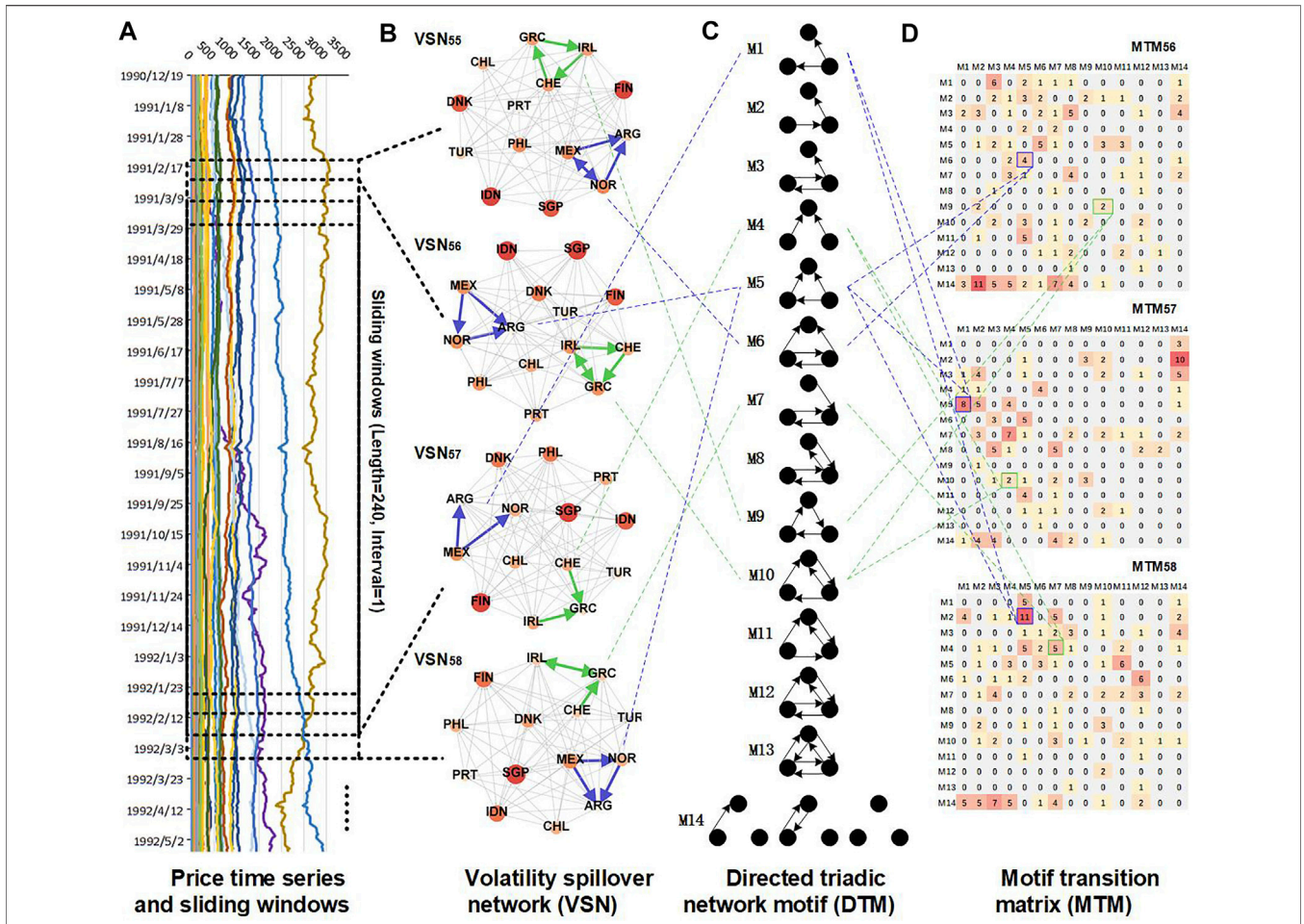


FIGURE 1 | Flowchart of the main methodology. **(A)** The price data are divided into subsets using sliding windows. Four time-related windows are illustrated. **(B)** The VSN of each window is established. Two different node triplets are illustrated, i.e., {Argentina, Mexico, Norway} marked in blue and {Greece, Ireland, Switzerland} marked in green. Their motifs are identified and linked to the corresponding morphology in **(C)**. **(D)** The statistics of motif transitions by analyzing the marginal change of each node triplet.

and stock networks have found empirical evidence that global network topologies can reveal financial crises [11–14]. However, a small portion of research has emphasized that more informative signals may hide in tiny changes of local network topologies [15] because networks in similar global topologies may differ noticeably at a local level [16]. Inspired by this phenomenon, we aim to propose a novel early warning indicator by analyzing local network topologies.

Network motif is a local network topology regarded as fundamental to a network [17, 18]. It shows intrinsic correlations with network resilience and robustness and can influence network functionality [16, 19]; thus is identified as a determinant of critical transition [20]. Considering that a financial crisis is rooted in a lack of system resilience and robustness, analyzing the evolution of the financial network motif deepens the understanding of financial stability and helps predict financial crises [15, 21]. Empirical studies have found that network motifs, in different morphologies, may change abruptly ahead of financial crises [22, 23]. However, it is difficult to robustly predict all financial crises by relying on one network motif with a specific morphology. To tackle this problem, simultaneously analyzing several network motifs in different morphologies is helpful. As each morphology of network motifs unveils a high-order correlation pattern of a financial network [24], their synchronous change represents the dramatic shift in the financial system's functionality and may indicate a financial crisis [25]. In recent studies, researchers have found predictive signals by investigating network motifs distributions [21] and flickering behaviors [25]. This finding enlightens us to propose a better early warning indicator by describing more network motifs' synchronous change in more detail.

According to the above idea, we propose motif transition intensity (MTI) as a novel early warning indicator for financial crises. It relies on directed triadic motifs (DTMs) that are node triplets with 13 morphologies [26]. By investigating all node triplets' changing dynamics, MTI statistics show how many node triplets change from one morphology to another at

TABLE 1 | Ten influential global financial crises from 1991 to 2020.

No.	Event	Period
1	Mexico financial crisis	1994.12–1995.03
2	Asia financial crisis	1997.08–1998.12
3	Russian default crisis	1997.10–1998.08
4	Brazil financial crisis	1999.01–1999.02
5	Argentina financial crisis	2001.07–2002.03
6	U.S. subprime mortgage crisis	2007.08–2008.12
7	Iceland's international debt crisis	2008.10–2008.11
8	European sovereign debt crisis	2010.02–2010.11 2011.05–2012.03
9	US-China Trade dispute	2018.03–2018.11
10	The global outbreak of COVID-19 and the March 2020 stock market crash	2020.03–2020.03

different evolution times (shown in **Figure 1**). The result is defined as motif transition, capturing the change of DTMs in all 13 morphologies in more detail. When motif transition is intense, the network motifs are changed synchronously, which indicates the dramatic shift of a financial system's correlation pattern and provides early warning signals for financial crises. Therefore, we quantify the intensity of motif transitions to build the MTI indicator. Compared to other methods, MTI has two advantages. 1) If the motif transition is calculated under different evolution times with ultrashort intervals, MTI can describe the marginal change of a financial system to unveil the leading force of the financial system's integral evolution trend [27]. 2) From a bottom-up point of view, a motif is built by node/edge, and many motifs may share one node/edge, so a financial network can be considered established by overlapping and splicing a mass of motifs [28]. Thus, a slight change in nodes/edges may result in intricate and abundant changes in different motif morphologies. With these two advantages, MTI could be considered a sensitive signal amplifier to achieve more precise predictions of financial crises.

This paper computes the MTI indicator based on the volatility spillover network (VSN), which uncovers more financial crisis information [29, 30]. Furthermore, we use the sliding window method to explore the changing dynamics of DTMs of the VSN [31, 32]. Moreover, to fully exhibit the performance of the proposed method, three intensity measurements are used to quantify the MTI indicator: quantity, density, and uniformity. Empirically, we conducted a horse race of the MTI indicators and 39 other widely used network-based indicators to predict ten influential global financial crises to demonstrate their efficiency. Methodologically, our novel approach contributes to designing more sensitive and reliable network-based early warning indicators, which can serve as a component in hybrid data-driven warning systems [33]. In term of applications, our indicators can extend applications to other vital socioeconomic crises, such as climate change, political conflicts, and pandemic influenza [1].

This paper is organized as follows: *Materials and Methods* describes the material and methods, *Results and Discussion* discusses empirical results, and *Conclusion* concludes the significant findings.

MATERIALS AND METHODS

Data

This paper focuses on the early warning of financial crises in the global financial system. We use the closing price of 73 MSCI country/region indices as proxies for country-level financial markets and build a VSN to represent the global financial system. Moreover, we choose the Chicago Board Options Exchange Volatility Index (VIX) as a benchmark. All data are accessed from the WIND database and span from 1990.12.19 to 2020.9.8 (7267 total trading days). In this period, we summarized ten influential financial crises, as shown in **Table 1**.

Names and abbreviations of the indices are Argentina (ARG), United Arab Emirates (United Arab Emirates), Oman (Oman), Egypt, Arab Rep. (EGY), Ireland (IRL), Estonia (EST), Austria (AUT), Australia (AUS), Pakistan (PAK), Bahrain (BHR), Brazil (BRA), Bulgaria (BGR), Belgium (BEL), Poland (POL), Botswana (BWA), Denmark (DNK), Germany (DEU), Russian Federation (RUS), France (FRA), Philippines (PHL), Finland (FIN), Colombia (COL), Kazakhstan (KAZ), Korea, Rep. (KOR), Netherlands (NLD), Canada (CAN), Ghana (GHA), Czech Republic (CZE), Qatar (QAT), Kuwait (KWT), Croatia (HRV), Kenya (KEN), Lebanon (LBN), Lithuania (LTU), Romania (ROU), Malaysia (MYS), Mauritius (MUS), United States (USA), Peru (PER), Morocco (MAR), Mexico (MEX), South Africa (ZAF), Nigeria (NGA), Norway (NOR), Portugal (PRT), Japan (JPN), Sweden (SWE), Switzerland (CHE), Saudi Arabia (SAU), Sri Lanka (LKA), Slovenia (SVN), Thailand (THA), Trinidad and Tobago (TTO), Tunisia (TUN), Turkey (TUR), Ukraine (UKR), Spain (ESP), Greece (GRC), Singapore (SGP), New Zealand (NZL), Hungary (HUN), Jamaica (JAM), Israel (ISR), Italy (ITA), India (IND), Indonesia (IDN), United Kingdom (GBR), Jordan (JOR), Vietnam (VNM), Chile (CHL), China (CHN), Taiwan, China (TWN), Hong Kong, China (HKG).

Methodology

We propose five steps to quantify the motif transition intensity and build novel early warning indicators. These steps are shown in **Figure 1** and listed below.

Step 1: Data preparations and the sliding window method.

This paper computes the return of each price time-series for analysis and uses the sliding window method to analyze the changing dynamics of the financial system. The sliding window method divides the full price return data into time-related subsets, as shown in **Figure 1A**. The length and ultrashort intervals of the window are 240 and 1 trading day, respectively. This helps us obtain 7028 data subsets, each of which is used to build a financial network.

For the price return under each sliding window, each should pass a stationary, normality, and ARCH effect test to provide statistically rigorous results. Moreover, if a price return is 24 (10% of the sliding window's length) or more consecutive days of the trading suspension, it will be abandoned due to possible high noise.

Step 2: Volatility spillover network establishment.

This paper builds a financial network based on investigating volatility spillover correlations among all components in a financial system. The volatility spillover correlation measures the co-movement interactions of financial entities, which helps capture risk contagion paths and is widely used in financial crisis studies. Examining the volatility spillover correlation relies on econometric models that provide more rigorous results to reveal more financial crisis information than other causal inference methods. Among them, the BEKK-GARCH model has the advantages of less information loss and more flexibility. Therefore, we adopt the bivariate BEKK-GARCH model of order one and lay one to build financial networks.

We run the BEKK-GARCH model on the return of two financial markets i and j under a sliding window s. As a result, if the upper off-diagonal parameter in conditional residual or covariances matrices is significant, it can be deemed that i's volatility can spill over to j. After investigating all markets, we link them according to their volatility spillover correlations to build a directed network. This network is defined as the volatility spillover network (VSN), denoted as VSN^s, which represents the global financial system and helps us analyze the global financial crises. This process is shown in **Figure 1B**. It is worth noting that the detailed methodology descriptions of Step 1 and Step 2 are in [34]. Moreover, the significance level of all tests in this study is set as 0.05.

Step 3: Network motif identifications.

Our work focuses on DTMs, whose 13 morphologies are defined as $M1, M2, \ldots, M13$; for more detailed analysis, $M14$ is defined as the structures that cannot form a DTM, i.e., an unconnected node triplet. All 14 morphologies are shown in **Figure 1C**. A VSN of N nodes has up to C_N^3 triplets denoted as $V_q^s(3) = \{i, j, k\}$, $q = 1, 2, \cdots, C_N^3$; each triplet can correspond to only one motif morphology. Mathematically, the matchup of every triplet and its motif morphology can be recorded in a $C_N^3 \times 14$ binary matrix denoted as MM^s. Specifically, each column represents a motif morphology; each row represents a triplet with a one-hot value that indicates its motif morphology. An example matrix is as follows.

$$MM^s = \begin{array}{c} \\ V_1^s(3) \\ V_2^s(3) \\ \vdots \\ V_{C_N^3}^s(3) \end{array} \begin{array}{c} \begin{array}{cccccccccccccc} M1 & M2 & M3 & M4 & M5 & M6 & M7 & M8 & M9 & M10 & M11 & M12 & M13 & M14 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}. \quad (1)$$

Step 4: Motif transition statistics.

Motif transition describes the number of changed motif morphologies of all node triplets between two time steps, providing more detailed information on network motif changes than the evolution of the network motif distribution. As mentioned in Step 1, the step size of the sliding windows is 1 day, which is sufficiently short of describing a financial system's marginal change. For every two time-adjacent windows, the motifs are identified and recorded in MM^s and MM^{s-1}. These two matrices should have the same number of rows. If it is not true, MM^s or MM^{s-1} should be supplemented according to the union of the node triplets in VSN^s and VSN^{s-1}.

Then, by operating matrix multiplication, motif transitions can be captured by a 14×14 square matrix, defined as MTM^s (shown in **Figure 1D**) and computed as **Eq. 2**. In **Eq. 2**, each row or column represents one morphology of the DTM. $mt_{m,n}^{s-1,s}$ quantifies how many node triplets shift from motif m (in window $s-1$) to motif n (in window s). Our research focuses only on the changed motifs; therefore, if $m = n$, $mt_{m,m}^{s-1,s} = 0$.

$$MTM^s = \left(MM^{s-1}\right)^T * MM^s = \begin{pmatrix} 0 & mt_{1,2}^{s-1,s} & \cdots & mt_{1,14}^{s-1,s} \\ mt_{2,1}^{s-1,s} & 0 & \cdots & mt_{2,14}^{s-1,s} \\ \vdots & \vdots & \ddots & \vdots \\ mt_{14,1}^{s-1,s} & mt_{14,2}^{s-1,s} & \cdots & 0 \end{pmatrix}. \quad (2)$$

Step 5: Early warning indicator development.

Intuitively, if motif transitions are intense, more network motifs are changed synchronously; this indicates the dramatic shift of a financial system's correlation pattern and provides early warning signals for financial crises. Based on this idea, we propose the motif transition intensity (MTI) indicator by using three intensity measures on MTM^s, i.e., quantity, diversity, and uniformity. To distinguish, the three MTI indicators are denoted as MT.S, MT.D, and MT.E.

First, MT.S measures the quantity of motif transition. It is a simple indicator that quantifies the total number of the changed motifs by summarizing all elements in MTM^s, computed as **Eq. 3**.

$$MT.S^s = \sum_m \sum_n mt_{m,n}^{s-1,s}. \quad (3)$$

Second, MT.D measures the diversity of motif transitions. Specifically, MT. D quantifies how many network motif morphologies are involved in the change of network motifs. As mentioned in the Introduction, network motif morphologies represent different financial correlation patterns, and a higher MT.D indicates a significant change in a financial system's functionality and may indicate a financial crisis. In MTM^s, the change in motif morphologies is up to M ($M = 14*13$) possibilities. Thus, we define the change rate of motif morphologies as the diversity of motif transitions,

$$MT.D^s = \sum_m \sum_n a_{m,n}^{s-1,s} \Big/ M, a_{m,n}^{s-1,s} = \begin{cases} 1, & mt_{m,n}^{s-1,s} > 0 \\ 0, & mt_{m,n}^{s-1,s} = 0 \end{cases} \quad (4)$$

Third, MT.E measures the uniformity of the motif transition, which is a comprehensive indicator that considers both the quantity and diversity of the motif transition. Imagining a situation where the motif transition involves many motif morphologies with a similar quantity, all network motifs change synchronously and indicate a financial crisis. MT.E aims to measure whether the network motifs in all 14 morphologies are changed equally by using an entropy measurement. In particular, we adopt the negative generalized entropy index [35, 36] to quantify the uniformity of MTM^s. It is

denoted as $MTM.E^s$ and computed following **Eq. 5**, where the preset parameter α is set as 0.5.

$$MTM.E^s = -\frac{1}{M\alpha(\alpha-1)}\sum_m\sum_n\left[\left(mt.r_{m,n}^{s-1,s}\right)^\alpha - 1\right] \quad (5)$$

In **Eq. 5**, to eliminate the influence of motifs' prior distribution, we scale $mt_{m,n}^{s-1,s}$ by dividing the total number of correlated motifs in the sliding window $s-1$, where $mt.r_{m,n}^{s-1,s} = mt_{m,n}^{s-1,s}/\sum_{m=1}^{m=14} mt_{m,n}^{s-1,s}$. In addition, considering that the uniformity of motif transition may greatly vary at different times, we use a log operation to scale $MTM.E^s$. More importantly, we deduct the information of the random motif transitions to highlight the uniqueness of motif transitions' uniformity. Specifically, we use null models[1] to generate random networks and compute their motif transition uniformity, denoted as $MTM.E^s_{RANDOM}$. Then, MT.E is calculated by subtracting the mean of p $MTM.E^s_{RANDOM}$, where p is set as 10,

$$MT.E^s = \log(MTM.E^s) - \frac{1}{p}\left(\sum_p \log\left(MTM.E^s_{RANDOM}\right)\right). \quad (6)$$

Early Warning Performance Evaluation

In our research, the global financial system is assumed to have two actual states, i.e., crisis and safe, which could be labeled according to the crisis events in **Table 1**. The proposed early warning indicators predict a crisis state of the global financial system if it exceeds a certain threshold; otherwise, they predict a safe state. If the predicted states exactly meet the actual states, the early warning indicator is regarded as good performance. To judge quantitatively, we selected five criteria: area under the receiver operating characteristic curve (AUC), accuracy (A), coverage rate (CR), F1 score, and F2 score. Among them, A is the ratio of the correct crisis predictions to the actual crisis states; CR is the ratio of the correct crisis predictions to the predicted crisis states; F1 and F2 are comprehensive measurements of A and CR, where F1 emphasizes A and F2 emphasizes CR; AUC measures whether a randomly chosen crisis state is risker than that of a safe state, which unveils the early warning signal's credibility. The descriptions and formulations of the five metrics have been comprehensively introduced in the related Ref. [37, 38].

RESULTS AND DISCUSSION

The Motif Transition Intensity Indicators

In **Figure 2**, we plot the three proposed MTI indicators and the benchmark indicator VIX for comparisons. All four indicators can successfully predict the financial crisis, yet our indicators perform better in three aspects. First, our indicators could send efficient warning signals for the U.S. subprime mortgage crisis and the European sovereign debt crisis (the periods are marked in red in **Figure 2**). Remarkably, the proposed indicators are at least 6 months ahead of VIX to the sent warning signals.

Second, our indicators are sensitive to early warning. Compared to VIX, they reveal three additional impactive events, i.e., the Crimea crisis, the United States withdrawal from the Trans-Pacific Partnership, and the United Kingdom's official launch of Brexit negotiations (all periods are marked in blue in **Figure 2**). The Crimea crisis shows deepening geographical and political conflict, and the other two events demonstrate that the development pattern of the global economy is reaching a tipping point [39]. They are external financial system shocks whose influence is not secondary to financial crises.

Third, our indicators send more comprehensible warning signals than VIX. Mainly, MT.D persistently obtains high values before and during financial crisis periods, similar to step signals. In contrast, VIX obtains short-lived high values before financial crises, such as pulse signals (the periods are marked in green in panel 4 of **Figure 2**). Noticeably, step signals can indicate financial crises without ambiguity compared to pulse signals.

In summary, the three proposed MTI indicators perform more efficiently, sensitively, and comprehensibly than VIX. That is especially true for MT.D. These results prove that the changing dynamics of motif transition intensity can validly capture the marginal change of the financial system to reveal financial crises, which provides a new perspective to detect early warning signals.

The Horse Race of Network-Based Early Warning Indicators

To quantitatively analyze the early warning abilities of the three proposed MTI indicators in detail, we conducted a horse race for the ten financial crises during 1991–2020. We choose both statistics-based indices and network topology-based indices as comparative variables to make a comprehensive comparison. The statistics-based indices includes VIX and the total variance of the global financial system (denoted as TV, computed by the sum of the variance and covariance of all indices' return of each sliding window). They are set as benchmarks of our study.

The network topology-based index includes 39 widely used indices. Among these, six indices quantify the global features of the VSN: edge number (EN), node number (NN), average distance (AD), density (DEN), diameter (DIA), and assortativity (ASO). Seven indices quantify the partial features of the VSN by averaging the network centralities of each node: indegree (AID), outdegree (AOD), closeness centrality (ACLO), betweenness centrality (ABTW), clustering coefficient (ACLU), eigenvector centrality (AEGV), and PageRank (APAG). The other 26 indices include the statistical quantity of the 13 motifs, denoted as M1-M13, and the z-score[2] of the 13 motifs, denoted as M1. Z-M13.Z. The descriptions and formulations of the

[1]The null model in this research is constructed by randomly reshuffling network links, while keeping the node and edge numbers the same as in the original networks. This could highlight the uniqueness of a network's structure property by comparing it to its corresponding null model.

[2]Network motif's z-score is computed to quantify the significance of a motif by comparing it to null models. It has been proven that the abrupt change of a network's z-score can help in early warning of the great financial crisis in 2008. In addition, we construct 10 null models for each VSN to compute each network motif's z-score.

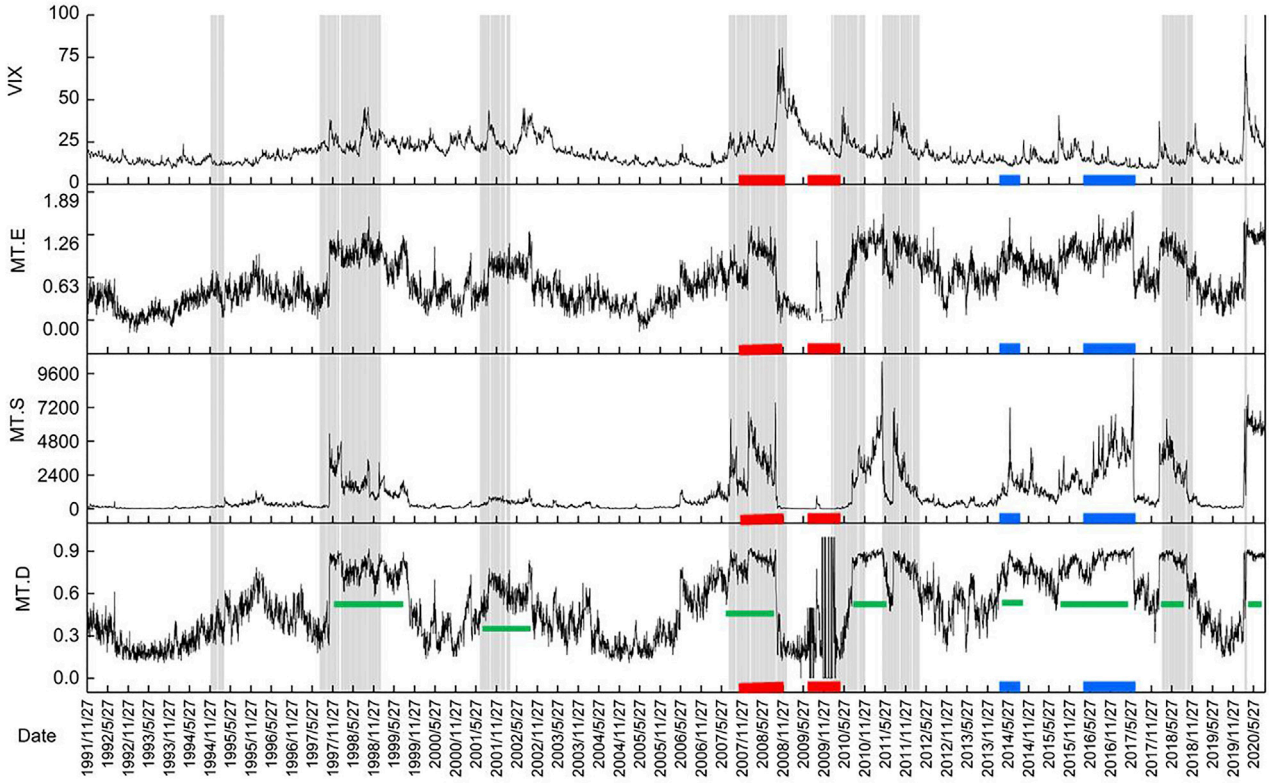


FIGURE 2 | Time series of the three novel early warning indicators and the VIX index. Four panels in this figure show the evolution of the global financial system's status. The x-axis of all panels is aligned. The background of the ten influential financial crises is marked in gray.

indices have been comprehensively introduced in the related Ref. [40–43].

We conducted two tests to investigate the early warning ability of all indices. In Test 1, we use data from January 1, 1996 to December 31, 2013 to make predictions. In Test 2, we use complete sample data to make predictions of all the ten influential financial crises. Considering that Test 1 involves an important period that includes the most destructive financial crises, e.g., the 1997 Asian financial crisis, the 2007 subprime crisis, and the 2010 European sovereign debt crisis, a better early warning indicator should have better performance in Test 1. More importantly, a robust indicator should obtain similar performance in both tests. As mentioned in *Early Warning Performance Evaluation*, we selected five criteria to fully express the early warning ability: area under the receiver operating characteristic curve (AUC), accuracy (A), coverage rate (CR), F1 score, and F2 score [37, 38]. We examine the early warning ability with a lead time of 0–400 trading days for each index and record the highest score and corresponding time (denoted as AUC.t, A.t, CR.t, F1.t, and F2.t). To provide a more intuitive presentation, we drew a color bubble chart to visualize the results, as shown in **Figure 3**; the detailed results are in the **Supplementary Material**.

When evaluating an early warning indicator, it is difficult to strike a balance between A and CR. Our purpose is to predict the influential financial crises that may result in grievous economic and social losses if underreported, so we think CR weighs higher than A and pay more attention to F2. Moreover, it is well known that a better early warning indicator should have a higher AUC. Therefore, we pay more attention to AUC and F2. As shown in **Figure 3**, the indices in the upper right corner of the plots perform better than the others. In Test 1, MT.D, MT.E, and AOD have higher AUC and F2 than other indicators. In addition, the lead times of MT. D and MT.E are longer than AOD. This observation indicates that our MTI indicators have better performance than others. In Test 2, the performance of all early warning indicators is changed more or less compared to Test 1. Among them, M1-M13 had the highest AUC in Test 2 but had a median AUC in Test 1. Considering that their performance is quite different between Test 1 and Test 2, such quantity measurements have less robustness. Moreover, their F2 and CR are relatively low, reducing their efficiency in early warning financial crises. Therefore, they are not the best early warning indicators. For the other indicators, VIX had the highest AUC, and TV had a higher CR. Among the network-based indices, AOD, EN, and NN have comparable AUCs with VIX; however, their CR is lower than those of VIX and TV. In contrast, MT. D and MT.E have close AUC with VIX and still have the highest F2. All results prove that our MTI indicators perform better than the benchmarks and other network-based indices.

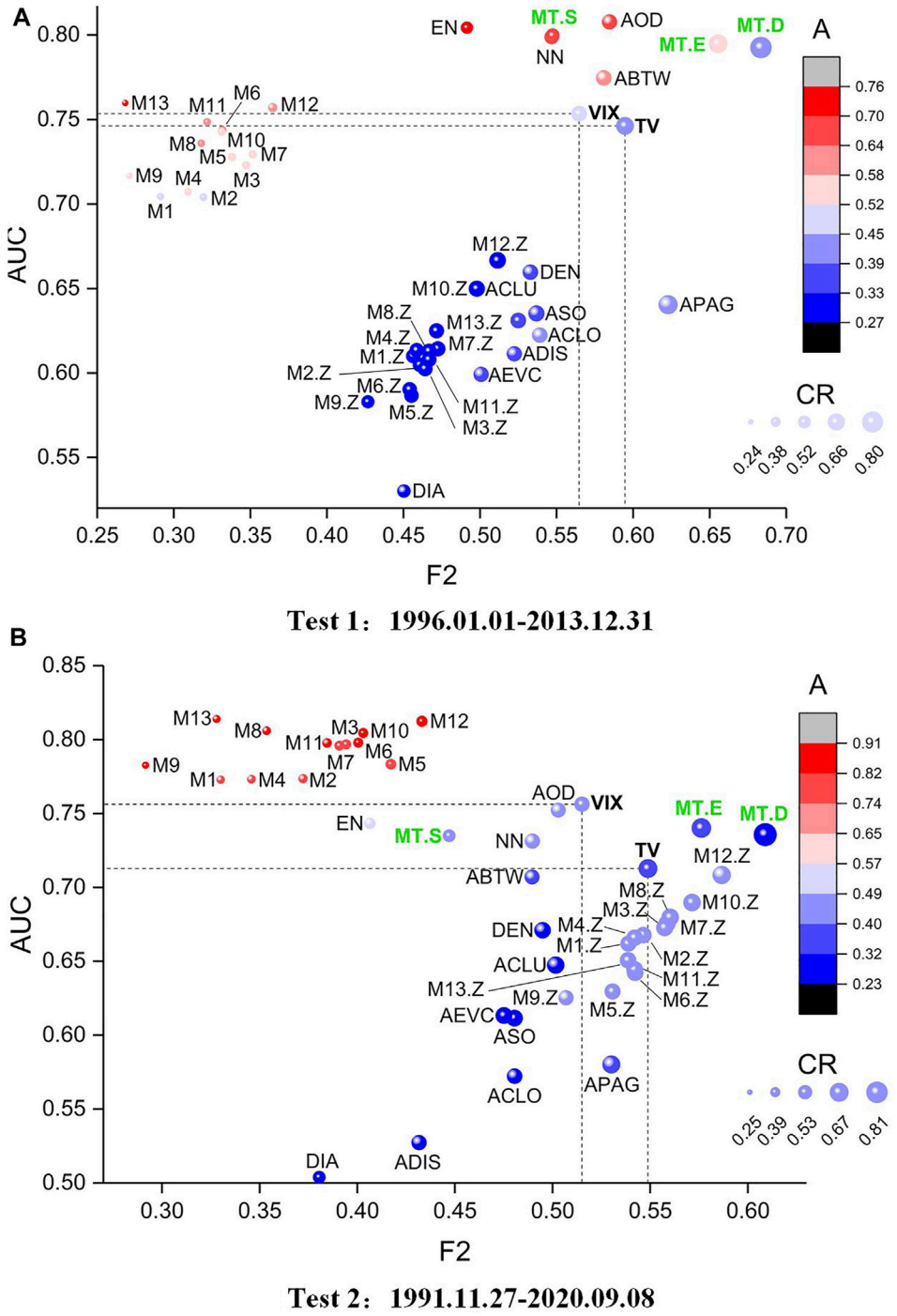


FIGURE 3 | Visualization of the results of the horse race. We use AUC and F2 as the y- and x-axes and CR and A for auxiliary analysis. The drop lines highlight the AUC and F2 of the two benchmarks. The labels of the three proposed MTI indicators (MT.S, MT.E, MT.D) are marked in green. **(A)** Test 1:1996.01.01-2013.12.31. **(B)** Test 2:1991.11.27-2020.09.08.

CONCLUSION

This study introduces motif transition intensity as a novel network-based approach to provide an early warning against financial crises. It provides a new perspective to detect early warning signals by analyzing the microstructure and marginal change of the volatility spillover network. We adopt three intensity measures to develop three indicators: MT.S, MT.D, MT.E. By conducting a horse race, the proposed indicators are shown to have better early warning abilities than VIX and the other 39 network-based indicators. More specifically, the proposed indicators can provide efficient and comprehensible

warning signals for influential global financial crises and even impactive socioeconomic events, which serve as a component in hybrid data-driven warning systems. Furthermore, the application of the proposed indicators can be extended beyond financial systems. Since crisis signals may embed in the time series of many other vital socioeconomic areas, the applications may reach climate and social systems, e.g., climate change, political conflicts, and pandemic influenza.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. This data can be found here: https://www.wind.com.cn/.

AUTHOR CONTRIBUTIONS

ZW, XG, and ZD designed the research. ZW, CH, SH, and SL performed the computations. SL compiled the dataset. ZW and SL prepared the figures and tables. ZW and RT analyzed the results. ZW, SL, CH, and ZD wrote the manuscript. All authors have read and approved the manuscript.

FUNDING

This research is supported by the China Postdoctoral Science Foundation (Grant No. 2020M680435), the National Natural Science Foundation of China (Grant Nos 71731002, 41801106, 71991485, 71991481, and 71991480), the Fundamental Research Funds for the Central Universities (Grant Nos 2652018247 and 2652019085), and the German Ministry for Education and Research (BMBF Grant No. 03EK3055B).

ACKNOWLEDGMENTS

The authors would like to express their gratitude to Prof. Ying Fan, Dr. Bowen Sun, Dr. Qingru Sun, and Dr. Xueyong Liu, who provided valuable suggestions.

SUPPLEMENTARY MATERIAL

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fphy.2021.800860/full#supplementary-material

REFERENCES

1. Scheffer M, Carpenter SR, Lenton TM, Bascompte J, Brock W, Dakos V, et al. Anticipating Critical Transitions. *Science* (2012) 338(6105):344–8. doi:10.1126/science.1225244
2. Shai S, Kenett DY, Kenett YN, Faust M, Dobson S, Havlin S Critical Tipping point Distinguishing Two Types of Transitions in Modular Network Structures. *Phys Rev E* (2015) 92(6):062805. doi:10.1103/PhysRevE.92.062805
3. Jurczyk J, Rehberg T, Eckrot A, Morgenstern I Measuring Critical Transitions in Financial Markets. *Sci Rep* (2017) 7(1):11564. doi:10.1038/s41598-017-11854-1
4. Diks C, Hommes C, Wang J Critical Slowing Down as an Early Warning Signal for Financial Crises. *Empir Econ* (2019) 57(4):1201–28. doi:10.1007/s00181-018-1527-3
5. Billio M, Getmansky M, Lo AW, Pelizzon L Econometric Measures of Connectedness and Systemic Risk in the Finance and Insurance Sectors. *J Financial Econ* (2012) 104(3):535–59. doi:10.1016/j.jfineco.2011.12.010
6. Sandhu RS, Georgiou TT, Tannenbaum AR Ricci Curvature: An Economic Indicator for Market Fragility and Systemic Risk. *Sci Adv* (2016) 2(5): e1501495. doi:10.1126/sciadv.1501495
7. Gai P, Kapadia S Networks and Systemic Risk in the Financial System. *Oxford Rev Econ Pol* (2019) 35(4):586–613. doi:10.1093/oxrep/grz023
8. Martinez-Jaramillo S, Carmona CU, Kenett DY Interconnectedness and Financial Stability. *J Risk Manag Financial Institutions* (2019) 12:168–83.
9. Samal A, Kumar S, Yadav Y, Chakraborti A Network-centric Indicators for Fragility in Global Financial Indices. *Front Phys* (2021) 8:624373. doi:10.3389/fphy.2020.624373
10. Li Y, Zhuang X, Wang J, Zhang W Analysis of the Impact of Sino-US Trade Friction on China's Stock Market Based on Complex Networks. *North Am J Econ Finance* (2020) 52:101185. doi:10.1016/j.najef.2020.101185
11. Gao Y-C, Wei Z-W, Wang B-H Dynamic Evolution of Financial Network and its Relation to Economic Crises. *Int J Mod Phys C* (2013) 24(2):1350005–10. doi:10.1142/S0129183113500058
12. Kuyyamudi C, Chakrabarti AS, Sinha S Emergence of Frustration Signals Systemic Risk. *Phys Rev E* (2019) 99(5):052306. doi:10.1103/PhysRevE.99.052306
13. Kukreti V, Pharasi HK, Gupta P, Kumar S A Perspective on Correlation-Based Financial Networks and Entropy Measures. *Front Phys* (2020) 8:00323. doi:10.3389/fphy.2020.00323
14. Yang M-Y, Ren F, Li S-P Stock Network Stability after Crashes Based on Entropy Method. *Front Phys* (2020) 8:00163. doi:10.3389/fphy.2020.00163
15. Bardoscia M, Battiston S, Caccioli F, Caldarelli G Pathways towards Instability in Financial Networks. *Nat Commun* (2017) 8:14416. doi:10.1038/ncomms14416
16. Dey AK, Gel YR, Poor HV What Network Motifs Tell Us about Resilience and Reliability of Complex Networks. *Proc Natl Acad Sci USA* (2019) 116(39): 19368–73. doi:10.1073/pnas.1819529116
17. Yu S, Feng Y.-F., Zhang D, Bedru HD, Xu B, Xia F Motif Discovery in Networks: A Survey. *Comp Sci Rev* (2020) 37:100267. doi:10.1016/j.cosrev.2020.100267
18. Mursa B-E -M, Dioşan L, Andreica A Network Motifs: A Key Variable in the Equation of Dynamic Flow between Macro and Micro Layers in Complex Networks. *Knowledge-Based Syst* (2021) 213:106648. doi:10.1016/j.knosys.2020.106648
19. Angulo MT, Liu Y-Y, Slotine J-J Network Motifs Emerge from Interconnections that Favour Stability. *Nat Phys* (2015) 11(10):848–52. doi:10.1038/nphys3402
20. Wunderling N, Stumpf B, Krönke J, Staal A, Tuinenburg OA, Winkelmann R, et al. How Motifs Condition Critical Thresholds for Tipping Cascades in Complex Networks: Linking Micro- to Macro-Scales. *Chaos* (2020) 30(4): 043129. doi:10.1063/1.5142827
21. Xie W-J, Yong Y, Wei N, Yue P, Zhou W-X Identifying States of Global Financial Market Based on Information Flow Network Motifs. *North Am J Econ Finance* (2021) 58:101459. doi:10.1016/j.najef.2021.101459
22. Squartini T, van Lelyveld I, Garlaschelli D Early-warning Signals of Topological Collapse in Interbank Networks. *Sci Rep* (2013) 3:3357. doi:10.1038/srep03357
23. Chen D.-D., Guo X.-C., Wang J.-J., Liu J.-T., Zhang Z.-H., Hancock ER Thermodynamic Motif Analysis for Directed Stock Market Networks. *Pattern Recognition* (2021) 114:107872. doi:10.1016/j.patcog.2021.107872
24. Benson AR, Gleich DF, Leskovec J Higher-order Organization of Complex Networks. *Science* (2016) 353(6295):163–6. doi:10.1126/science.aad9029
25. Gatfaoui H, de Peretti P Flickering in Information Spreading Precedes Critical Transitions in Financial Markets. *Sci Rep* (2019) 9:5671. doi:10.1038/s41598-019-42223-9
26. Milo R, Shen-Orr S, Itzkovitz S, Kashtan N, Chklovskii D, Alon U Network Motifs: Simple Building Blocks of Complex Networks. *Science* (2002) 298(5594):824–7. doi:10.1126/science.298.5594.824

27. Filatova T, Polhill JG, van Ewijk S Regime Shifts in Coupled Socio-Environmental Systems: Review of Modelling Challenges and Approaches. *Environ Model Softw* (2016) 75:333–47. doi:10.1016/j.envsoft.2015.04.003
28. Liu S.-Y., Huang S.-P., Chi Y.-X., Feng S.-D., Li Y, Sun Q.-R. Three-level Network Analysis of the North American Natural Gas price: A Multiscale Perspective. *Int Rev Financial Anal* (2020) 67:101420. doi:10.1016/j.irfa.2019.101420
29. Li W.-W., Hommel U, Paterlini S Network Topology and Systemic Risk: Evidence from the Euro Stoxx Market. *Finance Res Lett* (2018) 27:105–12. doi:10.1016/j.frl.2018.02.016
30. Mensi W, Boubaker FZ, Al-Yahyaee KH, Kang SH Dynamic Volatility Spillovers and Connectedness between Global, Regional, and GIPSI Stock Markets. *Finance Res Lett* (2018) 25:230–8. doi:10.1016/j.frl.2017.10.032
31. Silva TC, de Souza SRS, Tabak BM Structure and Dynamics of the Global Financial Network. *Chaos, Solitons & Fractals* (2016) 88:218–34. doi:10.1016/j.chaos.2016.01.023
32. Lee TK, Cho JH, Kwon DS, Sohn SY Global Stock Market Investment Strategies Based on Financial Network Indicators Using Machine Learning Techniques. *Expert Syst Appl* (2019) 117:228–42. doi:10.1016/j.eswa.2018.09.005
33. Samitas A, Kampouris E, Kenourgios D Machine Learning as an Early Warning System to Predict Financial Crisis. *Int Rev Financial Anal* (2020) 71:101507. doi:10.1016/j.irfa.2020.101507
34. Wang Z, Gao X.-Y., An H.-Z., Tang R.-W., Sun Q.-R. Identifying Influential Energy Stocks Based on Spillover Network. *Int Rev Financial Anal* (2020) 68:101277. doi:10.1016/j.irfa.2018.11.004
35. Kauê Dal'Maso Peron T, da Fontoura Costa L, Rodrigues FA The Structure and Resilience of Financial Market Networks. *Chaos* (2012) 22(1):013117. doi:10.1063/1.3683467
36. Zhou R.-X., Cai R, Tong G.-Q. Applications of Entropy in Finance: A Review. *Entropy* (2013) 15(11):4909–31. doi:10.3390/e15114909
37. Shao Z, Zheng Q.-R., Yang S.-L., Gao F, Cheng M.-L., Zhang Q, et al. Modeling and Forecasting the Electricity Clearing price: A Novel BELM Based Pattern Classification Framework and a Comparative Analytic Study on Multi-Layer BELM and LSTM. *Energ Econ* (2020) 86:104648. doi:10.1016/j.eneco.2019.104648
38. Spelta A, Flori A, Pecora N, Pammolli F Financial Crises: Uncovering Self-Organized Patterns and Predicting Stock Markets Instability. *J Business Res* (2021) 129:736–56. doi:10.1016/j.jbusres.2019.10.043
39. Womack B International Crises and China's Rise: Comparing the 2008 Global Financial Crisis and the 2017 Global Political Crisis. *Chin J Int Polit* (2017) 10(4):383–401. doi:10.1093/cjip/pox015
40. Lü L.-Y., Chen D.-B., Ren X-L, Zhang Q-M, Zhang Y-C, Zhou T Vital Nodes Identification in Complex Networks. *Phys Rep* (2016) 650:1–63. doi:10.1016/j.physrep.2016.06.007
41. León C, Machado C, Sarmiento M Identifying central Bank Liquidity Super-spreaders in Interbank Funds Networks. *J Financial Stab* (2018) 35:75–92. doi:10.1016/j.jfs.2016.10.008
42. Huang C.-X., Wen S.-G., Li M.-G., Wen F.-H., Yang X An Empirical Evaluation of the Influential Nodes for Stock Market Network: Chinese A-Shares Case. *Finance Res Lett* (2021) 38:101517. doi:10.1016/j.frl.2020.101517
43. Xue L.-Y., Zhang P, Zeng A Maximizing Spreading in Complex Networks with Risk in Node Activation. *Inf Sci* (2022) 586:1–23. doi:10.1016/j.ins.2021.11.064

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers in Physics

ORIGINAL RESEARCH
published: 22 February 2022
doi: 10.3389/fphy.2022.839462

Improving the Performance of Reputation Evaluation by Combining a Network Structure With Nonlinear Recovery

Meng Li[1,2], *Chengyuan Han*[3], *Yuanxiang Jiang*[1,2] *and Zengru Di*[1,2]*

[1]International Academic Center of Complex Systems, Beijing Normal University, Zhuhai, China, [2]School of Systems Science, Beijing Normal University, Beijing, China, [3]Institute for Theoretical Physics, University of Cologne, Köln, Germany

Characterizing the reputation of an evaluator is particularly significant for consumers to obtain useful information from online rating systems. Furthermore, overcoming the difficulties of spam attacks on a rating system and determining the reliability and reputation of evaluators are important topics in the research. We have noticed that most existing reputation evaluation methods rely only on using the evaluator's rating information and abnormal behaviour to establish a reputation system, which disregards the systematic aspects of the rating systems, by including the structure of the evaluator-object bipartite network and nonlinear effects. In this study, we propose an improved reputation evaluation method by combining the structure of the evaluator-object bipartite network with rating information and introducing penalty and reward factors. The proposed method is empirically analyzed on a large-scale artificial data set and two real data sets. The results have shown that this method has better performance than the original correlation-based and IARR2 in the presence of spamming attacks. Our work contributes a new idea to build reputation evaluation models in sparse bipartite rating networks.

Keywords: reputation evaluation, spam attack, online rating system, systematic factors, network structure

OPEN ACCESS

Edited by:
Gaogao Dong,
Jiangsu University, China

Reviewed by:
Chengyi Xia,
Tianjin University of Technology, China
Yongwen Zhang,
Kunming University of Science and Technology, China

***Correspondence:**
Zengru Di
zdi@bnu.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *20 December 2021*
Accepted: *14 January 2022*
Published: *22 February 2022*

Citation:
Li M, Han C, Jiang Y and Di Z (2022) Improving the Performance of Reputation Evaluation by Combining a Network Structure With Nonlinear Recovery. Front. Phys. 10:839462. doi: 10.3389/fphy.2022.839462

1 INTRODUCTION

The flourishing development of e-commerce has broad and far-reaching impacts on our daily lives, leading consumers to increasingly rely on using the internet to obtain information about products and services that help them decide how to consume [1–4]. However, with an overwhelming amount of products and services available, potential users may overloaded with information such as that from big data of the quality attributes, performance attributes, and previous reviews [5, 6]. To solve the information overload of users, some e-commerce platforms have implemented online rating systems to help users fuse information, where evaluators are encouraged to present reasonable ratings for the objects [7]. These ratings are representations of the inherent quality of objects and reflections of evaluators' credibility. In reality, current rating systems face many challenges. Unobjective ratings may be given simply because some users are unacquainted with the relevant field or due to their poor judgments [8]. However, unreliable evaluators even deliberately give maximal/minimal ratings for various psychosocial reasons [9–11]. These ubiquitous noises and distorted information purposefully mislead evaluators' choices and decisions and have a wicked effect on the reliability of the online rating systems [12, 13]. Therefore, establishing a reliable and efficient reputation

evaluation system is an extremely urgent task for an online rating system, which has a huge impact not only against spam attacks but also on the economy and society [14, 15].

In various evaluation systems, the reputation management of evaluators contributes to social governance. For instance, as an important platform for providing health services, online health communities are favoured by both physicians and patients as these communities establish an effective service channel between them [16]. In the evaluation of research funding applications, peer reviewers must distinguish the best applications from relatively weaker ones to appropriately allocate funding. Only peer reviewers with a good reputation can correctly guide the highly competitive allocation of limited resources [17, 18]. Moreover, the online reputation system for job seekers helps employers better understand job seekers and decide whether to hire them [19]. Similar problems exist in other scenarios, e.g., recommendations, selection, and voting, in which the credibility of the evaluators will affect the final result. One of the most important ways to solve this problem is by building reputation-evaluation systems [20–23].

Over the past decades, researchers have been increasingly interested in modelling reputations on web-based rating platforms [24, 25]. The earlier method of measuring the reputation of online evaluators is the iterative refinement (IR) algorithm designed by Laureti [26]. The correlation-based ranking (CR) method proposed in [27] by Zhou et al. is the most representative method, and it is robust against spam attacks. Very recently, the IARR2 algorithm was proposed by introducing two penalty factors to improve the CR method [28]. These aforementioned methods are based on the assumption that each rating given by the evaluators is the most objective reflection of the quality of the objects. Another kind of thinking is to consider the behavioural features of the evaluators in bipartite networks. Gao et al. proposed group-based ranking (GR) and iterative group-based ranking (IGR) algorithms, which group evaluators according to their ratings [29, 30] and measure the evaluators' reputation according to the sizes of the corresponding groups [31]. Other scholars employed the deviation-based ranking (DR) method to model evaluators' reputation [32], and Sun et al. combined this method with GR to construct the iterative optimization ranking (IOR) [33]. In addition, there are some other methods, such as the Bayesian-based method [7, 34] and others [35]. One can also read the review literature on reputation systems [36] for further insight.

Nevertheless, most existing reputation evaluation algorithms neglect the systematic aspects of the rating systems, especially the structural information of the evaluator-object bipartite network and nonlinear effects, both of which are core factors in complex systems. Considering that these factors lead to some new ideas to improve the classical CR method, in this paper, we introduce a new reputation evaluation method by combining the CR method with the clustering coefficient of evaluators in the evaluator-object bipartite network. Meanwhile, we also believe that if an evaluator has a relatively high reputation, he should receive some rewards to enhance his reputation further, and vice versa. Therefore, we construct a penalty reward function to update the weight of the evaluator's reputation. Extensive experiments on artificial data and two well-known real-world datasets suggest that the proposed method has higher accuracy and recall score of spammer identification. Its overall performance exceeds that of the classical CR method.

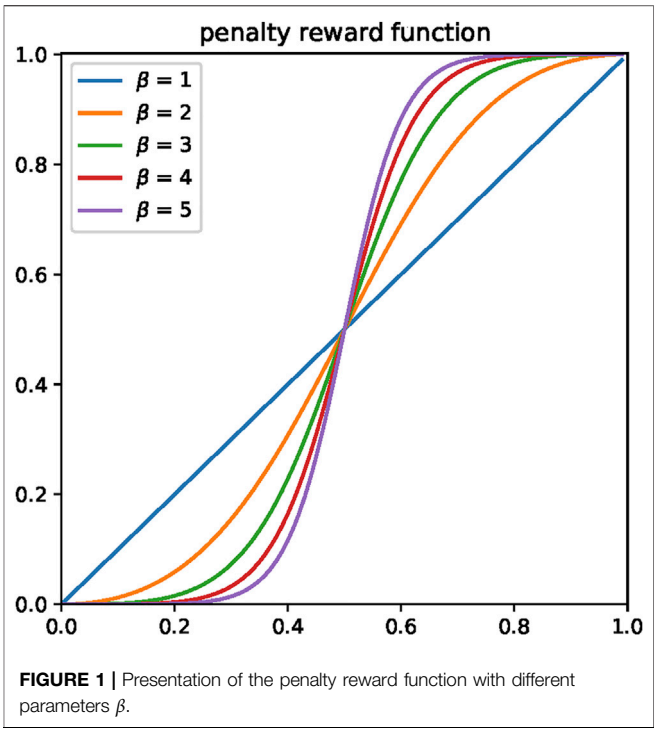


FIGURE 1 | Presentation of the penalty reward function with different parameters β.

The remainder of this paper is organized as follows. The proposed reputation-evaluation method is described in detail in **Section 2**. **Section 3** introduces the data and evaluation metrics. The experimental study and results are discussed and analysed in **Section 4**. Finally, conclusions are given in **Section 5**.

2 METHODS

We first briefly introduce some basic notations for online rating systems, which can be naturally represented as a weighted evaluator-object bipartite network. The set of evaluators is denoted E, and the set of objects is denoted O. The numbers of evaluators and objects are recorded as $|E|$ and $|O|$, respectively. We use Latin and Greek letters for evaluator-related and object-related indices, respectively. The degree of evaluator i and object α are indicated by k_i and k_α, respectively. The weight of the link in the bipartite network is the rating given by evaluator i to object α, denoted by $r_{i\alpha}$, and $r_{i\alpha} \in (0, 1)$. The set E_α describes the evaluators who rate object α, and the set O_i defines the objects rated by evaluator i.

A reputation value R_i should be assigned to each evaluator i by a reputation evaluation method. This value measures the evaluator's ability to reflect the intrinsic quality of the objects or items accurately, known as credibility. Similarly, each object α has a true quality that most objectively reflects its character. However, in practice, it is extremely challenging for us to

determine the intrinsic quality of an object, and we usually estimate quality Q_α with the weighted average of the ratings that object α has obtained. It is shown as

$$Q_\alpha = \frac{\sum_{i\in E_\alpha} R_i r_{i\alpha}}{\sum_{i\in E_\alpha} R_i}, \tag{1}$$

where the initial reputation of each evaluator is set as $R_i = k_i/|O|$.

Second, the CR method defines that the reputation is measured by the correlation between the rating vector from the evaluator and the corresponding quality vectors of the objects. We calculate the evaluator's temporary reputation as

$$TR_i = \frac{1}{k_i}\Sigma_{\alpha\in O_i}\left(\frac{r_{i\alpha}-\bar{r}_i}{\sigma_{r_i}}\right)\left(\frac{Q_\alpha-\bar{Q}_\alpha}{\sigma_{Q_\alpha}}\right), \tag{2}$$

where σ_{r_i} and σ_{Q_α} are, respectively, the standard deviations of the rating vector of evaluator i and the corresponding objects' quality vector, and $\bar{r}_i$ and $\bar{Q}_\alpha$ are their mean values. TR_i is reset to 0 if TR_i is less than 0 so that TR_i is limited in the range [0,1].

Next, we expect to refine the evaluator's reputation. In principle, when an evaluator rates the objects that are also familiar by the other evaluators, this evaluator is more likely to have a high reputation due to the popularity of these objects. As we mentioned in the introduction section, the clustering coefficient in the bipartite graph network are employed to refine the reputation of evaluators. Despite the one-mode projection network providing the interaction between each group member, it should be noted that substantial information may disappear after projection [37]. This paper adopts the concept of the clustering coefficient extended by Latapy et al. [37], who first defines the clustering coefficient for pairs of nodes cc (e_i, e_j). Mathematically, it reads

$$cc\left(e_i, e_j\right) = \frac{|N(e_i)\cap N\left(e_j\right)|}{|N(e_i)\cup N\left(e_j\right)|}. \tag{3}$$

Here, $N(e_i)$ denotes the objects evaluated by evaluator i, i.e., the neighbours of node i, and $|\cdot|$ denotes the number of elements in the set. Then, the clustering coefficient for one node is expressed as

$$cc(e_i) = \frac{\sum_{e_j\in N(N(e_i))} cc\left(e_i, e_j\right)}{|N(N(e_i))|} \tag{4}$$

We now refine the reputation of evaluators according to the clustering coefficient of each evaluator. This modified method is referred to as CRC, and can be expressed as follows:

$$TR_i' = \left(\frac{cc(e_i)}{\max\left\{cc\left(e_j\right)\right\}}\right)^{\frac{1}{2}} TR_i. \tag{5}$$

For evaluators with different reputation values, their credibility is different, so we rescale their reputation by nonlinear recovery. The penalty-reward function is used to update evaluators' reputation, which will allocate higher reputation as a reward to evaluators with a high reputation. In contrast, a penalty is given to further reduce the reputation of evaluators with a low reputation. The function is

$$R_i = \begin{cases} 0 & if \quad TR_i' = 0, \\ \left[1+\left(\frac{1}{TR_i'}-1\right)^{\beta}\right]^{-1} & if \quad 0 < TR_i' < 1, \\ 1 & if \quad TR_i' = 1. \end{cases} \tag{6}$$

This enhanced method is referred to as CRCN, and the function image is shown in **Figure 1**. The CRCN method will degrade to CRC when $\beta = 1$.

The evaluator reputation R_i and the quality of object Q_α are iteratively updated using **eqs. (1) to (6)** until the change of the quality $|Q - Q''|$ is less than the threshold value, and it is calculated in **Eq. 7**. In the process of reputation updating, the reputation of evaluators with higher clustering coefficient will be more rewards through nonlinear recovery, and vice versa. The effects of refining the reputation and estimating the quality are gradually accumulated in each step of the recurring algorithm.

$$|Q - Q''| = \frac{1}{|O|}\Sigma_{\alpha\in O}\left(Q_\alpha - Q_\alpha''\right)^2, \tag{7}$$

where Q'' is the quality from the previous step, and the threshold is set as 10^{-6}.

Finally, we sort evaluators in ascending order according to their reputation value, and the evaluators with L smallest reputation values are identified as spammers.

TABLE 1 | Basic statistical properties of the real datasets used in this paper, where $\langle k_u\rangle$ and $\langle k_o\rangle$ are the average degree of evaluators and objects.

Dataset	$\|E\|$	$\|O\|$	$\langle k_e\rangle$	$\langle k_o\rangle$	Sparsity
MovieLens	943	1,682	106	60	0.063
Netflix	4,960	17 237	295	85	0.017

3 DATA AND METRICS

3.1 Artificial Rating Data

To generate the artificial dataset, we generate a bipartite network with 6,000 evaluators and 4,000 objects, i.e., $|E| = 6{,}000$ and $|O| = 4{,}000$. The network sparsity is set as $\eta = 0.02$, which means that the total number of weighted links (ratings) is $0.02 \times |E||O| = 4.8 \times 10^5$. We employ the preferential attachment mechanism [38] to choose a pair of evaluator and object and add a link between them. At each time step t, the probabilities of selecting evaluator i and object α are

$$p_i(t) = \frac{k_i(t)+1}{\Sigma_{j\in E}\left(k_j(t)+1\right)}$$
$$p_\alpha(t) = \frac{k_\alpha(t)+1}{\Sigma_{\beta\in O}\left(k_\beta(t)+1\right)},$$

where $k_i(t)$ and $k_\alpha(t)$ are the degrees of evaluator i and object α at time step t.

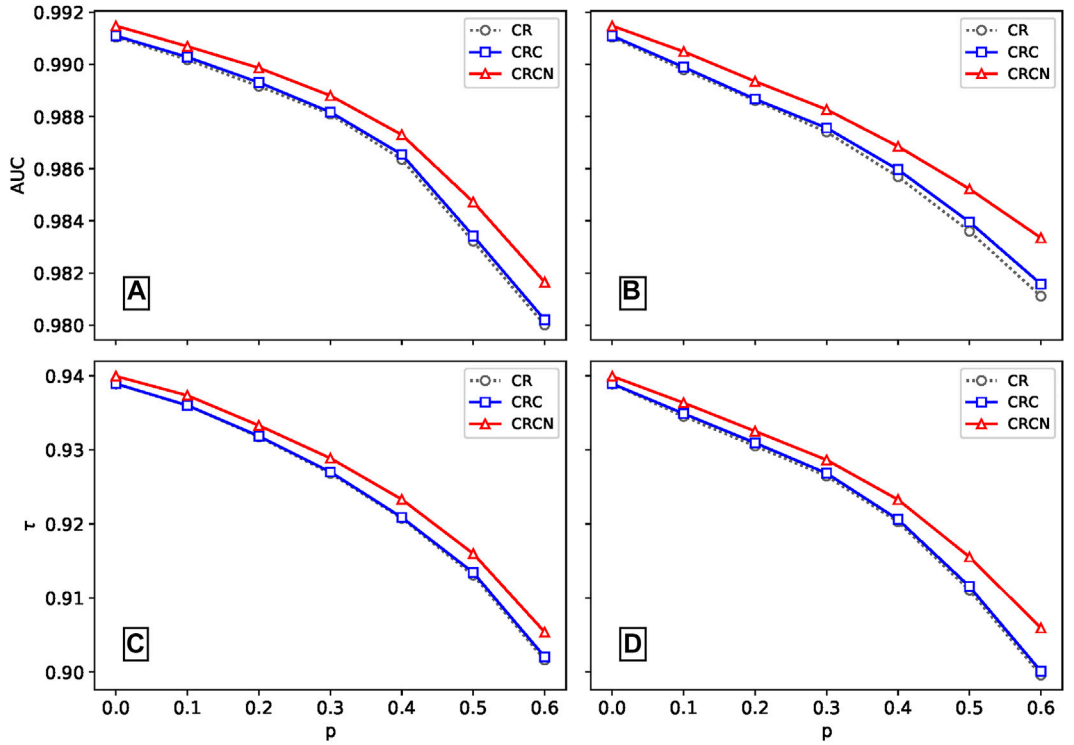


FIGURE 2 | Comparison of the robustness of the three algorithms. Panels **(A)** and **(C)** are the AUC and τ for different fractions p for random rating spamming, and panels **(B)** and **(D)** show the same for malicious rating spamming. The results are averaged over ten independent realizations.

We suppose that the rating $r_{i\alpha}$ given by evaluator i to object α is composed of the intrinsic quality of object Q'_α and the rating error $\delta_{i\alpha}$. The objects' qualities obey the uniform distribution U (0, 1), and the evaluators' rating errors are drawn from the normal distribution N (0, δ_i). δ_i indicates the rating error of evaluator i, and it is generated from a uniform distribution U ($\delta_{\min}$, $\delta_{\max}$). In the simulation, we set $\delta_{\min} = 0.1$ and $\delta_{\max} = 0.5$. Accordingly, the rating $r_{i\alpha}$ is defined as

$$r_{i\alpha} = Q'_\alpha + \delta_{i\alpha}. \tag{8}$$

Both evaluators' ratings and objects' qualities are limited to the range (0, 1).

3.2 Real Rating Data

We consider two commonly studied datasets in real online rating systems—MovieLens and Netflix, which contain ratings for movies provided by GroupLens (www.grouplens.org) and Netflix Prize (www.netflixprize.com), respectively—to investigate the effectiveness and accuracy of the proposed methods. These two datasets are given by integer ratings scaling from 1 to 5, with 1 being the worst and 5 being the best. Herein, we sample a subset from the original datasets in which each evaluator has at least 20 ratings. **Table 1** presents some basic statistical properties for these two datasets.

It is well known that ranking all evaluators and comparing them with the ground truth is an effective way to measure the performance of different evaluation algorithms. However, in real systems, there are no ground-truth ranks for evaluators. We manipulate the real dataset by randomly selecting some evaluators and assigning them as artificial spammers to test the proportion of these spammers detected by an evaluation method. In the implementation, we randomly select ρ fractions of evaluators and turn them into spammers by replacing their original ratings with distorted ratings: random integers in the set (1, 2, 3, 4, 5) for random spammers or integer 1 or 5 for malicious spammers. Thus, the number of spammers is $d = \rho|E|$. We also set $\omega = k/|O|$ as the activity of spammers; here, k is the degree of each spammer and is a tuneable parameter. If a spammer's original degree $k_i \geq k$, then k ratings are randomly selected and replaced with distorted ratings, and the unselected $k_i - \omega|O|$ ratings are ignored; if $k_i < k$, we first replace all the spammer's original ratings and randomly select $k - k_i$ of his/her unrated ratings and assign them with distorted ratings.

3.3 Evaluation Metrics

To evaluate the robustness and effectiveness of the reputation-evaluation methods, we adopt four widely used metrics: Kendall's tau [39], AUC (the area under the ROC curve) [40], recall [41], and ranking score [42].

Kendall's tau (τ) measures the rank correlation between the estimated quality of objects Q and their intrinsic quality Q':

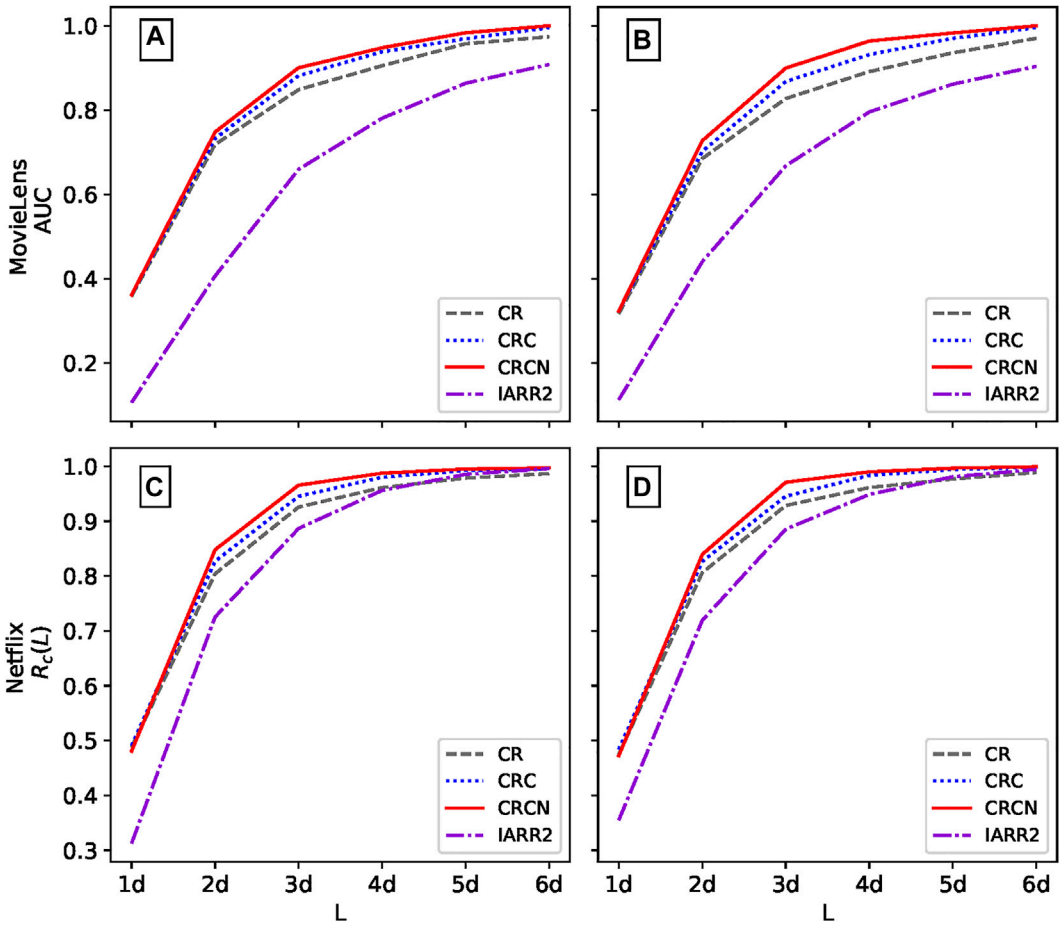


FIGURE 3 | The recall score R_c of different methods varies with length L in MovieLens and Netflix. Panels **(A)** and **(C)** represent random spammers, and panels **(B)** and **(D)** represent malicious spammers. The parameter ρ in both datasets is 0.05, and the parameter ω is 0.05 and 0.01 for MovieLens and Netflix, respectively. The results are averaged over ten independent realizations.

TABLE 2 | AUC and RS values of different methods on two real datasets (A) with random spammers and (B) with malicious spammers. The parameters ω and ρ are the same as those in **Figure 3**. The results are averaged over ten independent realizations. The most remarkable value in each row is emphasized in bold.

(a)	Data set	AUC				RS			
		CR	CRC	CRCN	IARR2	CR	CRC	CRCN	IARR2
	MovieLens	0.918 3	0.923 6	**0.925 2**	0.866 4	0.084 6	0.079 5	**0.078 0**	0.146 0
	Netflix	0.932 9	0.938 3	**0.940 0**	0.923 9	0.067 5	0.062 4	**0.060 8**	0.080 1
(b)	**Data set**	**AUC**				**RS**			
		CR	**CRC**	**CRCN**	**IARR2**	**CR**	**CRC**	**CRCN**	**IARR2**
	MovieLens	0.912 7	0.921 3	**0.925 3**	0.865 4	0.090 8	0.083 9	**0.080 6**	0.143 6
	Netflix	0.932 4	0.938 0	**0.939 7**	0.922 8	0.068 0	0.062 3	**0.060 9**	0.079 0

$$\tau = \frac{2}{|O|(|O|-1)} \Sigma_{\alpha<\beta} \mathrm{sgn}\left[\left(Q_\alpha - Q_\beta\right)\left(Q'_\alpha - Q'_\beta\right)\right], \qquad (9)$$

where $(Q_\alpha - Q_\beta)(Q'_\alpha - Q'_\beta) > 0$ indicates concordance and $(Q_\alpha - Q_\beta)(Q'_\alpha - Q'_\beta) < 0$ indicates discordance. Higher τ values indicate a more accurate measurement of object quality, and $\tau \in [-1, 1]$.

AUC measures the accuracy of the reputation evaluation methods. In artificial datasets, one can select a part of high-quality objects as benchmark objects, and the remaining objects are regarded as nonbenchmark objects. Here, we select 5% of the highest-quality objects as the benchmark objects. Nevertheless, in empirical datasets, as mentioned above, we randomly designate some evaluators as spammers. When the reputation of all

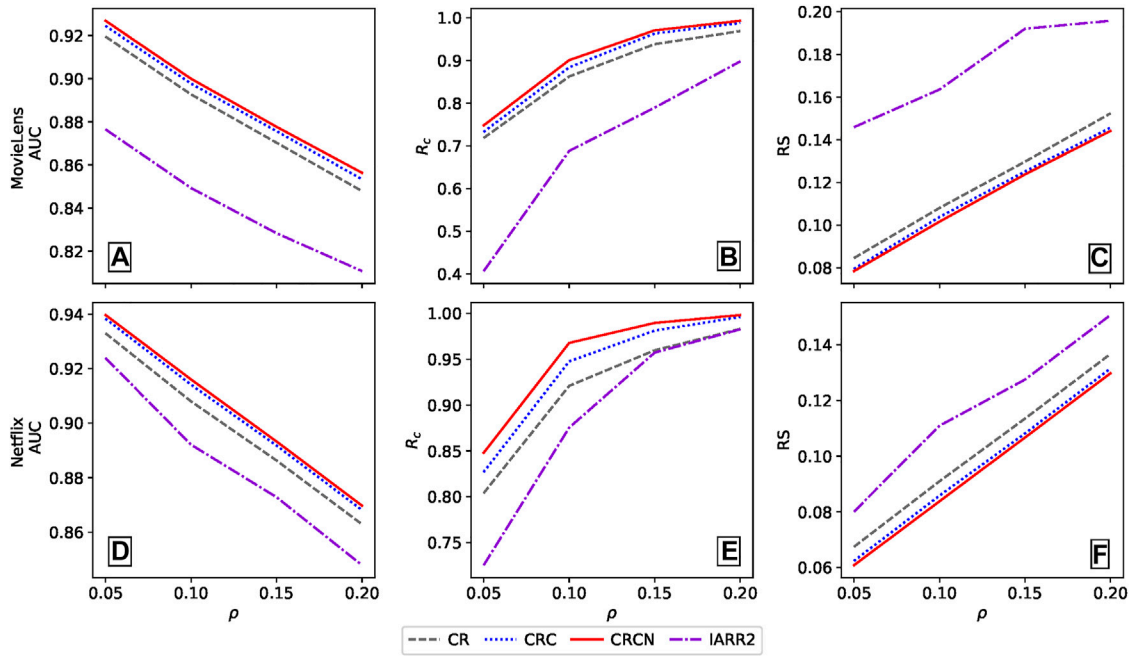


FIGURE 4 | The AUC, R_c and RS values of different methods with different ρ in the random spammer case for **(A-C)** MovieLens and **(D-F)** Netflix datasets. The parameter ω is 0.05 and 0.01 for MovieLens and Netflix, respectively. The results are averaged over 10 independent realizations.

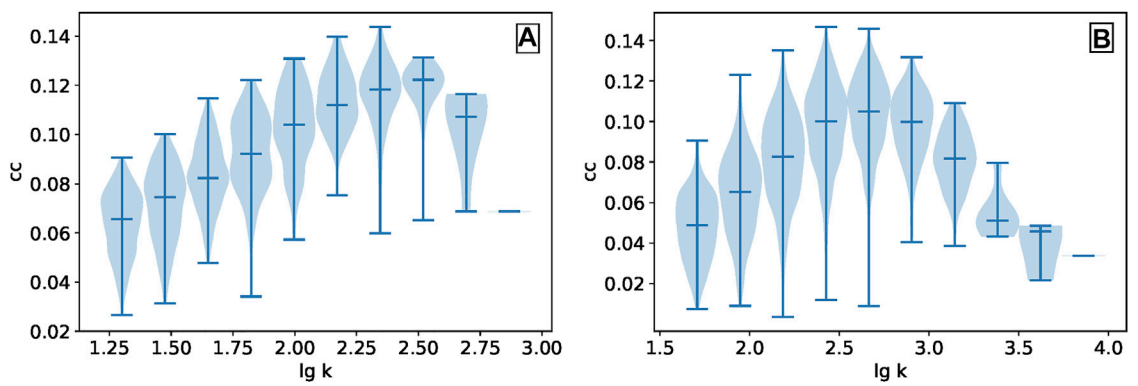


FIGURE 5 | The relationship between the evaluators' degree and the clustering coefficient in **(A)** MovieLens and **(B)** Netflix are presented by a violin plot. The evaluators in each dataset are divided into ten bins according to their degrees. The extreme value and median are marked with short bars, and the probability density is represented by shadows.

evaluators is provided, the AUC value can essentially be interpreted as the probability that the reputation of a randomly chosen normal evaluator is higher than the reputation of a randomly selected spammer. To calculate the AUC values, we control N independent comparisons of the reputations of a pair of normal evaluator and spammer and record N' as the number of times the spammer has a lower reputation and N'' as the number of times the spammer has the same reputation. Then, the value of AUC is defined as

$$AUC = \frac{N' + N''}{N}. \tag{10}$$

Therefore, the higher the AUC is, the more accurate the evaluation method is. If the AUC value is 0.5, it indicates that the method is randomly ranked for all evaluators.

The recall describes the proportion of spammers that can be identified among L evaluators with the lowest reputation. Mathematically, it can be defined as

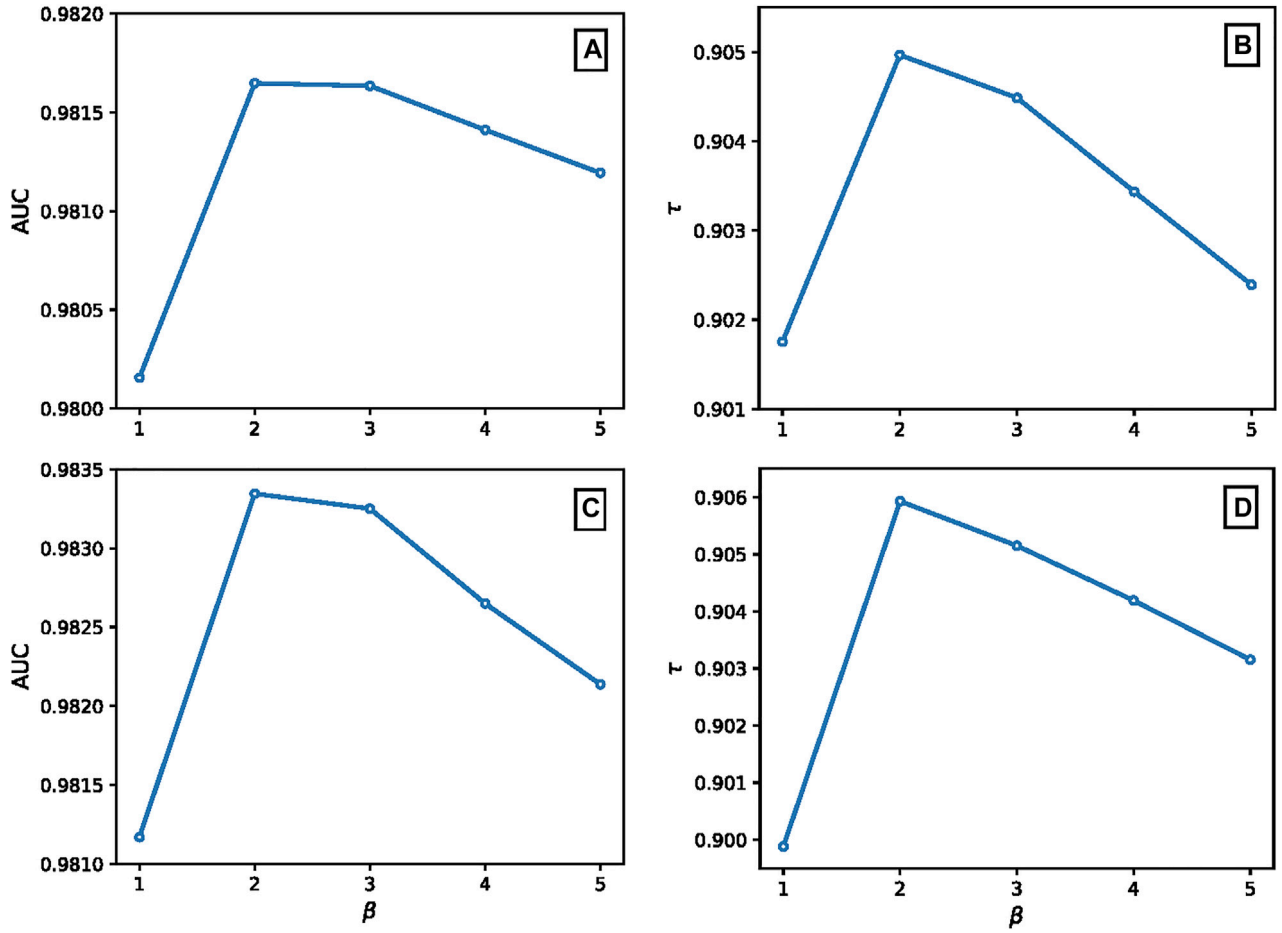


FIGURE 6 | The dependence of AUC and τ on the parameter β in CRCN method. Panels **(A)** and **(B)** show the AUC and τ values for different β with random-rating spamming, and panels **(C)** and **(D)** show the same for push-rating spamming. The results are averaged over ten independent realizations.

$$R_c(L) = \frac{d'(L)}{d}, \tag{11}$$

where $d'(L)$ is the number of detected spammers in the L lowest ranking list, and the range of R_c is [0, 1]. A higher R_c indicates a higher accuracy for reputation ranking.

The ranking score (RS) characterizes the effect of evaluation methods by focusing more on the influence of ranking position. Given the ranking of all evaluators, we measure the position of all spammers in the evaluator ranking list. The ranking score is obtained by averaging the rankings of all spammers, and the specific formula is as follows:

$$RS = \frac{1}{d}\Sigma_{i\in E_s}\frac{l_i}{|E|}, \tag{12}$$

where l_i indicates the rank of spammer i in the evaluator ranking list, and E_s denotes the set of spammers. Accordingly, RS has the range [0, 1]. A good evaluation algorithm is expected to give the spammer a higher rank, which causes a small ranking score. The smaller the RS is, the higher the ranking accuracy, and vice versa.

4 RESULTS AND DISCUSSION

We analyse the performance of the two proposed algorithms for the artificial dataset and two commonly studied empirical datasets and compare them with the classical CR algorithm and IARR2 algorithm.

4.1 Results From Artificial Rating Data

A well-performing evaluation algorithm should defend against any distorted information. We first calculate the values of Kendall's tau τ and AUC on the generated artificial rating data, including spammers, to investigate the robustness of the proposed two methods and the original CR method in protecting against different spammers. We suppose there are two types of distorted ratings: random ratings and malicious ratings. Random ratings mainly come from mischievous evaluators who provide arbitrary and meaningless rating values, and malicious ratings indicate that spammers always give maximum or minimum allowable rating values to push the target object's rating up or down.

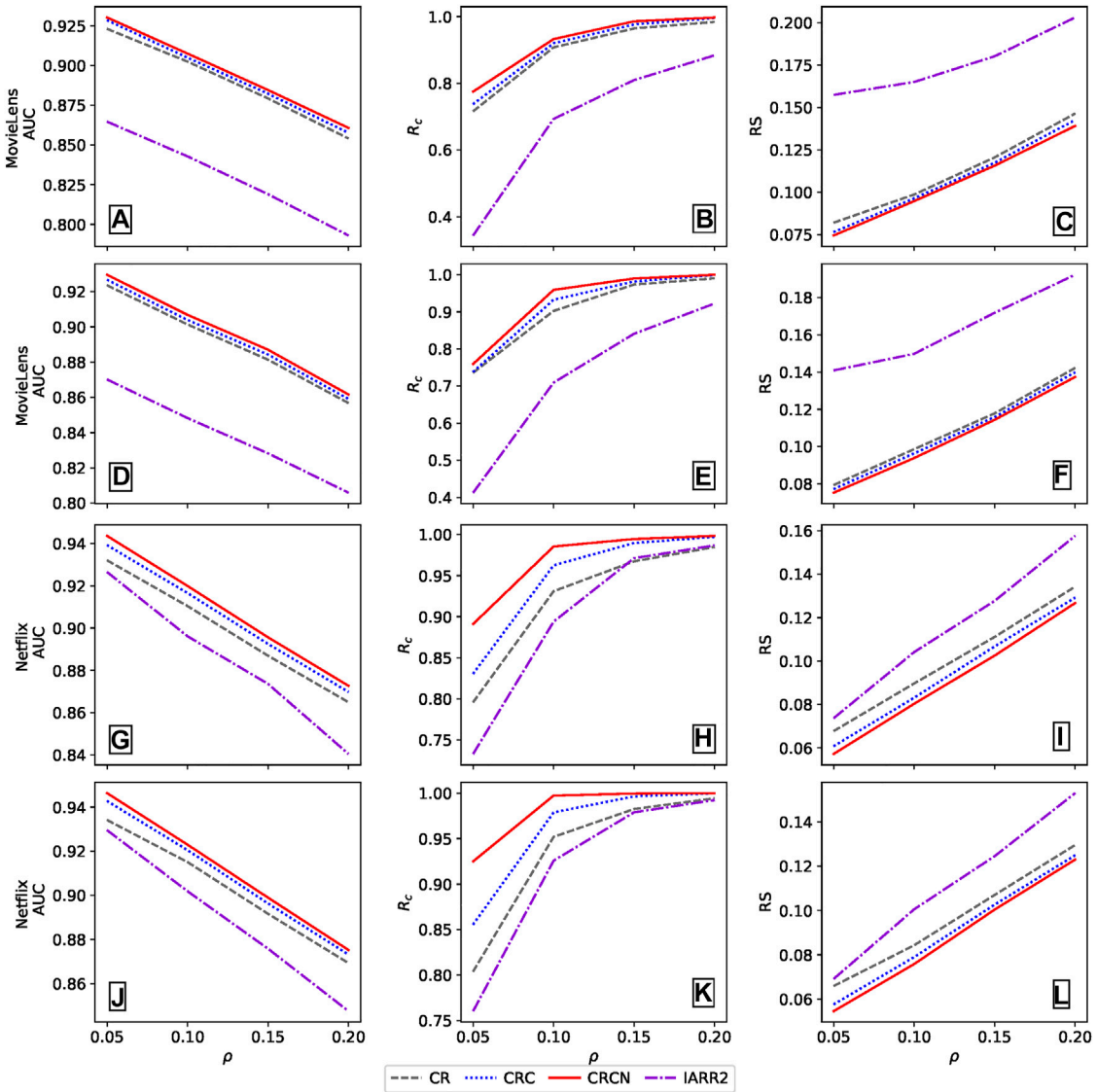


FIGURE 7 | The AUC, R_c and RS values of different methods with different ω and ρ in the random spammers for **(A-F)** MovieLens and **(G-L)** Netflix data sets, respectively. Each row represents a different parameter ω: a-c ($\omega = 0.75$); d-f ($\omega = 0.1$); g-i ($\omega = 0.02$); j-l ($\omega = 0.03$). The results are averaged over 10 independent realizations.

To create noisy information for the artificial datasets, we randomly switch p fractions of the links with the distorted ratings The larger the value of p is, the less true information there is in the dataset, while $p = 1$ means there is no true information. In the following analysis, we set $p \in [0, 0.6]$. We report the effectiveness of the two proposed algorithms and the CR method as the ratio of spammers increases. **Figure 2** shows the dependence of AUC and τ on different values of p for random ratings and malicious ratings. For both spammer cases, one can easily observe that the AUC value and τ of the CRC method are only slightly higher than those of the classical CR algorithm. However, the CRCN method is significantly better than the CR method, especially when the ratio of spammers is high. Thus, we conclude that both of our proposed algorithms, CRC and CRCN, have more advantages than the CR method.

We also investigated the effect of β on AUC and τ in the CRCN method, and the results are shown in **Appendix A**. It is obvious that the parameter β improves the effectiveness of the algorithm since CRCN degenerates to the CRC method when $\beta = 1$. Moreover, the difference in the AUC value between $\beta = 2$ and $\beta = 3$ is negligible, but τ is optimal when $\beta = 2$, which implies that the overall performance of the CRCN algorithm is better when $\beta = 2$. In the following analysis, we adopt $\beta = 2$. Please see **Appendix A** for the dependence of AUC and τ on the parameter β.

4.2 Results From Real Rating Data

We naturally consider the performance of the proposed algorithms on real datasets. The reputation values of all evaluators in each dataset are calculated and sorted in

ascending order to detect the proportion of the top L evaluators who are spammers. At the same time, the CR and IARR2 methods are compared with the proposed CRC and CRCN methods. We first turn 5% of evaluators in each real dataset to two types of spammers to test the effectiveness of the evaluation method, i.e., ρ = 5%. **Figure 3** presents the recall score of different methods calculated according to the length L of the spammer list. Regardless of the type of spamming, the CRCN method has a significant advantage over the CR method, and the CRC method is essentially an improvement over the CR method. In particular, this enhancement of CRCN is more remarkable for both datasets in the case of malicious spammers, which indicates that it is more challenging to detect random spammers.

The AUC and RS values are reported in **Table 2**. One can find that for both types of spammers, the AUC values of the CRC and CRCN methods are higher than those of the CR method for every dataset, which implies that the two methods have more advantages in accuracy. However, it is worth mentioning that the improvement of the CRC method over the CR method is very considerable. Moreover, RS verifies the effectiveness of CRC and CRCN from another aspect. The smaller the RS is, the higher the ranking of spammers. As shown in **Table 2**, we easily note that the RS of CRCN is the smallest for both types of spammers in both datasets. From the above analysis, we can find that the qualitative results of these methods for both types of spammers are very similar, so we will only consider the case of random spammers in the following analysis.

Next, we will analyse whether the performance of the proposed methods is still outstanding while varying ω and ρ; here, ω and ρ are the ratio of objects rated by spammers and the ratio of spammers, respectively. In the following, we set $\rho \in [0.05, 0.2]$ to test the robustness changing with the number of spammers in the ground truth and set the length of the detected spam list to twice the number of spammers, namely, L = 2d. The parameter ω is selected according to the sparsity of the datasets, and ω of the Netflix dataset is smaller than that of the MovieLens dataset since the Netflix dataset is sparser. **Figure 4** shows how the AUC, R_c, and RS values change under different methods when there are different proportions of spammers in the two datasets. Please see **Appendix B** for more details of different ω. It is worth noting that, as a whole, the performance of the CRCN method is better than other methods, especially when ρ is small. Moreover, the R_c values of all methods are positively correlated to the number of spammers. In contrast, the RS value of the CRCN method is always lower than that of the other methods, regardless of the number of spammers. Therefore, we conclude that the performance of the proposed CRCN method is stable and accurate.

One of the motivations of the IARR2 method is that evaluators should have a high reputation only when they have a high degree. From **Figure 4**, we can find that the performance of IARR2 method is not satisfactory compared with other methods in the two data sets, especially in the MovieLens data set. This fully demonstrates that the simple structural information, such as degree, cannot make a reliable correction to the original CR algorithm. It is indispensable to discuss the relationship between the clustering coefficients of evaluators and their degree in the bipartite network, as shown in **Figure 5**. As the evaluators' degrees are continuous and with different scales, we take the log of the degrees for both datasets and divide them into ten bins. It is not surprising that, similar to the conclusions of many studies [43], there is no relatively positive correlation between the evaluators' degree and the clustering coefficient in the two real datasets. To be sure, the introduction of the clustering coefficient in the reputation evaluation process considers the network association from systematic aspects, which effectively improves the classical CR algorithm.

5 CONCLUSION

Building a sound reputation evaluation system for online rating systems is a crucial issue that has great commercial value in e-commerce systems and has guiding significance for a wide range of systematic evaluations. In this paper, we propose a robust reputation evaluation algorithm that considers network association and nonlinear recovery from the systematic aspects of rating systems by combining the structural information of the evaluator-object bipartite network and the penalty reward function with the original correlation-based ranking method. More specifically, in the iterations, we introduced the clustering coefficient of evaluators in the bipartite network to refine their reputations and then used the penalty-reward function to strengthen the high-reputation evaluators further and weaken the impact of low-reputation evaluators. Extensive experiments on artificial data and two real-world datasets show that the proposed CRC and CRCN methods have better performance than the originally proposed CR and IARR2 algorithms. These two newly proposed methods outperform the previous ones in evaluating evaluator reputation, and their accuracy and recall scores are remarkably improved and can effectively identify spammers.

The proposed CRCN method has a similar framework as the previous IARR2 algorithm, but the new method focuses more on the core system factors in complex systems, and the CRCN method demonstrates its effectiveness and stability compared to the unsatisfying performance of IARR2. The results show that introducing the clustering coefficient as the most basic network association feature and nonlinear recovery in the iterative process can capture more profound evaluator behaviour characteristics to improve the CR method. This novel method has also been applied in related studies on the nonlinear behaviors of the earth systems [44, 45]. In future work, we can focus on more systematic factors to build a reputation evaluation system, such as the interactions among evaluators. We can also consider the impact of time on building a reputation system because normal evaluators rarely generate a large number of ratings in a short time, whereas spammers may do so. Additionally, we should also pay attention to the emotional language in the text comments of the evaluation

system, which can provide more meaningful information to individuals [46].

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. These data can be found in **Section 3.2**.

AUTHOR CONTRIBUTIONS

ML, CH and ZD contributed to conception and design of the study. ML and YJ performed the analysis and validated the analysis. ML and CH wrote the first draft of the manuscript. ZD designed the research and reviewed the manuscript. All authors have read and approved the content of the manuscript.

FUNDING

This work is supported by the National Natural Science Foundation of China through Grant No.71 731 002.

ACKNOWLEDGMENTS

CH gratefully acknowledges support from the German Federal Ministry of Education and Research under Grant No. 03EK3055B.

REFERENCES

1. Muchnik L, Aral S, TaylorTaylor SJ. Social Influence Bias: A Randomized experiment. *Science* (2013) 341(6146):647–51. doi:10.1126/science.1240466
2. Linyuan L, Medo M, Yeung CH, Zhang Y-C, Zhang Z-K, Zhou T. Recommender Systems. *Phys Rep* (2012) 519(1):1–49.
3. Wang D, Liang Y, Dong X, Feng X, Guan R. A Content-Based Recommender System for Computer Science Publications. *Knowledge-Based Syst* (2018) 157(1–9). doi:10.1016/j.knosys.2018.05.001
4. Ureña R, Kou G, Dong Y, Chiclana F, Herrera-Viedma E. A Review on Trust Propagation and Opinion Dynamics in Social Networks and Group Decision Making Frameworks. *Inf Sci* (2019) 478:461–75. doi:10.1016/j.ins.2018.11.037
5. Zeng A, Vidmer A, Medo M, Zhang Y-C. Information Filtering by Similarity-Preferential Diffusion Processes. *Epl* (2014) 105(5):58002. doi:10.1209/0295-5075/105/58002
6. Zhang F, Zeng A. Improving Information Filtering via Network Manipulation. *Epl* (2012) 100(5):58005. doi:10.1209/0295-5075/100/58005
7. Liu X-L, Liu J-G, Yang K, Guo Q, Han J-T. Identifying Online User Reputation of User-Object Bipartite Networks. *Physica A: Stat Mech its Appl* (2017) 467: 508–16. doi:10.1016/j.physa.2016.10.031
8. Zeng A, Cimini G. Removing Spurious Interactions in Complex Networks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2012) 85(3):036101. doi:10.1103/PhysRevE.85.036101
9. Chung C-Y, Hsu P-Y, Huang S-H. A Novel Approach to Filter Out Malicious Rating Profiles from Recommender Systems. *Decis Support Syst* (2013) 55(1): 314–25. doi:10.1016/j.dss.2013.01.020
10. Yang Z, Zhang Z-K, Zhou T. Anchoring Bias in Online Voting. *Epl* (2013) 100(6):68002. doi:10.1209/0295-5075/100/68002
11. Zhang Y-L, Guo Q, Ni J, Liu J-G. Memory Effect of the Online Rating for Movies. *Physica A: Stat Mech its Appl* (2015) 417:261–6. doi:10.1016/j.physa.2014.09.012
12. Toledo RY, Mota YC, Martínez L. Correcting Noisy Ratings in Collaborative Recommender Systems. *Knowledge-Based Syst* (2015) 76:96–108. doi:10.1016/j.knosys.2014.12.011
13. Zhang Q-M, Zeng A, Shang M-S. Extracting the Information Backbone in Online System. *PLoS One* (2013) 8(5):e62624. doi:10.1371/journal.pone.0062624
14. Allahbakhsh M, Ignjatovic A, Motahari-Nezhad HR, Benatallah B. Robust Evaluation of Products and Reviewers in Social Rating Systems. *World Wide Web* (2015) 18(1):73–109. doi:10.1007/s11280-013-0242-4
15. Dhingra K, Yadav SK. Spam Analysis of Big Reviews Dataset Using Fuzzy Ranking Evaluation Algorithm and Hadoop. *Int J Mach Learn Cyber* (2019) 10(8):2143–62. doi:10.1007/s13042-017-0768-3
16. Qiao W, Yan Z, Wang X. Join or Not: The Impact of Physicians' Group Joining Behavior on Their Online Demand and Reputation in Online Health Communities. *Inf Process Manage* (2021) 58(5):102634. doi:10.1016/j.ipm.2021.102634
17. Gallo SA, SullivanSullivan JH, GlissonGlisson SR. The Influence of Peer Reviewer Expertise on the Evaluation of Research Funding Applications. *PLoS One* (2016) 11(10):e0165147. doi:10.1371/journal.pone.0165147
18. Pier EL, Brauer M, Filut A, Kaatz A, Raclaw J, Nathan MJ, et al. Low Agreement Among Reviewers Evaluating the Same Nih grant Applications. *Proc Natl Acad Sci USA* (2018) 115(12):2952–7. doi:10.1073/pnas.1714379115
19. Alexander N, Spiekermann S. Oblivion of Online Reputation: How Time Cues Improve Online Recruitment. *Int J Electron Business* (2017) 13(2-3):183–204.
20. Fouss F, Achbany Y, Saerens M. A Probabilistic Reputation Model Based on Transaction Ratings. *Inf Sci* (2010) 180(11):2095–123. doi:10.1016/j.ins.2010.01.020
21. Jian Q, Li X, Wang J, Xia C. Impact of Reputation Assortment on Tag-Mediated Altruistic Behaviors in the Spatial Lattice. *Appl Maths Comput* (2021) 396:125928. doi:10.1016/j.amc.2020.125928
22. Xia C, Gracia-Lázaro C, Moreno Y. Effect of Memory, Intolerance, and Second-Order Reputation on Cooperation. *Chaos* (2020) 30(6):063122. doi:10.1063/5.0009758
23. Li X, Hao G, Wang H, Xia C, Perc M. Reputation Preferences Resolve Social Dilemmas in Spatial Multigames. *J Stat Mech* (2021) 2021(1):013403. doi:10.1088/1742-5468/abd4cf
24. Wang S, Zheng Z, Wu Z, Lyu MR, Yang F. Reputation Measurement and Malicious Feedback Rating Prevention in Web Service Recommendation Systems. *IEEE Trans Serv Comput* (2014) 8(5):755–67.
25. Chang MK, Cheung W, Tang M. Building Trust Online: Interactions Among Trust Building Mechanisms. *Inf Manage* (2013) 50(7):439–45. doi:10.1016/j.im.2013.06.003
26. Laureti P, Moret L, Zhang Y-C, Yu Y-K. Information Filtering via Iterative Refinement. *Europhys Lett* (2006) 75(6):1006–12. doi:10.1209/epl/i2006-10204-8
27. Zhou Y-B, Lei T, Zhou T. A Robust Ranking Algorithm to Spamming. *Epl* (2011) 94(4):48002. doi:10.1209/0295-5075/94/48002
28. Liao H, Zeng A, Xiao R, Ren Z-M, Chen D-B, Zhang Y-C. Ranking Reputation and Quality in Online Rating Systems. *PLoS One* (2014) 9(5):e97146. doi:10.1371/journal.pone.0097146
29. Gao J, Dong Y-W, Shang M-S, Cai S-M, Zhou T. Group-based Ranking Method for Online Rating Systems with Spamming Attacks. *Epl* (2015) 110(2): 28003. doi:10.1209/0295-5075/110/28003
30. Gao J, Zhou T. Evaluating User Reputation in Online Rating Systems via an Iterative Group-Based Ranking Method. *Physica A: Stat Mech its Appl* (2017) 473:546–60. doi:10.1016/j.physa.2017.01.055
31. Lu D, Guo Q, Liu X-L, Liu J-G, Zhang Y-C. Identifying Online User Reputation in Terms of User Preference. *Physica A: Stat Mech its Appl* (2018) 494:403–9.
32. Lee D, Lee MJ, Kim BJ. Deviation-based Spam-Filtering Method via Stochastic Approach. *Epl* (2018) 121(6):68004. doi:10.1209/0295-5075/121/68004
33. Sun H-L, Liang K-P, Liao H, Chen D-B. Evaluating User Reputation of Online Rating Systems by Rating Statistical Patterns. *Knowledge-Based Syst* 219: 1068952021.

34. Zhang J, Cohen R. A Framework for Trust Modeling in Multiagent Electronic Marketplaces with Buying Advisors to Consider Varying Seller Behavior and the Limiting of Seller Bids. *ACM Trans Intell Syst Technol* (2013) 4(2):1–22. doi:10.1145/2438653.2438659
35. Liu X-L, Guo Q, Hou L, ChengLiu J-G. Ranking Online Quality and Reputation via the User Activity. *Physica A: Stat Mech its Appl* (2015) 436: 629–36. doi:10.1016/j.physa.2015.05.043
36. Linyuan L, Chen D, Ren X-L, Zhang Q-M, Zhang Y-C, Zhou T. Vital Nodes Identification in Complex Networks. *Phys Rep* (2016) 650:1–63.
37. Latapy M, Magnien C, Del Vecchio N. Basic Notions for the Analysis of Large Two-Mode Networks. *Social Networks* (2008) 30(1):31–48. doi:10.1016/j.socnet.2007.04.006
38. Barabási A-L, Albert R. Emergence of Scaling in Random Networks. *Science* (1999) 286(5439):509–12. doi:10.1126/science.286.5439.509
39. Kendall MG. A New Measure of Rank Correlation. *Biometrika* (1938) 30(1/2): 81–93. doi:10.2307/2332226
40. James AH, McNeil BJ. The Meaning and Use of the Area under a Receiver Operating Characteristic (Roc) Curve. *Radiology* (1982) 143(1):29–36. doi:10.1148/radiology.143.1.7063747
41. Herlocker JL, Konstan JA, Terveen LG, Riedl JT. Evaluating Collaborative Filtering Recommender Systems. *ACM Trans Inf Syst (Tois)* (2004) 22(1):5–53. doi:10.1145/963770.963772
42. Zhou T, Ren J, Medo M, Zhang Y-C. Bipartite Network Projection and Personal Recommendation. *Phys Rev E* (2007) 76(4):046115. doi:10.1103/PhysRevE.76.046115
43. Ravasz E, Barabási A-L. Hierarchical Organization in Complex Networks. *Phys Rev E* (2003) 67(2):026112. doi:10.1103/PhysRevE.67.026112
44. Fan J, Meng J, Ludescher J, Chen X, Yosef A, Kurths J, et al. Statistical Physics Approaches to the Complex Earth System. *Phys Rep* (2021) 1–84. doi:10.1016/j.physrep.2020.09.005
45. Zhang Y, Yosef A, Havlin S. Asymmetry in Earthquake Interevent Time Intervals. *J Geophys Res Solid Earth* (2021) 126(9):e2021JB022454. doi:10.1029/2021jb022454
46. Rocklage MD, DerekRucker D, Nordgren LF. Mass-scale Emotionality Reveals Human Behaviour and Marketplace success. *Nat Hum Behav* (2021)(1–7). doi:10.1038/s41562-021-01098-5

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

APPENDIX A.

The dependence of parameter β in CRCN method. Here, we show the effect of β on AUC and τ in the CRCN method. We set the ratio of spammers to 0.6, and the results are shown in **Figure 6**. As mentioned in the main, the parameter β improves the effectiveness of the algorithm since CRCN degenerates to the CRC method when $\beta = 1$. Moreover, the difference in AUC value between $\beta = 2$ and $\beta = 3$ is negligible, but τ is optimal when $\beta = 2$, which implies that the overall performance of the CRCN algorithm is better when $\beta = 2$. Therefore, in the following analysis, we adopt $\beta = 2$.

APPENDIX B.

We also compared the performance of the proposed method with the classical CR method and the IARR2 method while varying ω and ρ. The results are shown in **Figure 7**. We can find that the performance of the CRCN method is better than other methods.

frontiers | Frontiers in Physics

BRIEF RESEARCH REPORT
published: 11 April 2022
doi: 10.3389/fphy.2022.896886

A Note on Resistance Distances of Graphs

*Wensheng Sun and Yujun Yang**

School of Mathematics and Information Sciences, Yantai University, Yantai, China

Let G be a connected graph with vertex set $V(G)$. The resistance distance between any two vertices $u, v \in V(G)$ is the net effective resistance between them in the electric network constructed from G by replacing each edge with a unit resistor. Let $S \subset V(G)$ be a set of vertices such that all the vertices in S have the same neighborhood in $G - S$, and let $G[S]$ be the subgraph induced by S. In this note, by the {1}-inverse of the Laplacian matrix of G, formula for resistance distances between vertices in S is obtained. It turns out that resistance distances between vertices in S could be given in terms of elements in the inverse matrix of an auxiliary matrix of the Laplacian matrix of $G[S]$, which derives the reduction principle obtained in [J. Phys. A: Math. Theor. 41 (2008) 445203] by algebraic method.

Keywords: resistance distance, Laplacian matrix, {1}-inverse, moore-penrose inverse, reduction principle

1 INTRODUCTION

The novel concept of resistance distance was introduced by Klein and Randić [8] in 1993. For a connected graph G with vertex set $V(G) = \{1, 2, \ldots, n\}$, the *resistance distance* between $u, v \in V(G)$, denoted by $\Omega_G(u, v)$, is defined to be the effective resistance between u and v in the corresponding electric network obtained from G by replacing each edge with a unit resistor. Since resistance distance is an intrinsic graph metric and an important component of circuit theory, with potential applications in chemistry, it has been extensively studied in mathematics, physics, and chemistry. For more information, we refer the readers to recent papers [2, 4, 6, 7, 10, 11, 15] and references therein.

Let G be a connected graph of order n. For any set of vertices $U \subset V(G)$, we use $G[U]$ to denote the subgraph induced by U, and $G - U$ to denote the subgraph obtained from G by removing all the vertices in U as well as all the edges incident to vertices of U. The *adjacency matrix* A_G of G is an $n \times n$ matrix such that the (i, j)-th element of A_G is equal to 1 if vertices i and j are adjacent and 0 otherwise. The *Laplacian matrix* of G is $L_G = D_G - A_G$, where D_G is the diagonal matrix of vertex degrees of G. Clearly, L_G is real symmetric and singular.

Let M be an $n \times m$ real matrix. An $m \times n$ real matrix X is called a {1}-inverse of M and denoted by $M^{(1)}$, if X satisfies the following equation:

$$MXM = M.$$

If M is singular, then it has infinite {1}-inverses. It is well known that resistance distances in a connected graph G can be obtained from any {1}-inverse of L_G (see [1]). So far, there are many well-established results on this inverse. For example, in 2014, Bu *et al* [4] obtained the {1}-inverse of the Laplacian matrix for a class of connected graphs, and investigated resistance distances in subdivision-vertex join and subdivision-edge join of graphs. Then in 2015, an exact expression for the {1}-inverse of the Laplacian matrix of connected graphs was obtained by Sun *et al.* [13]. After that, Liu *et al.* [9] obtained the {1}-inverses for the Laplacian matrix of subdivision-vertex and subdivision-edge coronae networks. Recently, Cao *et al.* [5] also

OPEN ACCESS

Edited by:
Yongxiang Xia,
Hangzhou Dianzi University, China

Reviewed by:
Jia-Bao Liu,
Anhui Jianzhu University, China
Audace A. V. Dossou-Olory,
Université d'Abomey-Calavi, Benin

***Correspondence:**
Yujun Yang
yangyj@yahoo.com

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *15 March 2022*
Accepted: *31 March 2022*
Published: *11 April 2022*

Citation:
Sun W and Yang Y (2022) A Note on Resistance Distances of Graphs. Front. Phys. 10:896886. doi: 10.3389/fphy.2022.896886

characterised the {1}-inverses for the Laplacian of corona and neighborhood corona networks. Sardar *et al.* [12] determined resistance distances of some classes of rooted product graphs via the Laplacian {1}-inverses method.

In this paper, some results on the {1}-inverses for Laplacian matrices of graphs with given special properties are established. As an application, for any given vertex set $S \subset V(G)$ such that all the vertices in S have the same neighborhood N in $G - S$, explicit formula for resistance distances between vertices in S is obtained. It turns out that resistance distances between vertices in S could be given in terms of elements in the inverse matrix of an auxiliary matrix of the Laplacian matrix of $G[S]$, which derives the reduction principle obtained in [J. Phys. A: Math. Theor. 41 (2008) 445203] by algebraic method.

2 PRELIMINARY RESULTS

In this section, we present some preliminary results. We first introduce the concept of group inverse and Moore-Penrose inverse of a matrix.

Definition 2.1. For a square matrix X, the *group inverse* of X, denoted by $X^{\#}$, is the unique matrix H that satisfies matrix equations:

$$XHX = X, \quad HXH = H, \quad XH = HX.$$

Definition 2.2. Let M be an $n \times m$ matrix. An $m \times n$ matrix X is called the *Moore-Penrose inverse* of M, if X satisfies the following conditions:

$$MXM = M, \quad XMX = X, \quad (MX)^H = MX, \quad (XM)^H = XM.$$

where X^H represents the conjugate transpose of the matrix X.

If M is real symmetric, then there exists a unique $M^{\#}$ and $M^{\#}$ is the symmetric {1}-inverse of M. In particular, $M^{\#}$ is equal to the Moore-Penrose inverse of M because M is symmetric [3].

Let $(M)_{ij}$ denote the (i, j)-entry of M. It is well known that resistance distances in a connected graph G can be obtained from any {1}-inverse of L_G according to the following lemma.

Lemma 2.3. *[3] Let G be a connected graph. Then for vertices i and j,*

$$\begin{aligned}\Omega_G(i,j) &= \left(L_G^{(1)}\right)_{ii} + \left(L_G^{(1)}\right)_{jj} - \left(L_G^{(1)}\right)_{ij} - \left(L_G^{(1)}\right)_{ji} \\ &= \left(L_G^{\#}\right)_{ii} + \left(L_G^{\#}\right)_{jj} - 2\left(L_G^{\#}\right)_{ij}.\end{aligned}$$

Let $\mathbf{0}$ and $\mathbf{e}$ be all-zero and all-one column vectors, respectively. Let $J_{n\times m}$ be the $n \times m$ all-one matrix. The following result is due to Sun et al. [13] which characterizes the {1}-inverse of the Laplacian matrix.

Lemma 2.4. *[13] Let $L_G = \begin{bmatrix} L_1 & L_2 \\ L_2^T & L_3 \end{bmatrix}$ be the Laplacian matrix of a connected graph. If L_1 is nonsingular, then $X = \begin{bmatrix} L_1^{-1} + L_1^{-1}L_2S^{\#}L_2^TL_1^{-1} & -L_1^{-1}L_2S^{\#} \\ -S^{\#}L_2^TL_1^{-1} & S^{\#} \end{bmatrix}$ is a symmetric {1}-inverse of L_G, where $S = L_3 - L_2^TL_1^{-1}L_2$.*

In particular, if each column vector of L_2^T is $-\mathbf{e}$ or $\mathbf{0}$, then X can be further simplified. For convenience, in the rest of this section (see Lemmas 2.5, 2.6, 2.7), we always assume that $L_G = \begin{bmatrix} L_1 & L_2 \\ L_2^T & L_3 \end{bmatrix}$, with the property that L_1 is nonsingular, and each column vector of L_2^T is $-\mathbf{e}$ or $\mathbf{0}$.

Lemma 2.5. *[4] Let L_G be defined as above. Then $X = \begin{bmatrix} L_1^{-1} & 0 \\ 0 & S^{\#} \end{bmatrix}$ is a symmetric {1}-inverse of L_G, where $S = L_3 - L_2^TL_1^{-1}L_2$.*

According to Lemma 2.4, we could get the following results.

Lemma 2.6. *Let L_G be defined as above. If each row of L_1 sums to k, then each column vector of $-L_1^{-1}L_2S^{\#}$ is proportional to the all-one vector, where $S = L_3 - L_2^TL_1^{-1}L_2$.*

Proof. Suppose that the number of columns of L_2 is n_2 and let $L_2 = [\,\mathbf{r}_1 \;\; \mathbf{r}_2 \;\; \ldots \;\; \mathbf{r}_{n_2}\,]$ with $\mathbf{r}_i$ being its i-th column vector, $i = 1, 2, \ldots, n_2$. First we show that for any $\mathbf{r}_i$, all the elements of $L_1^{-1}\mathbf{r}_i$ are the same. If $\mathbf{r}_i = \mathbf{0}$, then the assertion holds since $L_1\mathbf{r}_i = \mathbf{0}$. Otherwise, $\mathbf{r}_i = -\mathbf{e}$. Since L_1 is nonsingular with each row sum being k, it follows that each row of L_1^{-1} sums to $\frac{1}{k}$. Thus $L_1^{-1}\mathbf{r}_i = L_1^{-1}(-\mathbf{e}) = -\frac{1}{k}(\mathbf{e})$, which also implies that all the elements of $L_1^{-1}\mathbf{r}_i$ are the same. Hence, each column of $-L_1^{-1}L_2$ is proportional to the all-one vector, that is, all the row vectors of $-L_1^{-1}L_2$ are the same. It thus follows that each column of $-L_1^{-1}L_2S^{\#}$ is proportional to the all-one vector, i.e. all the elements in any given column of $-L_1^{-1}L_2S^{\#}$ are the same. □

According to Lemma 2.6, we have the following result.

Lemma 2.7. *Let L_G be defined as above. If each row of L_1 sums to k, then there exists a real number ξ such that $L_1^{-1}L_2S^{\#}L_2^TL_1^{-1} = \xi J_{n_1\times n_1}$, where $S = L_3 - L_2^TL_1^{-1}L_2$.*

Proof. Let $M_1 = L_1^{-1}L_2S^{\#}$. According to the argument in the proof of Lemma 2.6, all the row vectors in M_1 are the same. On the other hand, since L_1 is real symmetric, it follows that

$$L_2^TL_1^{-1} = L_2^T\left(L_1^{-1}\right)^T = \left(L_1^{-1}L_2\right)^T.$$

Let $M_2 = L_2^TL_1^{-1}$. Then all the column vectors in M_2 are the same since all the row vectors in $-L_1^{-1}L_2$ are the same. Thus, we conclude that there exists a real number ξ such that

$$L_1^{-1}L_2S^{\#}L_2^TL_1^{-1} = M_1M_2 = \xi J_{n_1\times n_1}.$$

This completes the proof. □

3 MAIN RESULTS

In this section, we consider resistance distances between vertices in a specific subset S of $V(G)$. Let $S \subset V(G)$ such that all the vertices in S have the same neighborhood N in $G - S$. In the

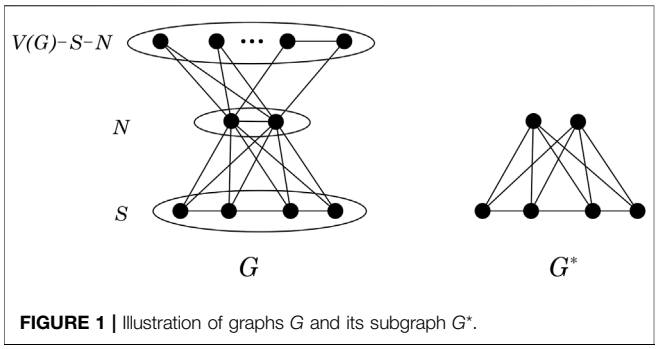


FIGURE 1 | Illustration of graphs G and its subgraph G^*.

following, we give explicit formula for resistance distances between vertices in S. For simplicity, we use L_S to denote the Laplacian matrix of the subgraph induced by S. Suppose that the cardinalities of S and N are n_1 and k, respectively. Then the Laplacian matrix of G can be written as follows.

$$L_G = \begin{bmatrix} L_S + kI_{n_1} & L_2 \\ L_2^T & L_3 \end{bmatrix},$$

where I_{n_1} is the identity matrix of order n_1.

Now we are ready to give formula for resistance distances between vertices in S.

Theorem 3.1. *Let $S \subset V(G)$ such that all the vertices in S have the same neighborhood N in $G - S$. Then for $i, j \in S$, we have*

$$\Omega_G(i,j) = \left(L_1^{-1}\right)_{ii} + \left(L_1^{-1}\right)_{jj} - 2\left(L_1^{-1}\right)_{ij}.$$

where $L_1 = L_S + kI_{n_1}$.

Proof. Let $L_1 = L_S + kI_{n_1}$. Clearly, L_1 is nonsingular, and each row of L_1 sums to k and each column vector of L_2 is $-\mathbf{e}$ or $\mathbf{0}$. Then by Lemma 2.7, there exists a real number ξ such that $L_1^{-1}L_2S^{\#}L_2^TL_1^{-1} = \xi J_{n_1\times n_1}$, where $S = L_3 - L_2^TL_1^{-1}L_2$. Then by Lemma 2.5, we can obtain the {1}-inverse of L_G as follows.

$$X = \begin{bmatrix} L_1^{-1} + \xi J_{n_1\times n_1} & -L_1^{-1}L_2S^{\#} \\ -S^{\#}L_2^TL_1^{-1} & S^{\#} \end{bmatrix}.$$

Thus, for vertices $i, j \in S$, by Lemma 2.3, we have

$$\begin{aligned}\Omega_G(i,j) &= (X)_{ii} + (X)_{jj} - (X)_{ij} - (X)_{ji} \\ &= \left(L_1^{-1} + \xi J_{n_1\times n_1}\right)_{ii} + \left(L_1^{-1} + \xi J_{n_1\times n_1}\right)_{jj} - \left(L_1^{-1} + \xi J_{n_1\times n_1}\right)_{ij} - \left(L_1^{-1} + \xi J_{n_1\times n_1}\right)_{ji} \\ &= \left(L_1^{-1}\right)_{ii} + \xi + \left(L_1^{-1}\right)_{jj} + \xi - \left(L_1^{-1}\right)_{ij} - \xi - \left(L_1^{-1}\right)_{ji} - \xi \\ &= \left(L_1^{-1}\right)_{ii} + \left(L_1^{-1}\right)_{jj} - 2\left(L_1^{-1}\right)_{ij}.\end{aligned}$$

The proof is complete. □

Theorem 3.1indicates that, if $S \subset V(G)$ satisfies that all the vertices in S have the same neighborhood N in $G - S$, then resistance distances between vertices in S depends only on the subgraph $G[S]$ and the cardinality of N. In other words, if we use $G^\star$ to denote the subgraph obtained from $G[S \cup N]$ by deleting all the edges between vertices in N (see **Figure 1**), then resistance distances between vertices in S depends only on $G^\star$. In fact, for $i, j \in S$, $\Omega_G(i,j) = \Omega_{G^*}(i,j)$, as shown in the following.

Theorem 3.2. *Let $S \subset V(G)$ such that all the vertices in S have the same neighborhood N in $G - S$. Let $G^\star$ the graph obtained from $G[S \cup N]$ by deleting all the edges between vertices in N. Then for $i, j \in S$, we have*

$$\Omega_{G^*}(i,j) = \left(L_1^{-1}\right)_{ii} + \left(L_1^{-1}\right)_{jj} - 2\left(L_1^{-1}\right)_{ij}.$$

where $L_1 = L_S + kI_{n_1}$.

Proof. According to the definition of $G^\star$, it is readily to see that the Laplacian matrix of $G^\star$ is

$$L_{G^*} = \begin{bmatrix} L_1 & -J_{n_1\times k} \\ -J_{k\times n_1} & kI_k \end{bmatrix}.$$

Since each column vector of $-J_{k\times n_1}$ is $-\mathbf{e}$, by Lemma 2.5, we can obtain the symmetric {1}-inverse of L_{G^*} as follows:

$$Y = \begin{bmatrix} L_1^{-1} & 0 \\ 0 & S^{\#} \end{bmatrix},$$

where $S = kI_k - J_{k\times n_1}L_1^{-1}J_{n_1\times k}$. Hence by Lemma 2.3, we have

$$\Omega_{G^*}(i,j) = \left(L_1^{-1}\right)_{ii} + \left(L_1^{-1}\right)_{jj} - 2\left(L_1^{-1}\right)_{ij},$$

as required. □

Remark 1. Combining Theorems 3.1 and 3.2, we could conclude that if $S \subset V(G)$ satisfies that all the vertices in S have the same neighborhood N in $G - S$, then resistance distances between vertices in S can be computed as in the subgraph obtained from $G[S \cup N]$ by deleting all the edges between vertices in N. It should be mentioned that this fact, known as the reduction principle, was established in [14]. We confirm this result by algebraic method, rather than electric network method as used in [14]. Furthermore, we also give an exact formula for resistance distances between vertices in S. By Theorem 3.1, we are able to establish some interesting properties.

Theorem 3.3. *Let $S \subset V(G)$ such that all the vertices in S have the same neighborhood N in $G - S$. Then for $i, j \in S$ and $u \in G - S$, we have*

$$\Omega_G(i,u) - \Omega_G(j,u) = \left(L_1^{-1}\right)_{ii} - \left(L_1^{-1}\right)_{jj}.$$

where $L_1 = L_S + kI_{n_1}$.

Proof. As given in the proof of Theorem 3.1, we know that the {1}-inverse of L_G is

$$X = \begin{bmatrix} L_1^{-1} + \xi J_{n_1\times n_1} & -L_1^{-1}L_2S^{\#} \\ -S^{\#}L_2^TL_1^{-1} & S^{\#} \end{bmatrix}.$$

where ξ be a real number and $S = L_3 - L_2^TL_1^{-1}L_2$. By Lemma 2.3, we have

$$\begin{aligned}\Omega_G(i,u) - \Omega_G(j,u) = (X)_{ii} + (X)_{uu} - (X)_{iu} - (X)_{ui} \\ - \left[(X)_{jj} + (X)_{uu} - (X)_{ju} - (X)_{uj}\right].\end{aligned}$$

Note that L_1 is nonsingular and every row sums to k and each column vector of L_2 is $-\mathbf{e}$ or a zero vector. So by Lemma 2.6, we know that each column of $-L_1^{-1}L_2S^{\#}$ is proportional to all-one vector, which implies that $(X)_{iu} = (X)_{ju}$. Since X is real symmetric, we also have $(X)_{ui} = (X)_{uj}$. It follows that

$$\begin{aligned}\Omega_G(i,u) - \Omega_G(j,u) &= (X)_{ii} + (X)_{uu} - (X)_{jj} - (X)_{uu}\\ &= (L_1^{-1})_{ii} + \xi + (L_1^{-1})_{uu} + \xi - (L_1^{-1})_{jj} - \xi - (L_1^{-1})_{uu} - \xi\\ &= (L_1^{-1})_{ii} - (L_1^{-1})_{jj}.\end{aligned}$$

This completes the proof. □

It is interesting to note from Theorem 3.2 that the difference between $\Omega_G(i, u)$ and $\Omega_G(j, u)$ depends only on the subgraph $G[S]$ and the cardinality of N, no matter the chosen of u. Then we have the following result.

Corollary 3.4. *Let $S \subset V(G)$ such that all the vertices in S have the same neighborhood N in $G - S$. Then for $i, j \in S$ and $u, v \in G - S$, we have*

$$\Omega_G(i,u) - \Omega_G(j,u) = \Omega_G(i,v) - \Omega_G(j,v).$$

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

YY contributed to conception and design of the study. WS performed the theoretical analysis and wrote the first draft of the manuscript. YY revised the manuscript. Both authors read, and approved the submitted version.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous referees for their helpful comments and suggestions. The support of the National Natural Science Foundation of China (through Grant No. 12171414) and Natural Science Foundation of Shandong Province (through no. ZR2019YQ02) is greatly acknowledged.

REFERENCES

1. Bapat RB. Resistance Distance in Graphs. *Math Stud* (1999) 68(1-4):87–98.
2. Bapat RB, Gupta S. Resistance Distance in Wheels and Fans. *Indian J Pure Appl Math* (2010) 41(1):1–13. doi:10.1007/s13226-010-0004-2
3. Bu C, Sun L, Zhou J, Wei Y. A Note on Block Representations of the Group Inverse of Laplacian Matrices. *Electron J Linear Algebra* (2012) 23:866–76. doi:10.13001/1081-3810.1562
4. Bu C, Yan B, Zhou X, Zhou J. Resistance Distance in Subdivision-Vertex Join and Subdivision-Edge Join of Graphs. *Linear Algebra its Appl* (2014) 458: 454–62. doi:10.1016/j.laa.2014.06.018
5. Cao J, Liu J, Wang S. Resistance Distances in corona and Neighborhood corona Networks Based on Laplacian Generalized Inverse Approach. *J Algebra Appl* (2019) 18(3):1950053. doi:10.1142/s0219498819500531
6. Chen H, Zhang F. Resistance Distance and the Normalized Laplacian Spectrum. *Discrete Appl Maths* (2007) 155:654–61. doi:10.1016/j.dam.2006.09.008
7. Fowler PW. Resistance Distances in Fullerene Graphs. *Croat Chem Acta* (2002) 75(2):401–8.
8. Klein DJ, Randić M. Resistance Distance. *J Math Chem* (1993) 12:81–95. doi:10.1007/bf01164627
9. Liu JB, Pan XF, Hu FT. The {1}-inverse of the Laplacian of Subdivision-Vertex and Subdivision-Edge Coronae with Applications. *Linear and Multilinear Algebra* (2017) 65(1):178–91. doi:10.1080/03081087.2016.1179249
10. Liu JB, Wang WR, Zhang YM, Pan XF. On Degree Resistance Distance of Cacti. *Discrete Appl Maths* (2016) 203:217–25. doi:10.1016/j.dam.2015.09.006
11. Palacios JL. Resistance Distance in Graphs and Random Walks. *Int J Quant Chem* (2001) 81(1):29–33. doi:10.1002/1097-461x(2001)81:1<29::aid-qua6>3.0.co;2-y
12. Sardar MS, Alaeiyan M, Farahani MR, Cancan M, Ediz S. Resistance Distance in Some Classes of Rooted Product Graphs Obtained by Laplacian Generalized Inverse Method. *J Inf Optimization Sci* (2021) 42(7):1447–67. doi:10.1080/02522667.2021.1899210
13. Sun L, Wang W, Zhou J, Bu C. Some Results on Resistance Distances and Resistance Matrices. *Linear and Multilinear Algebra* (2015) 63(3):523–33. doi:10.1080/03081087.2013.877011
14. Yang Y, Zhang H. Some Rules on Resistance Distance with Applications. *J Phys A: Math Theor* (2008) 41(44):445203. doi:10.1088/1751-8113/41/44/445203
15. Zhang H, Yang Y. Resistance Distance and Kirchhoff index in Circulant Graphs. *Int J Quan Chem.* (2007) 107(2):330–9. doi:10.1002/qua.21068

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

frontiers | Frontiers in Physics

ORIGINAL RESEARCH
published: 23 June 2022
doi: 10.3389/fphy.2022.872798

Results on Resistance Distance and Kirchhoff Index of Graphs With Generalized Pockets

Qun Liu[1]* *and Jiaqi Li*[2]

[1]School of Mathematics and Statistics, Hexi University, Zhangye, China, [2]Institute of Intelligent Information, Hexi University, Zhangye, China

F, H_v are considered simple connected graphs on n and $m + 1$ vertices, and v is a specified vertex of H_v and $u_1, u_2, \ldots u_k \in F$. The graph $G = G[F, u_1, \ldots, u_k, H_v]$ is called a graph with k pockets, obtained by taking one copy of F and k copies of H_v and then attaching the ith copy of H_v to the vertex u_i, $i = 1, \ldots, k$, at the vertex v of H_v. In this article, the closed-form formulas of the resistance distance and the Kirchhoff index of $G = G[F, u_1, \ldots, u_k, H_v]$ are obtained in terms of the resistance distance and Kirchhoff index F and H_v.

Keywords: resistance distance, Kirchhoff index, generalized inverse, Schur complement, generalized pockets

1 INTRODUCTION

All graphs considered in this article are simple and undirected. The resistance distance between vertices u and v of G was defined by Klein and Randić [1] to be the effective resistance between nodes u and v as computed with Ohm's law when all the edges of G are considered to be unit resistors. The Kirchhoff index $Kf(G)$ was defined in Ref. 1 as $Kf(G) = \sum_{u<v} r_{uv}$, where $r_{uv}(G)$ denotes the resistance distance between u and v in G. Resistance distance are, in fact, intrinsic to the graph, with some nice purely mathematical interpretations and other interpretations. The Kirchhoff index was introduced in chemistry as a better alternative to other parameters used for discriminating different molecules with similar shapes and structures [1]. The resistance distance and Kirchhoff index have attracted extensive attention due to their wide applications in physics, chemistry, and other fields. Until now, many results on the resistance distance and Kirchhoff index are obtained. The references in [2–5] can be referred to know more. However, the resistance distance and Kirchhoff index of the graph is, in general, a difficult thing from the computational point of view. The bigger the graph, the more difficult it is to compute the resistance distance and Kirchhoff index; so a common strategy is to consider a complex graph as a composite graph and to find relations between the resistance distance and Kirchhoff index of the original graphs. Let $G = (V(G), E(G))$ be a graph with the vertex set $V(G)$ and edge set $E(G)$. Let d_i be the degree of vertex i in G and $D_G = diag\,(d_1, d_2, \cdots d_{|V(G)|})$ the diagonal matrix with all vertex degrees of G as its diagonal entries. For graph G, let A_G and B_G denote the adjacency matrix and vertex-edge incidence matrix of G, respectively. The matrix $L_G = D_G - A_G$ is called the Laplacian matrix of G, where D_G is the diagonal matrix of vertex degrees of G. We use $\mu_1(G) \geq u_2(G) \geq \cdots \geq \mu_n(G) = 0$ to denote the spectrum of L_G. For other undefined notations and terminology from graph theory, the readers may refer to Ref. 6 and the references therein [7–23]. The computation of the resistance distance between two nodes in a resistor network is a classical problem in electric theory and graph theory. For certain families of graphs, it is possible to identify a graph by looking at the resistance distance and Kirchhoff index. More generally, this is not possible. In some cases, the resistance distance and Kirchhoff index of a relatively larger graph can be described in terms of the resistance distance and Kirchhoff index of some smaller (and simpler) graphs using some simple graph operations. There are results that discuss the resistance distance and Kirchhoff

OPEN ACCESS

Edited by:
Yongxiang Xia,
Hangzhou Dianzi University, China

Reviewed by:
Jia-Bao Liu,
Anhui Jianzhu University, China
Yujun Yang,
Yantai University, China

***Correspondence:**
Qun Liu
liuqun@fudan.edu.cn

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *10 February 2022*
Accepted: *14 March 2022*
Published: *23 June 2022*

Citation:
Liu Q and Li J (2022) Results on Resistance Distance and Kirchhoff Index of Graphs With Generalized Pockets. Front. Phys. 10:872798. doi: 10.3389/fphy.2022.872798

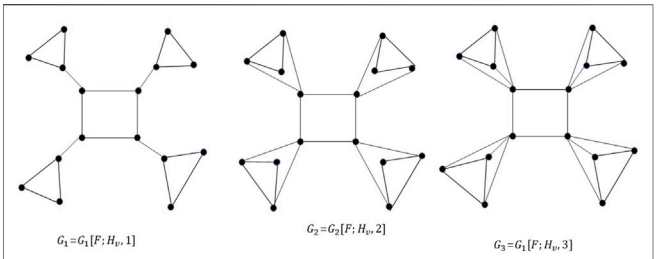


FIGURE 1 | [F; H_v, l] for different l.

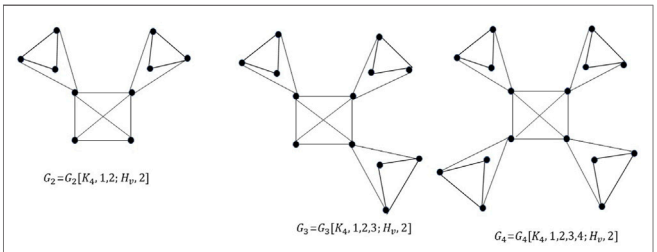


FIGURE 2 | Graphs having different numbers of pockets.

index of graphs obtained using some operations on graphs, such as join, graph products, corona, and many variants of corona, such as edge corona and neighborhood corona. For such operations, it is possible to describe the resistance distance and Kirchhoff index of the resulting graph using the resistance distance and Kirchhoff index of the corresponding constituting graph; Refs. 14 and 15 can be referred for reference. This article considers the resistance distance and Kirchhoff index of the graph operations as follows, obtained from Ref. 11.

Definition 1. [11]: Let F, H_v be connected graphs, v be a specified vertex of H_v and $u_1, u_2, \ldots, u_k \in F$. Let $G = G[F, u_1, u_2, \ldots, u_k, H_v]$ be the graph obtained by taking one copy of F and k copies of H_v and then attaching the ith copy of H_v to the vertex u_i, $i = 1, 2, \ldots, k$, at the vertex v of H_v(identify u_i with the vertex v of the ith copy). Then, the copies of the graph H_v that are attached to the vertices u_i, $i = 1, 2, \ldots, k$ are referred to as pockets, and G is described as a graph with k pockets.

Barik [11] has described the Laplacian spectrum of $G = G[F, u_1, u_2, \ldots, u_k, H_v]$ using the Laplacian spectrum of F and H_v in a particular case when $deg(v) = m$. Recently, Barik and Sahoo [12] have described the Laplacian spectrum of more such graphs' relaxing condition $deg(v) = m$. Let $deg(v) = l$, $1 \le l \le m$. In this case, we denoted $G = G[F, u_1, u_2, \ldots, u_k, H_v]$ more precisely by $G = G[F, u_1, u_2, \ldots, u_k; H_v, l]$. When $k = n$, we denoted simply by $G = G[F; H_v, l]$. If $deg(v) = l$, $1 \le l \le m$, let $N(v) = \{v_1, v_2, \ldots, v_l\} \subset V(H_v)$ be the neighborhood set of v in H_v. Let H_1 be the subgraph of H_v induced by the vertices in $N(v)$ and H_2 be the subgraph of H_v induced by the vertices which are in $V(H_v)\backslash(N(v) \cup \{v\})$. When $H_v = H_1 \vee (H_2 + \{v\})$, we described the resistance distance and Kirchhoff index of $G = G[F, u_1, u_2, \ldots, u_k, H_v]$. The graphs $F = C_4$ and $H - v = C_3$ are considered. Taking $l = 1$, 2 and 3, we obtained graphs $G_1 = G_1[F; H_v, 1]$, $G_2 = G_2[F; H_v, 2]$, and $G_3 = G_3[F; H_v, 3]$, respectively. **Figure 1** is referred. In this case, we described the resistance distance and Kirchhoff index of $G = G[F; H_v, l]$ in terms of the resistance distance and Kirchhoff index of F and H_v. The results are contained in **Section 3** of this article. Furthermore, when $F = F_1 \vee F_2$, F_1 is the subgraph of F induced by the vertices $u_1, u_2, \ldots, u_k$ and F_2 is the subgraph of F induced by the vertices $u_{k+1}, u_{k+2}, \ldots, u_n$. The considered three graphs G_2, G_3, and G_4 are shown in **Figure 2**, obtained from the two graphs $F = K_4$ and H_v such that $H_v \backslash \{v\} = K_3$. It is observed that $F = K_1 \vee K_3$, G_2, G_3, and G_4 are graphs with 2, 3, and 4 pockets, respectively. **Figure 2** can be referred. In this case, we described the resistance distance and Kirchhoff index of $G[F, u_1, u_2, \ldots, u_k; H_v, l]$ in terms of the resistance distance and Kirchhoff index of F and H_v. These results are contained in **Section 4**.

2 PRELIMINARIES

The {1}-inverse of M is a matrix X such that $MXM = M$. If M is singular, then it has infinite {1}-inverse [16]. For a square matrix M, the group inverse of M, denoted by $M^{\#}$, is the unique matrix X such that $MXM = M$, $XMX = X$, and $MX = XM$. It is known that $M^{\#}$ exists if and only if $rank(M) = rank(M^2)$ [16, 17]. If M is really symmetric, then $M^{\#}$ exists, and $M^{\#}$ is a symmetric {1}-inverse of M. Actually, $M^{\#}$ is equal to the Moore–Penrose inverse of M since M is symmetric [17].

It is known that the resistance distance in a connected graph G can be obtained from any {1}- inverse of G [13]. We used $M^{(1)}$ to denote any {1}-inverse of a matrix M, and $(M)_{uv}$ denotes the (u, v)-entry of M.

Lemma 2.1. [17]: Let G be a connected graph, then

$$\begin{aligned} r_{uv}(G) &= \left(L_G^{(1)}\right)_{uu} + \left(L_G^{(1)}\right)_{vv} - \left(L_G^{(1)}\right)_{uv} - \left(L_G^{(1)}\right)_{vu} \\ &= \left(L_G^{\#}\right)_{uu} + \left(L_G^{\#}\right)_{vv} - 2\left(L_G^{\#}\right)_{uv}. \end{aligned}$$

Let 1_n denote the column vector of dimension n with all the entries equal to one. We often use 1 to denote all-ones column vector if the dimension can be read from the context.

Lemma 2.2. [14]: For any graph, we have $L_G^{\#}1 = 0$.

Lemma 2.3. [18]: Let

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

be a nonsingular matrix. If A and D are nonsingular, then

$$\begin{aligned} M^{-1} &= \begin{pmatrix} A^{-1} + A^{-1}BS^{-1}CA^{-1} & -A^{-1}BS^{-1} \\ -S^{-1}CA^{-1} & S^{-1} \end{pmatrix} \\ &= \begin{pmatrix} (A - BD^{-1}C)^{-1} & -A^{-1}BS^{-1} \\ -S^{-1}CA^{-1} & S^{-1} \end{pmatrix}, \end{aligned}$$

where $S = D - CA^{-1}B$.

Lemma 2.4. [15]: Let L be the Laplacian matrix of a graph of order n. For any $a > 0$, we have

$$\left(L + aI_n - \frac{a}{n}J_{n\times n}\right)^{\#} = (L + aI)^{-1} - \frac{1}{an}J_{n\times n}.$$

Lemma 2.5. [5]: Let G be a connected graph on n vertices, then

$$Kf(G) = ntr\left(L_G^{(1)}\right) - 1^T L_G^{(1)} 1 = ntr\left(L_G^{\#}\right).$$

Lemma 2.6. [19]: Let

$$L = \begin{pmatrix} A & B \\ B^T & D \end{pmatrix}$$

be the Laplacian matrix of a connected graph. If D is nonsingular, then

$$X = \begin{pmatrix} H^{\#} & -H^{\#}BD^{-1} \\ -D^{-1}B^T H^{\#} & D^{-1} + D^{-1}B^T H^{\#} BD^{-1} \end{pmatrix}$$

is a symmetric {1}-inverse of L, where $H = A - BD^{-1}B^T$.

3 THE RESISTANCE DISTANCE AND KIRCHHOFF INDEX OF $G[F; H_v, L]$

Let F be a connected graph with the vertex set $\{u_1, u_2, \ldots, u_n\}$. Let H_v be a connected graph on $m + 1$ vertices with a specified vertex v and $V(H_v) = \{v_1, v_2, \ldots, v_m, v\}$. Let $G = G[F; H_v, l]$. It is noted that G has $n(m + 1)$ vertices. Let $deg(v) = l$, $1 \le l \le m$. With loss of generality, it is assumed that $N(v) = \{v_1, v_2, \ldots, v_l\}$. Let H_1 be the subgraph of H_v induced by the vertices in $\{v_1, v_2, \ldots, v_l\}$ and H_2 be the subgraph of H_v induced by the vertices $\{v_{l+1}, v_{l+2}, \ldots, v_m\}$. It is supposed that $H_v = H_1 \vee (H_2 + \{v\})$. In this section, we focused on determining the resistance distance and Kirchhoff index of $G[F; H_v, l]$ in terms of the resistance distance and Kirchhoff index of F, H_1 and H_2.

Theorem 3.1. Let G $[F; H_v, l]$ be the graph, as described previously. It is supposed that $H_v = H_1 \vee (H_2 + \{v\})$. Let the Laplacian spectrum of H_1 and H_2 be $\sigma(H_1) = (0 = \mu_1, \mu_2, \ldots \mu_l)$ and $\sigma(H_2) = (0 = \nu_1, \nu_2, \ldots \nu_{m-l})$. Then, G $[F; H_v, l]$ has the resistance distance and Kirchhoff index as follows:

(i) For any $i, j \in V(F)$, we obtained

$$r_{ij}(G[F; H_v, l]) = \left(L^{\#}(F)\right)_{ii} + \left(L^{\#}(F)\right)_{jj} - 2\left(L^{\#}(F)\right)_{ij} = r_{ij}(F).$$

(ii) For any $i \in V(F)$ and $j \in V(H_1)$, we obtained

$$r_{ij}(G[F; H_v, l]) = \left(L^{\#}(F)\right)_{ii} + \left[\left(L(H_1) + (m - l + 1)I_l - \frac{m-l}{l}J_{l\times l}\right)^{-1} \otimes I_n + (1_l \otimes I_n)L^{\#}(F)(1_l^T \otimes I_n)\right]_{jj} - 2L^{\#}(F)(1_l^T \otimes I_n)_{ij}.$$

(iii) For any $i \in V(F)$ and $j \in V(H_2)$, we obtained

$$r_{ij}(G[F; H_v, l]) = \left(L^{\#}(F)\right)_{ii} + \left[\left(L(H_2) + lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1} \otimes I_n\right]_{jj} - 2\left(L^{\#}(F)\right)_{ij}.$$

(iv) For any $i \in V(H_1)$ and $j \in V(H_2)$, we obtained

$$r_{ij}(G[F; H_v, l]) = \left[\left(L(H_1) + (m - l + 1)I_l - \frac{m-l}{l}J_{l\times l}\right)^{-1} \otimes I_n\right]_{ii} + \left[\left(L(H_2) + lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1} \otimes I_n\right]_{jj} - 2\left[(L(H_1) + (m - l + 1)I_l - \frac{m-l}{l}J_{l\times l})^{-1} \otimes I_n\right]_{ij}.$$

(v) For any $i \in V(H_2)$ and $j \in V(H_1)$, we obtained

$$r_{ij}(G[F; H_v, l]) = \left[\left(L(H_2) + lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1} \otimes I_n\right]_{ii} + \left[\left(L(H_1) + (m - l + 1)I_l - \frac{m-l}{l}J_{l\times l}\right)^{-1} \otimes I_n\right]_{jj} - 2\left[\left(L(H_2) + lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1} \otimes I_n\right]_{ij}.$$

(vi) Let

$$Kf(G[F; H_v, l]) = n(m+1)\left(\frac{m+1}{n}Kf(F) + \left(n\sum_{i=2}^{l}\frac{1}{\mu_i(H_1) + (m - l + 1)} + n\right) + \left(n\sum_{i=2}^{m-l}\frac{1}{\nu_i(H_2) + l} + \frac{nl}{m-l+1}\right)\right) - \left((m-l)^2\frac{m-l+1}{l} + l^2\right).$$

Proof: Let v_j^i denote the jth vertex of H in the ith copy of H_v in G, for $i = 1, 2, \ldots, n$; $j = 1, 2, \ldots, m$, and let $V_j(H_v) = \{v_j^1, v_j^2, \ldots, v_j^n\}$. Then, $V(F) \cup (\cup_{j=1}^{m} V_j(H_v))$ is a partition of $V(G)$. Using this partition, the Laplacian matrix of $G = G[F; H_v, l]$ can be expressed as

$$L(G[F; H_v, l]) = \begin{pmatrix} L(F) + lI_n & -1_l^T \otimes I_n & 0 \\ -1_l \otimes I_n & (L(H_1) + (m - l + 1)I_l) \otimes I_n & -J_{l\times(m-l)} \otimes I_n \\ 0 & -J_{(m-l)\times l} \otimes I_n & (L(H_2) + lI_{m-l}) \otimes I_n \end{pmatrix}.$$

We began with the computation of {1}-inverse of the Laplacian matrix $L(G)$ of $G = G[F; H_v, l]$. Let $A = L(F) + lI_n$, $B = (-1_l^T \otimes I_n \;\; 0)$, $B^T = \begin{pmatrix} -1_l \otimes I_n \\ 0 \end{pmatrix}$ and

$$D = \begin{pmatrix} (L(H_1) + (m - l + 1)I_l) \otimes I_n & -J_{l\times(m-l)} \otimes I_n \\ -J_{(m-l)\times l} \otimes I_n & (L(H_2) + lI_{m-l}) \otimes I_n \end{pmatrix}.$$

First, we computed the D^{-1}. By Lemma 2.3, we obtained

$$\begin{aligned} A_1 - B_1D_1^{-1}C_1 &= (L(H_1) + (m - l + 1)I_l) \otimes I_n - (-J_{l\times(m-l)} \otimes I_n)\\ &\quad ((L(H_2) + lI_{m-l})^{-1} \otimes I_n)(-J_{(m-l)\times l} \otimes I_n)\\ &= (L(H_1) + (m - l + 1)I_l) \otimes I_n - 1_l[1_{m-l}^T(L(H_2)\\ &\quad + lI_{m-l})^{-1}1_{m-l}]1_l^T \otimes I_n\\ &= (L(H_1) + (m - l + 1)I_l) \otimes I_n - \frac{m-l}{l}J_{l\times l} \otimes I_n\\ &= \left[L(H_1) + (m - l + 1)I_l - \frac{m-l}{l}J_{l\times l}\right] \otimes I_n, \end{aligned}$$

so

$$(A_1 - B_1D_1^{-1}C_1)^{-1} = \left[(L(H_1) + (m - l + 1)I_l - \frac{m-l}{l}J_{l\times l}\right]^{-1} \otimes I_n.$$

By Lemma 2.3, we obtained

$$\begin{aligned}S^{-1} &= \left(D_1 - C_1A_1^{-1}B_1\right)^{-1}\\ &= \left[\left(L(H_2)+lI_{m-l}\right)\otimes I_n - \left(-J_{(m-l)\times l}\otimes I_n\right)\left(\left(L(H_1)+(m-l+1)I_l\right)^{-1}\otimes I_n\right)\right.\\ &\quad \left.\left(-J_{l\times(m-l)}\otimes I_n\right)\right]^{-1}\\ &= \left[\left(L(H_2)+lI_{m-l}\right)\otimes I_n - \left(J_{(m-l)\times l}\left(L(H_1)+(m-l+1)I_l\right)^{-1}J_{l\times(m-l)}\right)\otimes I_n\right]^{-1}\\ &= \left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1}\otimes I_n.\end{aligned}$$

By Lemma 2.3, we obtained

$$\begin{aligned}-A_1^{-1}B_1S^{-1} &= -\left[\left(L(H_1)+(m-l+1)I_l\right)^{-1}\otimes I_n\right]\left(-J_{l\times(m-l)}\otimes I_n\right)\\ &\quad \left[L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right]^{-1}\otimes I_n\\ &= \left(\frac{1}{m-l+1}1_l\otimes I_n\right)\left(\frac{m-l+1}{l}1_{m-l}^T\otimes I_n\right)\\ &= \frac{1}{l}J_{l\times(m-l)}\otimes I_n.\end{aligned}$$

Similarly, $-S^{-1}C_1A_1^{-1} = \left(-A_1^{-1}B_1S^{-1}\right)^T = \frac{1}{l}J_{(m-l)\times l}\otimes I_n$. So

$$D^{-1} = \begin{pmatrix} P_1 & \frac{1}{l}J_{l\times(m-l)}\otimes I_n\\ \frac{1}{l}J_{(m-l)\times l}\otimes I_n & Q_1\end{pmatrix},$$

where $P_1 = \left[\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right]^{-1}\otimes I_n\right.$, $Q_1 = \left[\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)\right]^{-1}\otimes I_n$. Now, we computed the {1}-inverse of $G[F; H_v, l]$. By Lemma 2.6, we obtained

$$\begin{aligned}H &= A - BD^{-1}B^T\\ &= L(F)+lI_n - \left(-1_l^T\otimes I_n\ \ 0\right)\begin{pmatrix} P_1 & \frac{1}{l}J_{l\times(m-l)}\otimes I_n\\ \frac{1}{l}J_{(m-l)\times l}\otimes I_n & Q_1\end{pmatrix}\begin{pmatrix}-1_l\otimes I_n\\ 0\end{pmatrix}\\ &= L(F)+lI_n - \left(1_l^T\otimes I_n\right)\left[\left(L(H_1)+(m-l+1)I_l\right.\right.\\ &\quad \left.\left.-\frac{m-l}{l}J_{l\times l}\right]^{-1}\otimes I_n\right]\left(1_l\otimes I_n\right)\\ &= L(F)+lI_n-lI_n = L(F),\end{aligned}$$

so $H^{\#} = L^{\#}(F)$. According to Lemma 2.6, we calculated $-H^{\#}BD^{-1}$ and $-D^{-1}B^TH^{\#}$.

$$\begin{aligned}-H^{\#}BD^{-1} &= -L^{\#}(F)\left(-1_l^T\otimes I_n\ \ 0\right)\begin{pmatrix} P_1 & \frac{1}{l}J_{l\times(m-l)}\otimes I_n\\ \frac{1}{l}J_{(m-l)\times l}\otimes I_n & Q_1\end{pmatrix}\\ &= \left(L^{\#}(F)\left(1_l^T\otimes I_n\right), L^{\#}(F)\left(1_{m-l}^T\otimes I_n\right)\right)\end{aligned}$$

and

$$-D^{-1}B^TH^{\#} = \begin{pmatrix}\left(1_l\otimes I_n\right)L^{\#}(F)\\ \left(1_{m-l}\otimes I_n\right)L^{\#}(F)\end{pmatrix}.$$

We are ready to compute the $D^{-1}B^TH^{\#}BD^{-1}$.

$$\begin{aligned}D^{-1}B^TH^{\#}BD^{-1} &= \begin{pmatrix}\left(1_l\otimes I_n\right)L^{\#}(F)\\ \left(1_{m-l}\otimes I_n\right)L^{\#}(F)\end{pmatrix}\left(\left(1_l^T\otimes I_n\right), \left(1_{m-l}^T\otimes I_n\right)\right)\\ &= \begin{pmatrix}\left(1_l\otimes I_n\right)L^{\#}(F)\left(1_l^T\otimes I_n\right) & \left(1_l\otimes I_n\right)L^{\#}(F)\left(1_{m-l}^T\otimes I_n\right)\\ \left(1_{m-l}\otimes I_n\right)L^{\#}(F)\left(1_l^T\otimes I_n\right) & \left(1_{m-l}\otimes I_n\right)L^{\#}(F)\left(1_{m-l}^T\otimes I_n\right)\end{pmatrix}.\end{aligned}$$

Let $P = \left[\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right]\otimes I_n\right.$, $Q = \left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1}\otimes I_n$, and $M = \frac{1}{l}J_{l\times(m-l)}\otimes I_n + \left(1_l\otimes I_n\right)L^{\#}(F)\left(1_{m-l}^T\otimes I_n\right)$; then, based on Lemma 2.6, the following matrix

$$N = \begin{pmatrix} L^{\#}(F) & L^{\#}(F)\left(1_l^T\otimes I_n\right) & L^{\#}(F)\left(1_{m-l}^T\otimes I_n\right)\\ \left(1_l\otimes I_n\right)L^{\#}(F) & P_1 & M\\ \left(1_{m-l}\otimes I_n\right)L^{\#}(F) & M^T & Q_1\end{pmatrix}, \tag{1}$$

is a symmetric {1}-inverse of $G[F; H_v, l]$, where $P_1 = P^{-1} + \left(1_l\otimes I_n\right)L^{\#}(F)\left(1_l^T\otimes I_n\right)$ and $Q_1 = Q^{-1} + \left(1_{m-l}\otimes I_n\right)L^{\#}(F)\left(1_{m-l}^T\otimes I_n\right)$. For any $i, j \in V(F)$, by Lemma 2.1 and **Eq. 1**, we obtained

$$r_{ij}\left(G[F; H_v, l]\right) = \left(L^{\#}(F)\right)_{ii} + \left(L^{\#}(F)\right)_{jj} - 2\left(L^{\#}(F)\right)_{ij} = r_{ij}(F),$$

as stated in (i).

For any $i \in V(F)$ and $j \in V(H_1)$, by Lemma 2.1 and **Eq. 1**, we obtained

$$\begin{aligned}r_{ij}\left(G[F; H_v, l]\right) = \left(L^{\#}(F)\right)_{ii} &+ \left[\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)^{-1}\otimes I_n+\right.\\ &\left.\left(1_l\otimes I_n\right)L^{\#}(F)\left(1_l^T\otimes I_n\right)\right]_{jj} - 2L^{\#}(F)\left(1_l^T\otimes I_n\right)_{ij},\end{aligned}$$

as stated in (ii).

For any $i \in V(F)$ and $j \in V(H_2)$, by Lemma 2.1 and **Eq. 1**, we obtained

$$\begin{aligned}r_{ij}\left(G[F; H_v, l]\right) = \left(L^{\#}(F)\right)_{ii} &+ \left[\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1}\otimes I_n\right]_{jj}\\ &-2\left(L^{\#}(F)\right)_{ij},\end{aligned}$$

as stated in (iii).

For any $i \in V(H_1)$ and $j \in V(H_2)$, by Lemma 2.1 and **Eq. 1**, we obtained

$$\begin{aligned}r_{ij}\left(G[F; H_v, l]\right) = &\left[\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)^{-1}\otimes I_n\right]_{ii}+\\ &\left[\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1}\otimes I_n\right]_{jj}\\ &-2\left[\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)^{-1}\otimes I_n\right]_{ij},\end{aligned}$$

as stated in (iv).

For any $i \in V(H_2)$ and $j \in V(H_1)$, by Lemma 2.1 and **Eq. 1**, we obtained

$$\begin{aligned}r_{ij}\left(G[F; H_v, l]\right) = &\left[\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1}\otimes I_n\right]_{ii}\\ &+\left[\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)^{-1}\otimes I_n\right]_{jj}-2\\ &\left[\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1}\otimes I_n\right]_{ij},\end{aligned}$$

as stated in (v). Now, we computed the Kirchhoff index of $G[F; H_v, l]$. By Lemma 2.5, we obtained

$Kf(G[F; H_v, l])$

$$\begin{aligned}&= n(m+1)tr(N) - 1^TN1\\ &= n(m+1)\left[\left(tr\left(L^{\#}(F)\right)+tr\left(\left(L(H_1)+(m-l+1)I_l+\frac{m-l}{l}J_{l\times l}\right)^{-1}\otimes I_n\right)\right)+\right.\\ &\quad +tr\left(\left(L(H_2)+lI_{m-l}+\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1}\otimes I_n\right)\Big)+\\ &\quad \left.tr\left(\left(1_l\otimes I_n\right)L^{\#}(F)\left(1_l^T\otimes I_n\right)\right)+tr\left(\left(1_{m-l}\otimes I_n\right)L^{\#}(F)\left(1_{m-l}^T\otimes I_n\right)\right)\right]-1^TN1.\end{aligned}$$

It is noted that the eigenvalues of $(L(H_2)+lI_{m-l})$ are $0+l$, $\nu_2(H_2)+l, \ldots, \nu_{m-l}(H_2)+l$ and the eigenvalues of $J_{(m-l)\times(m-l)}$ are $(m-l)$, $0^{(m-l-1)}$. Then,

$$tr\left(\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)}\right)^{-1}\otimes I_n\right)$$
$$=n\sum_{i=2}^{m-l}\frac{1}{\nu_i(H_2)+l}+\frac{n(m-l+1)}{l}. \quad (2)$$

Similarly,

$$tr\left(\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)^{-1}\otimes I_n\right)$$
$$=n\sum_{i=2}^{l}\frac{1}{\mu_i(H_1)+(m-l+1)}+n.$$

It is easily obtained

$$tr\left((1_l\otimes I_n)L^{\#}(F)\left(1_l^T\otimes I_n\right)\right)+tr\left((1_{m-l}\otimes I_n)L^{\#}(F)\left(1_{m-l}^T\otimes I_n\right)\right)$$
$$=tr\left(J_{l\times l}\otimes L^{\#}(F)\right)+tr\left(J_{(m-l)\times(m-l)}\otimes L^{\#}(F)\right)$$
$$=ltr\left(L^{\#}(F)\right)+(m-l)tr\left(L^{\#}(F)\right)=mtr\left(L^{\#}(F)\right). \quad (3)$$

Let $P=(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l})\otimes I_n$, then

$$1^TP^{-1}1=\begin{pmatrix}1_l^T & 1_l^T & \cdots & 1_l^T\end{pmatrix}\begin{pmatrix}P^{-1} & 0 & 0 & \ldots & 0\\ 0 & P^{-1} & 0 & \ldots & 0\\ 0 & 0 & \ldots & \ldots & 0\\ 0 & 0 & 0 & \ldots & P^{-1}\end{pmatrix}\begin{pmatrix}1_l\\ 1_l\\ \cdots\\ 1_l\end{pmatrix}, \quad (4)$$
$$=l1_l^T\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)^{-1}1_l=l^2.$$

Let $Q=(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)})\otimes I_n$, then

$$1^TQ^{-1}1=\begin{pmatrix}1_{m-l}^T & 1_{m-l}^T & \cdots & 1_{m-l}^T\end{pmatrix}\begin{pmatrix}Q^{-1} & 0 & 0 & \ldots & 0\\ 0 & Q^{-1} & 0 & \ldots & 0\\ 0 & 0 & \ldots & \ldots & 0\\ 0 & 0 & 0 & \ldots & Q^{-1}\end{pmatrix}\begin{pmatrix}1_{m-l}\\ 1_{m-l}\\ \cdots\\ 1_{m-l}\end{pmatrix}, \quad (5)$$
$$=(m-l)1_{m-l}^T\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1}1_{m-l}$$
$$=(m-l)^2\frac{m-l+1}{l}.$$

$$1_{ln}^T(1_l\otimes I_n)L^{\#}(F)\left(1_l^T\otimes I_n\right)1_{ln}=\begin{pmatrix}1_n^T & 1_n^T & \cdots & 1_n^T\end{pmatrix}\begin{pmatrix}I_n\\ I_n\\ \cdots\\ I_n\end{pmatrix}, \quad (6)$$
$$L^{\#}(F)\begin{pmatrix}I_n & I_n & \cdots & I_n\end{pmatrix}\begin{pmatrix}1_n\\ 1_n\\ \cdots\\ 1_n\end{pmatrix}$$
$$=n^21_n^TL^{\#}(F)1_n=0.$$

Similarly, $1^T((1_l\otimes I_n)L^{\#}(F)(1_{m-l}^T\otimes I_n)1=0, 1^T((1_{m-l}\otimes I_n)L^{\#}(F)(1_l^T\otimes I_n)1=0$ and $1^T((1_{m-l}\otimes I_n)L^{\#}(F)(1_l^T\otimes I_n)1=0$

Plugging **Eqs 2–6** and the aforementioned equations into $Kf(G[F; H_v, l])$, we obtained the required result in (vi).

4 RESISTANCE DISTANCE AND KIRCHHOFF INDEX OF $G[F, U_1, U_2, \ldots, U_K; H_V, L]$

In this section, we considered the case when $F=F_1\vee F_2$, where F_1 is the subgraph of F induced by the vertices $u_1, u_2, \ldots, u_k$ and F_2 is the subgraph of F induced by the vertices $u_{k+1}, u_{k+2}, \ldots, u_n$. In this case, we indicated the explicit formulae of the resistance distance and Kirchhoff index of $G=G[F, u_1, u_2, \ldots, u_k; H_v, l]$ in terms of the resistance distance and Kirchhoff index of G and H_v.

Theorem 4.1. Let $G=G[F, u_1, u_2, \ldots, u_k; H_v, l]$ be the graph, as described previously. Let $\sigma(F_1)=(0=\alpha_1, \alpha_2, \ldots \alpha_k)$, $\sigma(F_2)=(0=\beta_1, \beta_2, \ldots \beta_{n-k})$, $\sigma(H_1)=(0=\mu_1, \mu_2, \ldots \mu_l)$, and $\sigma(H_2)=(0=\nu_1, \nu_2, \ldots \nu_{m-l})$. Then, G has the resistance distance and Kirchhoff index as follows:

(i) For any $i, j\in V(F_1)$, we obtained

$$r_{ij}(G)=\left((L(F_1)+(n-k)I_k)^{-1}-\frac{n-k}{k}\right)_{ii}+\left((L(F_1)+(n-k)I_k)^{-1}-\frac{n-k}{k}\right)_{jj}$$
$$-2\left((L(F_1)+(n-k)I_k)^{-1}-\frac{n-k}{k}\right)_{ij}.$$

(ii) For any $i, j\in V(F_2)$, we obtained

$$r_{ij}(G)=(L(F_2)+kI_{n-k})_{ii}^{-1}+(L(F_2)+kI_{n-k})_{jj}^{-1}$$
$$-2(L(F_2)+kI_{n-k})_{ij}^{-1}.$$

(iii) For any $i, j\in V(H_1)$, we obtained

$$r_{ij}(G)=\left(\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)\otimes I_k\right)_{ii}$$
$$+\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)\otimes I_k)_{jj}$$
$$-2\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)\otimes I_k)_{ij}.$$

(iv) For any $i, j\in V(H_2)$, we obtained

$$r_{ij}(G)=\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)\otimes I_k)_{ii}+$$
$$\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)\otimes I_k)_{jj}$$
$$-2\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)\otimes I_k)_{ij}.$$

(v) For any $i\in V(F)$ and $j\in V(H_1)$, we obtained

$$r_{ij}(G) = \left(L^{\#}(F)\right)_{ii} + \left[\left(L(H_1) + (m-l+1)I_l - \frac{m-l}{l}J_{l\times l}\right)\right]^{-1} \otimes I_n - 2\left(L^{\#}(F)\right)_{ij}.$$

(vi) For any $i \in V(F)$ and $j \in V(H_2)$, we obtained

$$r_{ij}(G) = \left(L^{\#}(F)\right)_{ii} + \left[\left(L(H_2) + lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)\right]^{-1} \otimes I_n - 2\left(L^{\#}(F)\right)_{ij}.$$

(vii) For any $i \in V(H_1)$ and $j \in V(H_2)$, we obtained

$$r_{ij}(G) = \left[\left(L(H_1) + (m-l+1)I_l - \frac{m-l}{l}J_{l\times l}\right)^{-1} \otimes I_n\right]_{ii} + \left[\left(L(H_2) + lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1} \otimes I_n\right]_{jj} - 2\left[\left(L(H_1) + (m-l+1)I_l - \frac{m-l}{l}J_{l\times l}\right)^{-1} \otimes I_n\right]_{ij}.$$

(viii) For any $i \in V(H_2)$ and $j \in V(H_1)$, we obtained

$$r_{ij}(G) = \left[\left(L(H_2) + lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1} \otimes I_n\right]_{ii} + \left[(L(H_1) + (m-l+1)I_l - \frac{m-l}{l}j_{l\times l}\right)^{-1} \otimes I_n\Big]_{jj} - 2\left[\left(L(H_2) + lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1} \otimes I_n\right]_{ij}.$$

(ix) Let

$$Kf(G) = (n+mk)\left[2\sum_{i=1}^{k}\left(\frac{1}{\alpha_i + (n-k)} - \frac{1}{(n-k)}\right) + \sum_{i=1}^{n-k}\frac{1}{\beta_i + k} + \left(k\sum_{i=2}^{l}\frac{1}{\mu_i + (m-l+1)} + k\right) + \left(k\sum_{i=2}^{m-l}\frac{1}{\nu_i + l} + \frac{l(2m-2l+1)}{m-l+1}\right) + k + \frac{k(m-l)}{l}\right] - \left(l^2 + \frac{(m-l)(m-l+1)}{l} + 2k(m-l)\right).$$

Proof: Let v_j^i denote the jth vertex of H in the ith copy of H_v in G, for $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, m$, and let $V_j(H_v) = \{v_j^1, v_j^2, \ldots, v_j^k\}$. Then, $V(F_1) \cup V(F_2) \cup (\cup_{j=1}^{m} V_j(H_v))$ is a partition of the vertex set of $G = G[F, u_1, u_2, \ldots, u_k; H_v, l]$. Using this partition, the Laplacian matrix of G can be expressed as

$$L(G) = \begin{pmatrix} L_1 & -J_{k\times(n-k)} & -1_l^T \otimes I_k & 0 \\ -J_{(n-k)\times k} & L_2 & 0 & 0 \\ -1_l \otimes I_k & 0 & L_3 & -J_{l\times(m-l)} \otimes I_k \\ 0 & 0 & -J_{(m-l)\times l} \otimes I_k & L_4 \end{pmatrix},$$

where $L_1 = L(F_1) + (n-k+l)I_k$, $L_2 = L(F_2) + kI_{n-k}$, $L_3 = (L(H_1) + (m-l+1)I_l) \otimes I_k$, and $L_4 = (L(H_2) + lI_{m-l}) \otimes I_k$. Let $A = L_1$, $B = (-J_{k\times(n-k)} \;\; -1_l^T \otimes I_k \;\; 0)$, $B^T = \begin{pmatrix} -J_{(n-k)\times k} \\ -1_l \otimes I_k \\ 0 \end{pmatrix}$, and

$$D = \begin{pmatrix} L_2 & 0 & 0 \\ 0 & L_3 & -J_{l\times(m-l)} \otimes I_k \\ 0 & -J_{(m-l)\times l} \otimes I_k & L_4 \end{pmatrix}.$$

First, we computed

$$D_1^{-1} = \begin{pmatrix} L_3 & -J_{l\times(m-l)} \otimes I_k \\ -J_{(m-l)\times l} \otimes I_k & L_4 \end{pmatrix}^{-1}.$$

By Lemma 2.3, we obtained

$$\begin{aligned} A_1 - B_1D_1^{-1}C_1 &= (L(H_1) + (m-l+1)I_l) \otimes I_k - (-J_{l\times(m-l)} \otimes I_k)\left((L(H_2) + lI_{m-l})^{-1} \otimes I_k\right)(-J_{(m-l)\times l} \otimes I_k) \\ &= (L(H_1) + (m-l+1)I_l) \otimes I_k - 1_l\left(1_{m-l}^T(L(H_2) + lI_{m-l})^{-1}1_{m-l}\right)1_l^T \otimes I_k \\ &= (L(H_1) + (m-l+1)I_l) \otimes I_k - \frac{m-l}{l}J_{l\times l} \otimes I_k \\ &= \left[L(H_1) + (m-l+1)I_l - \frac{m-l}{l}J_{l\times l}\right] \otimes I_k, \end{aligned}$$

so $(A_1 - B_1D_1^{-1}C_1)^{-1} = [(L(H_1) + (m-l+1)I_l - \frac{m-l}{l}J_{l\times l}]^{-1} \otimes I_k$. By Lemma 2.3, we obtained

$$\begin{aligned} S^{-1} &= \left(D_1 - C_1A_1^{-1}B_1\right)^{-1} \\ &= \left[(L(H_2) + lI_{m-l}) \otimes I_k - (-J_{(m-l)\times l} \otimes I_k)\left((L(H_1) + (m-l+1)I_l)^{-1} \otimes I_k\right)(-J_{l\times(m-l)} \otimes I_k\right]^{-1} \\ &= \left[(L(H_2) + lI_{m-l}) \otimes I_k - \left(J_{(m-l)\times l}(L(H_1) + (m-l+1)I_l)^{-1}J_{l\times(m-l)}\right) \otimes I_k\right]^{-1} \\ &= \left[L(H_2) + lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right]^{-1} \otimes I_k. \end{aligned}$$

By Lemma 2.3, we obtained

$$\begin{aligned} -A_1^{-1}B_1S^{-1} &= -\left[(L(H_1) + (m-l+1)I_l)^{-1} \otimes I_k\right](-J_{l\times(m-l)} \otimes I_k)\left[L(H_2) + lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right]^{-1} \otimes I_k \\ &= \frac{1}{m-l+1}1_l \times \frac{m-l+1}{l}1_{m-l}^T \otimes I_k \\ &= \frac{1}{l}J_{l\times(m-l)} \otimes I_k. \end{aligned}$$

Similarly, $-S^{-1}C_1A_1^{-1} = (-A_1^{-1}B_1S^{-1})^T = \frac{1}{l}J_{(m-l)\times l} \otimes I_k$. So

$$D_1^{-1} = \begin{pmatrix} P_1 & \frac{1}{l}J_{l\times(m-l)} \otimes I_k \\ \frac{1}{l}J_{(m-l)\times l} \otimes I_k & Q_1 \end{pmatrix},$$

where $P_1 = [(L(H_1) + (m-l+1)I_l - \frac{m-l}{l}J_{l\times l}]^{-1} \otimes I_n$, $Q_1 = [(L(H_2) + lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)})]^{-1} \otimes I_n$. Now, we computed the $\{1\}$-inverse of $G[F, u_1, u_2, \ldots, u_k; H_v, l]$. Let $P = [(L(H_1) + (m-l+1)I_l - \frac{m-l}{l}J_{l\times l}] \otimes I_k$ and $Q = [(L(H_2) + lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)})] \otimes I_k$. By Lemma 2.6, we obtained

$$\begin{aligned} H &= A - BD^{-1}B^T \\ &= L(F_1) + (n-k+l)I_k - \begin{pmatrix} -J_{k\times(n-k)} & -1_l^T \otimes I_k & 0 \end{pmatrix} \begin{pmatrix} (L(F_2) + kI_{n-k})^{-1} & 0 & 0 \\ 0 & P^{-1} & \frac{1}{l}J_{l\times(m-l)} \otimes I_k \\ 0 & \frac{1}{l}J_{(m-l)\times l} \otimes I_k & Q^{-1} \end{pmatrix} \begin{pmatrix} -J_{(n-k)\times k} \\ -1_l \otimes I_k \\ 0 \end{pmatrix} \\ &= L(F_1) + (n-k+l)I_k - \frac{n-k}{k}J_{k\times k} - lI_k \\ &= L(F_1) + (n-k)I_k - \frac{n-k}{k}J_{k\times k}, \end{aligned}$$

so $H^{\#} = (L(F_1) + (n-k)I_k - \frac{n-k}{k}J_{k\times k})^{\#}$. By Lemma 2.4, we obtained $H^{\#} = (L(F_1) + (n-k)I_k)^{-1} - \frac{1}{k(n-k)}J_{k\times k}$.

According to Lemma 2.6, we calculated $-H^{\#}BD^{-1}$ and $-D^{-1}B^{T}H^{\#}$.

$$-H^{\#}BD^{-1} = -H^{\#}\begin{pmatrix} -J_{k\times(n-k)} & -1_l^T\otimes I_k & 0\end{pmatrix}\begin{pmatrix} (L(F_2)+kI_{n-k})^{-1} & 0 & 0\\ 0 & P^{-1} & \frac{1}{l}J_{l\times(m-l)}\otimes I_k\\ 0 & \frac{1}{l}J_{(m-l)\times l}\otimes I_k & Q^{-1}\end{pmatrix} = \begin{pmatrix}\frac{1}{k}H^{\#}J_{k\times(n-k)} & H^{\#}(1_l^T\otimes I_k) & H^{\#}(1_{m-l}^T\otimes I_k)\end{pmatrix}$$

and

$$-D^{-1}B^{T}H^{\#} = \begin{pmatrix}\frac{1}{k}J_{(n-k)\times k}H^{\#}\\ (1_l\otimes I_k)H^{\#}\\ (1_{m-l}\otimes I_k)H^{\#}\end{pmatrix}.$$

We are ready to compute the $D^{-1}B^{T}H^{\#}BD^{-1}$.

$$D^{-1}B^{T}H^{\#}BD^{-1} = \begin{pmatrix}\frac{1}{k}J_{(n-k)\times k}H^{\#}\\ (1_l\otimes I_k)H^{\#}\\ (1_{m-l}\otimes I_k)H^{\#}\end{pmatrix}\begin{pmatrix}\frac{1}{k}J_{k\times(n-k)} & (1_l^T\otimes I_k) & (1_{m-l}^T\otimes I_k)\end{pmatrix} = \begin{pmatrix}\frac{1}{k^2}JH^{\#}J & \frac{1}{k}JH^{\#}(1_l^T\otimes I_k)\\ \frac{1}{k}(1_l\otimes I_k)H^{\#}J_{k\times(n-k)} & (1_l\otimes I_k)H^{\#}(1_l^T\otimes I_k)\\ \frac{1}{k}(1_{m-l}\otimes I_k)H^{\#}J_{k\times(n-k)} & (1_{m-l}\otimes I_k)H^{\#}(1_l^T\otimes I_k)\end{pmatrix}\begin{pmatrix}\frac{1}{k}JH^{\#}(1_{m-l}^T\otimes I_k)\\ (1_l\otimes I_k)H^{\#}(1_{m-l}^T\otimes I_k)\\ (1_{m-l}\otimes I_k)H^{\#}(1_{m-l}^T\otimes I_k)\end{pmatrix}.$$

Let $M = 1_{m-l}^T\otimes I_k$ and $N = 1_l^T\otimes I_k$. Based on Lemma 2.6, the following matrix

$$T = \begin{pmatrix} H^{\#} & \frac{1}{k}H^{\#}J & H^{\#}N & H^{\#}M\\ \frac{1}{k}JH^{\#} & (L(F_2)+kI)^{-1} & 0 & 0\\ N^TH^{\#} & 0 & P^{-1}+N^TH^{\#}N & N^TH^{\#}M+\frac{1}{l}J\otimes I_k\\ M^TH^{\#} & 0 & M^TH^{\#}N+\frac{1}{l}J\otimes I_k & Q^{-1}+M^TH^{\#}M\end{pmatrix}, \quad (7)$$

is a symmetric {1}-inverse of $G = G[F, u_1, u_2, \ldots, u_k; H_v, l]$, where $P = [(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}]\otimes I_k$ and $Q = [(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)})]\otimes I_k$.

For any $i, j\in V(F_1)$, by Lemma 2.1 and **Eq. 7**, we obtained

$$r_{ij}(G) = \left((L(F_1)+(n-k)I_k)^{-1}-\frac{1}{k(n-k)}\right)_{ii}+\left((L(F_1)+(n-k)I_k)^{-1}-\frac{1}{k(n-k)}\right)_{jj} -2\left((L(F_1)+(n-k)I_k)^{-1}-\frac{1}{k(n-k)}\right)_{ij},$$

as stated in (i).

For any $i, j\in V(F_2)$, by Lemma 2.1 and **Eq. 7**, we obtained

$$r_{ij}(G) = (L(F_2)+kI_{n-k})_{ii}^{-1}+(L(F_2)+kI_{n-k})_{jj}^{-1} -2(L(F_2)+kI_{n-k})_{ij}^{-1},$$

as stated in (ii).

For any $i, j\in V(H_1)$, by Lemma 2.1 and **Eq. 7**, we obtained

$$r_{ij}(G) = \left(\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)\otimes I_k\right)_{ii}^{-1} +\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)\otimes I_k)_{jj}^{-1} -2\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)\otimes I_k)_{ij}^{-1},$$

as stated in (iii).

For any $i, j\in V(H_2)$, by Lemma 2.1 and **Eq. 7**, we obtained

$$r_{ij}(G) = \left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)\otimes I_k)_{ii}^{-1} +\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)\otimes I_k)_{jj}^{-1}-2(L(H_2)+lI_{m-l} -\frac{l}{m-l+1}J_{(m-l)\times(m-l)})\otimes I_k)_{ij}^{-1},$$

as stated in (iv).

For any $i\in V(F)$ and $j\in V(H_1)$ by Lemma 2.1 and **Eq. 7**, we obtained

$$r_{ij}(G) = \left(L^{\#}(F)\right)_{ii} +\left[\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)^{-1}\otimes I_n\right]_{jj} -2\left(L^{\#}(F)\right)_{ij},$$

as stated in (v).

For any $i\in V(F)$ and $j\in V(H_2)$, by Lemma 2.1 and **Eq. 7**, we obtained

$$r_{ij}(G) = \left(L^{\#}(F)\right)_{ii}+\left[\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1}\otimes I_n\right]_{jj} -2\left(L^{\#}(F)\right)_{ij},$$

as stated in (vi).

For any $i\in V(H_1)$ and $j\in V(H_2)$, by Lemma 2.1 and **Eq. 7**, we obtained

$$r_{ij}(G) = \left[\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)^{-1}\otimes I_n\right]_{ii} +\left[\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1}\otimes I_n\right]_{jj} -2\left[\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)^{-1}\otimes I_n\right]_{ij},$$

as stated in (vii).

For any $i\in V(H_2)$ and $j\in V(H_1)$, by Lemma 2.1 and **Eq. 7**, we obtained

$$r_{ij}(G) = \left[\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1}\otimes I_n\right]_{ii} +\left[\left(L(H_1)+(m-l+1)I_l-\frac{m-l}{l}J_{l\times l}\right)^{-1}\otimes I_n\right]_{jj} -2\left[\left(L(H_2)+lI_{m-l}-\frac{l}{m-l+1}J_{(m-l)\times(m-l)}\right)^{-1}\otimes I_n\right]_{ij},$$

as stated in (viii).

Now, we computed the Kirchhoff index of $G[F, u_1, u_2, \ldots u_k; H_v, l]$ as $Kf(G[F, u_1, u_2, \ldots, u_k; H_v, l])$

$$
\begin{aligned}
&= (n+mk)tr(T) - 1^T T1\\
&= (n+mk)\Bigg(tr\Bigg((L(F_1)+(n-k)I_k)^{-1} - \frac{1}{k(n-k)}J_{k\times k}\Bigg)\\
&\quad + tr\,(L(F_2)+kI_{n-k})^{-1} + ktr\Bigg(L(H_1)+(m-l+1)I_l - \frac{m-l}{l}J_{l\times l}\Bigg)^{-1}\\
&\quad + ktr\Bigg(L(H_2)+lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)}\Bigg)^{-1}\\
&\quad + \frac{1}{l}tr\left(J_{l\times(m-l)}\otimes I_k\right) + \frac{1}{l}tr\left(J_{(m-l)\times l}\otimes I_k\right)\\
&\quad + tr\left(N^T H^{\#} N\right) + tr\left(M^T H^{\#} M\right)\Big) - 1^T T1.
\end{aligned}
$$

It is noted that the eigenvalues of $(L(F_1)+(n-k)I_k)$ are $\alpha_1+(n-k)$, $\alpha_2+(n-k)$, …, $\alpha_k+(n-k)$. Then,

$$
tr\Bigg((L(F_1)+(n-k)I_k)^{-1} - \frac{1}{k(n-k)}J_{k\times k}\Bigg) = \sum_{i=1}^{k}\frac{1}{\alpha_i+(n-k)} - \frac{k}{k(n-k)}.
$$

Similarly, $tr\,((L(F_2)+kI_{n-k})^{-1}) = \sum_{i=1}^{n-k}\frac{1}{\beta_i+k}$. It is noted that the eigenvalues of $(L(H_1)+(m-l+1)I_l$ are $0+(m-l+1)$, $\mu_2(H_1)+(m-l+1)$, …, $\mu_l(H_1)+(m-l+1)$ and the eigenvalues of $J_{(m-l)\times(m-l)}$ are $(m-l)$, $0^{(m-l-1)}$. Then,

$$
tr\Bigg(L(H_1)+(m-l+1)I_l + \frac{m-l}{l}J_{l\times l})^{-1}\otimes I_k\Bigg)^{-1} = k\sum_{i=2}^{l}\frac{1}{\mu_i+(m-l+1)} + k.
$$

Similarly,

$$
tr\Bigg(\Bigg(L(H_2)+lI_{m-l} - \frac{l}{m-l+1}J_{(m-l)\times(m-l)}\Bigg)\otimes I_k\Bigg)^{-1} = k\sum_{i=2}^{m-l}\frac{1}{\nu_i+l} + \frac{kl(2m-2l+1)}{m-l+1}.
$$

It is easily obtained that $tr(J_{l\times(m-l)}\otimes I_k) = lk$, $tr(J_{(m-l)\times l}\otimes I_k) = (m-l)k$ and $tr(N^T H^{\#} N) + tr(M^T H^{\#} M) = tr(J_{l\times l}\otimes H^{\#}) + tr(J_{(m-l)\times(m-l)}\otimes H^{\#}) = ltr(H^{\#}) + (m-l)tr(H^{\#}) = mtr(H^{\#})$. Since $1_k^T H^{\#} = 1_k^T[(L(F_1)+(n-k)I_k)^{-1} - \frac{1}{k(n-k)}J_{k\times k}] = \frac{1}{n-k}1_k^T - \frac{1}{k(n-k)}1_k^T = 0$, then

$$
1^T N1 = 1^T(L(F_2)+kI_{n-k})^{-1}1 + 1^T P^{-1}1 + 1^T Q^{-1}1
$$

$$
+1^T N^T H^{\#} N1 + 1^T N^T H^{\#} M1 + 1^T M^T H^{\#} N1 + 1^T M^T H^{\#} M1 + \frac{1}{l}1^T\left(J_{l\times(m-l)}\otimes I_k\right)1 + \frac{1}{l}1^T\left(J_{(m-l)\times l}\otimes I_k\right)1.
$$

By the process of Theorem 4.1, we obtained

$$
1^T P^{-1}1 = l^2,\ 1^T Q^{-1}1 = (m-l)\frac{m-l+1}{l}.
$$

$$
1^T\left(N^T H^{\#} N\right)1 = 1_{lk}^T(1_l\otimes I_k)H^{\#}(1_l^T\otimes I_k)1_{lk} = \left(1_k^T\ \ 1_k^T\ \ \cdots\ \ 1_k^T\right)\begin{pmatrix} I_k\\ I_k\\ \cdots\\ I_k\end{pmatrix}H^{\#}
$$

$$
\left(I_k\ \ I_k\ \ \cdots\ \ I_k\right)\begin{pmatrix}1_k\\1_k\\\cdots\\1_k\end{pmatrix} = k^2 1_k^T H^{\#}1_k = 0.
$$

Similarly, $1^T(M^T H^{\#} M)1 = 0$, $1^T N^T H^{\#} M1 = 0$, and $1^T M^T H^{\#} N1 = 0$.

$$
1^T\left(J_{l\times(m-l)}\otimes I_k\right)1 = \left(1_k^T\ \ 1_k^T\ \ \cdots\ \ 1_k^T\right)\begin{pmatrix} I_k & I_k & \cdots I_k\\ I_k & I_k & \cdots I_k\\ \cdots & \cdots & \\ I_k & I_k & \cdots I_k\end{pmatrix}\begin{pmatrix}1_k\\1_k\\\cdots\\1_k\end{pmatrix} = lk(m-l).
$$

Similarly, $1^T(J_{(m-l)\times l}\otimes I_k) = lk(m-l)$. Applying the aforementioned equations into $Kf(G[F, u_1, u_2, \ldots, u_k; H_v, l])$, we obtained the required result in (ix).

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

All the authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

FUNDING

This work was supported by the National Natural Science Foundation of China (no. 61963013), the Science and Technology Plan of Gansu Province(18JR3RG206), and the Research and Innovation Fund Project of President of Hexi University(XZZD2018003).

REFERENCES

1. Klein DJ, Randić M. *acutec*Resistance Distance. *J Math Chem* (1993) 12:81–95. doi:10.1007/bf01164627
2. Huang S, Zhou J, Bu C. Some Results on Kirchhoff index and Degree-Kirchhoff index. *MATCH Commun Math Comput Chem* (2016) 75: 207–22.
3. Cao J, Liu J, Wang S. Resistance Distances in corona and Neighborhood corona Networks Based on Laplacian Generalized Inverse

Approach. *J Algebra Appl* (2019) 18(3):1950053. doi:10.1142/s0219498819500531
4. Liu J-B, Pan X-F, Yu L, Li D. Complete Characterization of Bicyclic Graphs with Minimal Kirchhoff index. *Discrete Appl Maths* (2016) 200:95–107. doi:10.1016/j.dam.2015.07.001
5. Sun L, Wang W, Zhou J, Bu C. Some Results on Resistance Distances and Resistance Matrices. *Linear and Multilinear Algebra* (2015) 63(3):523–33. doi:10.1080/03081087.2013.877011
6. Bapat RB. *Graphs and Matrices*. London/New Delhi: Springer/Hindustan Book Agency (2010). Universitext.
7. Chen H, Zhang F. Resistance Distance and the Normalized Laplacian Spectrum. *Discrete Appl Maths* (2007) 155:654–61. doi:10.1016/j.dam.2006.09.008
8. Xiao W, Gutman I. Resistance Distance and Laplacian Spectrum. *Theor Chem Acc Theor Comput Model (Theoretica Chim Acta)* (2003) 110:284–9. doi:10.1007/s00214-003-0460-4
9. Yang Y, Klein DJ. A Recursion Formula for Resistance Distances and its Applications. *Discrete Appl Maths* (2013) 161:2702–15. doi:10.1016/j.dam.2012.07.015
10. Yang Y, Klein DJ. Resistance Distance-Based Graph Invariants of Subdivisions and Triangulations of Graphs. *Discrete Appl Maths* (2015) 181:260–74. doi:10.1016/j.dam.2014.08.039
11. Barik S. On the Laplacian Spectra of Graphs with Pockets. *Linear and Multilinear Algebra* (2008) 56:481–90. doi:10.1080/03081080600906463
12. Barik S, Sahoo G. Some Results on the Laplacian Spectra of Graphs with Pockets. *Electron Notes Discrete Maths* (2017) 63:219–28. doi:10.1016/j.endm.2017.11.017
13. Bapat RB, Gupta S. Resistance Distance in Wheels and Fans. *Indian J Pure Appl Math* (2010) 41:1–13. doi:10.1007/s13226-010-0004-2
14. Bu C, Yan B, Zhou X, Zhou J. Resistance Distance in Subdivision-Vertex Join and Subdivision-Edge Join of Graphs. *Linear Algebra its Appl* (2014) 458:454–62. doi:10.1016/j.laa.2014.06.018
15. Liu X, Zhou J, Bu C. Resistance Distance and Kirchhoff index of *R*-Vertex Join and *R*-Edge Join of Two Graphs. *Discrete Appl Maths* (2015) 187:130–9. doi:10.1016/j.dam.2015.02.021
16. Ben-Israel A, Greville TNE. *Generalized Inverses: Theory and Applications*. 2nd ed. New York: Springer (2003).
17. Bu C, Sun L, Zhou J, Wei Y. A Note on Block Representations of the Group Inverse of Laplacian Matrices. *Electron J Linear Algebra* (2012) 23:866–76. doi:10.13001/1081-3810.1562
18. Zhang FZ. *The Schur Complement and its Applications*. New York: Springer-Verlag (2005).
19. Liu Q. Some Results of Resistance Distance and Kirchhoff index of Vertex-Edge corona for Graphs. *Adv Mathematics(China)* (2016) 45(2):176–83.
20. Liu J-B, Pan X-F, Hu F-T. The {1}-inverse of the Laplacian of Subdivision-Vertex and Subdivision-Edge Coronae with Applications. *Linear and Multilinear Algebra* (2017) 65:178–91. doi:10.1080/03081087.2016.1179249
21. Liu J-B, Cao J. The Resistance Distances of Electrical Networks Based on Laplacian Generalized Inverse. *Neurocomputing* (2015) 167:306–13. doi:10.1016/j.neucom.2015.04.065
22. Xie P, Zhang Z, Comellas F. On the Spectrum of the Normalized Laplacian of Iterated Triangulations of Graphs. *Appl Maths Comput* (2016) 273:1123–9. doi:10.1016/j.amc.2015.09.057
23. Xie P, Zhang Z, Comellas F. The Normalized Laplacian Spectrum of Subdivisions of a Graph. *Appl Maths Comput* (2016) 286:250–6. doi:10.1016/j.amc.2016.04.033

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

frontiers | Frontiers in Physics

REVIEW
published: 28 June 2022
doi: 10.3389/fphy.2022.823564

Network Robustness Revisited

Thilo Gross[1,2,3]* *and Laura Barth*[1,2,3]

[1]Helmholtz Institute for Functional Marine Biodiversity (HIFMB), Oldenburg, Germany, [2]Alfred-Wegener-Institute, Helmholtz Centre for Marine and Polar Research, Bremerhaven, Germany, [3]Institute for Chemistry and Biology of the Marine Environment (ICBM), Carl-von-Ossietzky University, Oldenburg, Germany

The robustness of complex networks was one of the first phenomena studied after the inception of network science. However, many contemporary presentations of this theory do not go beyond the original papers. Here we revisit this topic with the aim of providing a deep but didactic introduction. We pay attention to some complications in the computation of giant component sizes that are commonly ignored. Following an intuitive procedure, we derive simple formulas that capture the effect of common attack scenarios on arbitrary (configuration model) networks. We hope that this easy introduction will help new researchers discover this beautiful area of network science.

Keywords: generating functions, attacks on networks, giant component, complex networks, robustness

OPEN ACCESS

Edited by:
Saray Shai,
Wesleyan University, United States

Reviewed by:
Renaud Lambiotte,
University of Oxford, United Kingdom
Sergio Gómez,
University of Rovira i Virgili, Spain

***Correspondence:**
Thilo Gross
thilo2gross@gmail.com

Specialty section:
This article was submitted to Social Physics, a section of the journal Frontiers in Physics

Received: *27 November 2021*
Accepted: *30 May 2022*
Published: *28 June 2022*

Citation:
Gross T and Barth L (2022) Network Robustness Revisited. Front. Phys. 10:823564. doi: 10.3389/fphy.2022.823564

1 INTRODUCTION

In 2000 Albert, Jeong, and Barabási published a groundbreaking paper on the error and attack tolerance of complex networks [1]. At the time of writing this paper has been cited nearly 10^4 times, and one of the paper's take-home messages, the uncanny stability of scale-free networks, is widely known beyond the academia. Today the study by Albert et al. is rightfully counted among the founding papers of modern network science. Shortly thereafter, Newman, Strogatz, and Watts published a mathematical theory on the size of connected components in networks with arbitrary degree distribution [2]. Although some of these results were already known in computer science [3], Newman et al.'s rediscovery popularized them in physics by phrasing them in a convenient and accessible way. Together with other landmark papers published around the same time, these works further accelerated network science which at the time was already rapidly gaining momentum.

Looking back from the present day, it is clear that several important lines of research directly originated from these foundational papers. The mathematics of attacks on networks, has informed work on the prevention of power cuts [4, 5], fragmentation of communication networks [6, 7], cascading species loss in food webs [8], epidemics [9–11], financial crashes [12–14] and misinformation [15]. Some important subsequent developments include the extension of the theory to networks with degree correlations [16, 17], clustering [18, 19], and block structure [20]. Moreover structural robustness has been extended to other types of attacks such as cascading failures [21] and bootstrap percolation [22, 23] and also other classes of systems such multilayer [5, 24], higher order [25] and feature-enriched networks [26].

The broad variety of applications makes clear that the theory of network robustness is not the study of an isolated phenomenon, but provides a powerful tool for thinking about network structure. When such new tools are discovered in science they usually go through a phase of tempering where, the underlying mathematics get formulated and subsequently reshaped until a canonical form emerges. For network robustness an important step in this tempering process is the Review by Mark Newman [27], which combines known results from graph theory with new approaches to formulate a widely applicable mathematical theory of network robustness.

Our goal here is not to argue that robustness is the most important topic in network science. There are other topics which were already going strong at the time, and some of them such as network dynamics, and community structure may address a wider range of applications. In fact, to a network scientist it should be apparent that arguing about the relative importance of field is largely meaningless as long as they remain densely interlinked and thus form part of an emergent whole.

Over the past decades the theory of network robustness has certainly grown into one of the main pillars of modern network science. It is included in several influential reviews and textbooks [28–31]. However, in current literature, the discussion of robustness does not usually go deeper than Newman's concise presentation. Moreover, there seem to be several very useful corollaries to basic results on robustness, which have not been spelled out in the literature. Finally, while the hallmark robustness of scale-free networks is widely known, the several caveats and flip-sides to this result are known by experts but have received much lesser attention.

It is our belief that under normal circumstances much more tempering of the theory of network robustness would likely have happened. However, at the time network science was moving extremely fast and a small number of network scientists found themselves suddenly in a position where they could suddenly make a significant impact on a vast range of applications. In this situation, it was more attractive to go forward to apply and extend the theory rather than to try to rephrase its equations, provide didactic examples, or ponder philosophical issues at its foundations. While all of these things have still happened to some extent, we believe that it is nevertheless valuable to revisit those basic foundations.

The present paper is based on experience gathered while teaching the mathematics of networks robustness over 12 years to different audiences in different departments and on different continents. The paper seeks to provide a retelling of the basic theory that governs the structural robustness of simple networks (configuration model graphs) against different forms of node and link removal. We take the liberty to discuss certain issues at greater length than comparative texts to provide a deep but simple introduction. The presentation is mathematical but, broken into simple steps. We further illustrate the theory by worked examples, including a class of attack scenarios that is exactly solvable with pen and paper. Along the way, we discover some shortcuts and neat equations by which even complicated scenarios can be quickly evaluated. Going beyond mathematics we crystallize the main insights from the calculations into concise take-home messages. We hope that new researchers entering this field will find this introduction of a well-known topic helpful.

2 GENERATING FUNCTIONS

The exploration of networks builds heavily on the combinatorics of probability distributions. When working with such distributions, we often represent them in the form of sequences

$$p_k = (p_0, p_1, p_2, p_3, ...). \tag{1}$$

FIGURE 1 | A four-sided die. In contrast to six-sided dice the outcome of a roll is determined by the number of the face on the bottom. The configuration shown in the picture corresponds to an outcome of 2.

Sequences are intuitive objects, which store information straight forwardly, but they do not come equipped with a lot of powerful machinery. If we want to compute, say, the mean of a distribution, we have to take the elements out of the sequence one-by-one and then process them one-by-one [32]. By contrast, continuous functions, are mathematical objects that come with a lot of machinery attached; they can be evaluated at different points, inverted, and concatenated. Most importantly, they can be differentiated, enabling us to apply the powerful toolkit of calculus.

The idea to use functions instead of sequences to store and process distributions lead to the concept of generating functions. An excellent introduction to generating functions can be found in [32]. In this section, we provide a brief summary of their main properties that are relevant in the context of attacks on networks.

A sequence can be converted into a function by interpreting it as the sequence of coefficients arising from a Taylor expansion. Applying the Taylor expansion backward turns a sequence p_k into the function

$$G(x) = p_0 + p_1 x + p_2 x^2 + p_3 x^3 + ... = \sum_{k=0}^{\infty} p_k x^k. \tag{2}$$

This function is the so-called *generating function* of p_k. Note that the variable x does not have any physical meaning, it is merely used as a prop that helps us encode the distribution.

In the following we omit writing the argument of generating functions explicitly if it is just x, i.e. we will refer to the generating function above just as G, instead of writing $G(x)$.

For illustration we consider the probability distribution of a (not necessarily fair) four-sided die (see **Figure 1**). We denote the probability of rolling k on a single die roll as p_k. Then the generating function for the four-sided die is

$$G_{1d4} = p_1 x + p_2 x^2 + p_3 x^3 + p_4 x^4, \tag{3}$$

where we borrowed the notation 1d4 for "1 four-sided die roll" that is commonly used in roleplaying games.

2.1 Distribution

From the generating function we can recover the distribution by a Taylor expansion,

$$p_k = \frac{1}{k!}\left(\frac{d}{dx}\right)^k G\Big|_{x=0}. \tag{4}$$

2.2 Norm

In many cases it is unnecessary to recover the sequence as many properties of interest can be computed directly from the generating function. One of these is the norm of p_k, which we can compute as

$$|p_k| = G(1). \tag{5}$$

For example, for our four-sided dice, we can confirm

$$G_{1d4}(1) = p_1 + p_2 + p_3 + p_4. \tag{6}$$

2.3 Mean

Let's see what happens if we differentiate a generating function. For example,

$$G'_{1d4} = p_1 + 2p_2x + 3p_3x^2 + 4p_4x^3 = \sum_{k=0}^{\infty} k p_k x^{k-1}. \tag{7}$$

The differentiation has put a factor k in front of each of the terms. If we now evaluate this expression at $x = 1$ we arrive at

$$G'_{1d4}(1) = p_1 + 2p_2 + 3p_3 + 4p_4. \tag{8}$$

which is the expectation value of the die roll. Also, for any other distribution, we can compute the mean of the distribution as

$$\langle k \rangle = G'(1). \tag{9}$$

2.4 Higher Moments

We can also compute higher moments of the distribution from the generating function in a similar manner. Above, we saw that we can use differentiation to put a prefactor k in front of the terms of the sum in the generating function, however, this also lowered the exponents on the x one count. We can 'heal' the exponents after differentiation by multiplying x again, i.e.

$$x\frac{dG}{dx} = \sum_{k=0}^{\infty} k p_k x^k. \tag{10}$$

Repeating the differentiation and multiplication n times a prefactor of k^n can be constructed, which allows us to compute

$$\langle k^n \rangle = \sum_{k=0}^{\infty} k^n p_k = \left(x\frac{d}{dx}\right)^n G\Big|_{x=1}. \tag{11}$$

2.5 Adding Distributions

Suppose we are interested in the probability distribution of the sum of two rolls of the four-sided die. We could work out the probability for the individual outcomes. For example we can arrive at a result of 4 by rolling a 2 on the first roll and a 2 on the second roll (probability ${p_2}^2$) or a 1 on the first and a 3 on the second (p_1p_3) or vice versa (p_3p_1) which adds to up to a total probability ${p_2}^2 + 2p_1p_3$ for a result of 4.

The generating function for the sum of two four-sided die rolls is

$$\begin{aligned} G_2d4 = {} & {p_1}^2x^2 + 2p_1p_2x^3 + ({p_2}^2 + 2p_1p_3)x^4 + (2p_1p_4 + 2p_2p_3)x^5 \\ & + ({p_3}^2 + 2p_2p_4)x^6 + 2p_3p_4x^7 + {p_4}^2x^8. \end{aligned} \tag{12}$$

Here the first term says that you can get a two by rolling two ones, and so on.

Looking at the expression for G_{2d4} it is interesting to note that the combinatorics of the terms is the same that we find in the multiplication of polynomials. This points to a more efficient way for finding G_{2d4}:

$$G_{2d4} = \left(p_1x + p_2x^2 + p_3x^3 + p_4x^4\right)^2 = (G_{1d4})^2. \tag{13}$$

So, we can find the generating function for the sum of two die rolls simply as the square of the generating function of one die roll. The same rule holds more generally: Even if we compute the sum of random variables drawn from different distributions, then the generating function for the sum is the product of the generating functions for the parts.

2.6 Adding Constants to Distributions

Suppose we want to roll our four-sided die and then add 2 two to the result. We can think of the number 2 as the result of a random process that results in the outcome 2 with 100% probability. The generating function for such a process is

$$G_2 = x^2. \tag{14}$$

We can now use the rule for adding distributions to find the generating function that describes the result of adding two to a four-sided die roll,

$$G_{1d4+2} = G_2G_{1d4} = x^2G_{1d4}. \tag{15}$$

Generalizing from this result, we can say that when we add n to the outcome of a random process, the generating function that describes the sum is the generating function of the process times x^n.

2.7 Adding a Random Number of Random Variables (Dice of Dice)

Picture a situation in a game where you find a random number of bags, each containing a random number of gold pieces. The player rolls one die to determine the number of bags, and then one die for each bag to determine the gold in that particular bag. The total amount of gold found can then be computed by summing over the values from the individual bags. For example, the player might roll a 2 on the first roll, showing that they found 2 bags. Then they roll 1 and 3, finding a single gold piece in the first bag and three in the second for a total of four.

To find the generating function that governs the amount of gold, we could think as follows: With probability p_1, we roll a 1 on the first roll, so in this case, we find only one bag. Hence the generating function for the outcome is identical to the generating function of one bag (say, G_{1d4}). With probability p_2, we roll a 2 on the first roll. Thus, we get two bags and, using the results above, our earnings, in this case, are described by $G_{2d4} = (G_{1d4})^2$. Putting all four possible scenarios together, we find the generating function for the total amount of gold

$$G_{(1d4)d4} = p_1 G_{1d4} + p_2 (G_{1d4})^2 + p_3 (G_{1d4})^3 + p_4 (G_{1d4})^4, \quad (16)$$

where the first term corresponds to the scenario where we get one bag, the second corresponds to the scenario where we get two, etc.

Looking at the equation above, we note that it resembles a polynomial of G_{1d4}; we can write it as

$$G_{(1d4)d4} = G_{1d4}(G_{1d4}). \quad (17)$$

Again, the same rule holds generally: Suppose we have a random process p described by a generating function P, and we want to sum over s outcomes of p together, where s is drawn from a distribution with generating function S. The generating function for the sum is then

$$G = S(P). \quad (18)$$

3 EXISTENCE OF THE GIANT COMPONENT

Large sufficiently-random networks have two distinct phases. In one of these, the network consists of isolated nodes and small components, whereas in the other there is a giant component that contains a finite fraction of all nodes, and hence has an infinite size in the limit of large network size [33–35]. The central question that we review in this paper is how the removal of nodes and links affects the giant component.

3.1 Essential Distributions

An important starting point for our exploration of giant components is the networks *degree distribution*, i.e. the probability distribution that a randomly-picked node has k links. We describe this distribution by the sequence p_k and its generating function

$$G = \sum_{k=0}^{\infty} p_k x^k. \quad (19)$$

the expectation value of the degree distribution is the mean degree

$$z = \sum_{k=0}^{\infty} k p_k = G'(1). \quad (20)$$

A second distribution of interest is the *excess degree distribution* q_k. If we follow a random link in a random direction, q_k is the probability to arrive at a node that has k links in addition to the one we are traveling on. Finding the excess degree distribution is an example of many calculations in network science that become easier when we think about it in terms of endpoints of links. When we follow a random link (in a random direction) we arrive at a random endpoint. The probability to find k additional links on the node is the same as the probability that a randomly-picked endpoint is on a node of degree $k + 1$. Hence we can compute the excess degree distribution as

$$q_k = \frac{\text{Number of endpoints on nodes of degree } k+1}{\text{Number of all endpoints in the network}} = \frac{N(k+1)p_{k+1}}{Nz} = \frac{(k+1)p_{k+1}}{z}. \quad (21)$$

The generating function for this distribution is

$$Q = \sum_{k=0}^{\infty} q_k x^k = \sum_{k=0}^{\infty} \frac{(k+1)p_{k+1}}{z} x^k = \frac{1}{z} \sum_{k=0}^{\infty} k p_k x^{k-1} = \frac{G'}{z}. \quad (22)$$

The expectation value of the excess degree distribution is the *mean excess degree*,

$$q = \sum_{k=0}^{\infty} k q_k = Q'(1) = \frac{G''(1)}{z}, \quad (23)$$

i.e., the expected number of additional links we find when arriving at a node at the end of a random link.

3.2 Existence of the Giant Component

In the following, we consider configuration model networks, that is, networks that are formed by randomly connecting nodes of prescribed degree [3, 36]. In such networks a giant component exists if $q > 1$. A mathematical derivation of this result can be found in [2]. The same result is already derived in principle [36], but stated in a more complicated and less catchy form, as the concept of excess degree had not been formulated. Here, we skip this derivation of this formula, but, to gain intuition, consider the following argument: if we walk on a network and find on average more than one new link on every node that we visit, we can continue exploring new links until we have seen a finite fraction of the network.

Despite its intuitive nature, it is good to keep in mind that the $q > 1$ condition does not hold in networks subjected to other organizing principles. Thus it is easy to come up with specific networks that have $q = 100$ but no giant component or a network with $q = 0.01$ that has a giant component (see **Supplementary Appendix**). Although such exceptional networks exist, the $q > 1$ condition provides a reasonable guide for many real-world applications. In particular, the configuration model does not have degree correlations or an abundance of short cycles and under these conditions, the $q > 1$ condition holds.

3.3 Size of the Giant Component

One of the most subtle and intriguing calculations in network science is determining the size of the giant component. The canonical derivation of this equation starts with a self-consistency statement.

A node is not part of the giant component if none of its neighbors is part of the giant component.

Note that the statement is phrased in negative form; it is a condition for being outside the giant component, rather than

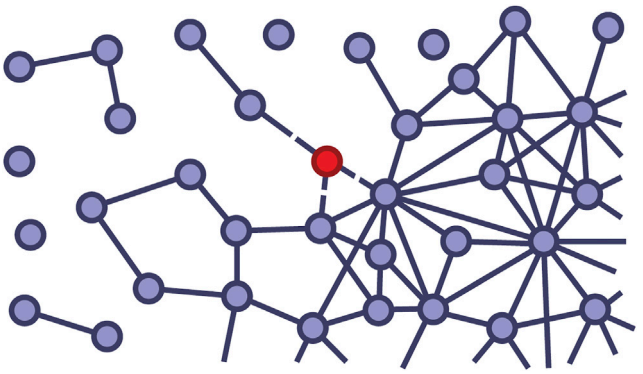


FIGURE 2 | Illustration of the hypothetical cutting of links to find a formula for the giant component size. We pick a random node (red), then cut all of its links. We can say that the probability that the randomly picked node is not in the giant component before the cutting is the same as the probability that none of the node's former neighbors are part of the giant component after the cutting. This statement gives us a self-consistency condition from which the giant component size can be calculated. The cutting of links is essential, as it enables us to treat giant component members of the former neighbors as independent random variables.

being inside it. One good reason for this formulation is that it makes the equations more concise, as we'll see below. An unfortunate side effect is that it makes it easier to gloss over a complication that occurs in the next steps.

To arrive at a useful mathematical equation, we need to translate the self-consistency statement into a probabilistic form

> The probability that a randomly picked node is not part of the giant component is the same as the probability that none of its neighbors is part of the giant component.

We can now assign a symbol to 'the probability that a node is not part of the giant component'; say u. So, the first half of the statement above says, $u = \ldots$. But what about the second half? It is tempting to jump to the conclusion that for a node of degree k, a term of the form u^k will appear. But, let's not go so fast, we first need to deal with some complications.

One problem is that the probabilities in the second half of our statement are not *independent* probabilities. After all, if a node is in the giant component, all of its neighbors must be in the giant component as well. This is bad news because the common mathematical rules for working with probabilities that we often take for granted do not apply.

For example, if a and b are independent probabilities of events, the probability that both events occur is ab, but this isn't necessarily true if the events are interdependent. But if event b must occur if a occurs then, the probability that both occur is just a. If we take the interdependence of probabilities into account, our carefully crafted statement above just translates to $u = u$, which would be useless.

The beauty of mathematical modeling is that by carefully thinking about our definitions, we can often arrive at quantities that work well with mathematics. In the present case, we can use a little twist in the statement to make the probabilities independent:

> The probability that a randomly picked node is not part of the giant component is the same as the probability that none of the neighbor's neighbors nodes remain in the giant component after we have removed all of the random node's links.

So now we pick a random node, make a list of all of it is neighbors, remove all links from the node and then check whether it is former neighbors are still part of the giant component (**Figure 2**). Because the links to the randomly picked node are broken by the time that we check giant component membership, the probability that the former neighbors are part of the giant component is now independent.

Having dealt with the issue of interdependence, we could go straight to the solution. However, instead, let us first make an intuitive, but naive attempt. This will lead to a wrong but nevertheless interesting result.

As before, we read the first half of the statement above as $u = \ldots$. To deal with the second half of the statement, we define v as the probability that a given neighbor is not part of the giant component (after the links have been cut). Moreover, let's assume that the degree of our randomly picked node is the mean degree z (for a first attempt, it is worth a try). Under these assumptions, we can translate the statement above to

$$u = v^z. \qquad [\textbf{Naive attempt, first half}] \tag{24}$$

Now we have to ask, what is the probability that one of the neighbors is not part of the giant component? If the neighbors were completely random nodes, we could assume $v \approx u$, but we have reached these nodes by the following link. We can now apply the same idea as before: The neighbor is not part of the giant component if none of their neighbors is part of the giant component (after cutting off their links), and hence

$$v = v^q. \qquad [\textbf{Naive attempt, second half}] \tag{25}$$

Note that the previous **Eq. 24** links two different variables u and v, which appear because a randomly-picked node is statistically different from a randomly picked neighbor. By contrast, the second equation **Eq. 25** contains two references to v because a random neighbor is statistically similar to a neighbor's neighbor. The second equation is closed, so we can solve it for v and then use v to compute u. Using that the proportion of nodes in the giant component is $s = 1 - u$, we can summarize the solution as follows

$$\begin{aligned} s &= 1 - v^z \\ v &= v^q. \end{aligned} \qquad [\textbf{Naive attempt, summary}] \tag{26}$$

This was a fund derivation, but unfortunately, the result is now what we wanted from the second equation we can see that the solutions are $v = 0$ or $v = 1$, which mean $s = 0$ or $s = 1$, which seems to say, all nodes are in the giant component or none. This can't be right. In addition, there is solution $q = 1$, which perhaps hints that something is happening at $q = 1$, so perhaps not all is lost?

Thinking about the solutions again, we can see that $s = 0$ is a direct consequence of the self-referential nature of our approach: If we just declare every node to be not in the giant component, the result is wrong but self-consistent. Hence it is good to keep in mind that $s = 0$ can be a pathological solution that arises from the peculiarities of the approach. The situation is worse for the solution $s = 1$. This is clearly wrong as our network may well contain some nodes of degree 0 which, certainly can't be in the giant component. Let's understand why we arrive at this erroneous result: In our reasoning, we assumed that every node had the mean degree z. By making all nodes the same, we have ended up at a result where all nodes join or leave the giant component together.

We now understand that the key to a better result is to take the heterogeneity between nodes into account. So instead of assuming that all nodes have the mean degree z or q, let's work with the full degree distributions. Our randomly picked node has degree k with probability p_k, and, using the same reasoning as above, the neighbors of a node of degree k are not part of the giant component (after link-cutting) with probability v^k. So that a randomly picked node has degree k *and* is not in the giant component is $p_k v^k$. Similarly, the probability that a randomly picked neighbor has excess degree k and is not in the giant component is $q_k v^k$. Summing over all possibilities for k, we find the equations

$$\begin{aligned} s &= 1 - \sum_k p_k v^k \\ v &= \sum_k q_k v^k. \end{aligned} \qquad [\textbf{Solution}] \tag{27}$$

Examining the form of the solution, we may notice that the generating functions G and Q appear. Hence, we can write the equations for the giant component size as

$$\begin{aligned} v &= Q(v) \\ s &= 1 - G(v). \end{aligned} \qquad [\textbf{Elegant form of solution}] \tag{28}$$

3.4 Degree Distribution Inside the Giant Component

A final ingredient that is sometimes useful is the degree distribution inside the giant component, i.e. the degree distribution that we would find if all the nodes outside the giant component were removed [3, 37]. We already know that the probability that a randomly drawn node has degree k and is not in the giant component is

$$p_k{}^{\text{out}} = p_k v^k. \tag{29}$$

The probability that a node has degree k and is inside the giant component, can be written as

$$p_k{}^{\text{in}} = p_k - p_k{}^{\text{out}} = p_k(1 - v^k). \tag{30}$$

This probability distribution gives us the probability that a node is inside the giant component and has degree k, but what we are interested in is the degree distribution of random nodes picked from the giant component. We can find this by dividing $p_k{}^{\text{in}}$ by the probability s that a randomly picked node is in the giant component, which leads to

$$p_k{}^{\text{gc}} = \frac{p_k(1 - v^k)}{s}. \tag{31}$$

We can use this result to write the generating function for the degree distribution inside the giant component as

$$G_{\text{gc}} = \frac{\sum_k p_k(1 - v^k)x^k}{s} = \frac{G(x) - G(vx)}{1 - G(v)}. \tag{32}$$

4 ATTACKS AND DAMAGE IN NETWORKS

In the sections above, we established some useful mathematics for estimating the size of the giant component in networks. We are now ready to build a second layer of tools on top of these that capture the effect of different types of attacks and damage in networks.

4.1 Random Link Removal

We start by considering an attack that removes links from the network at random. Before the attack, the network is described by the degree distribution p_k. Then links are removed at random, such that after the attack, each link survives with probability c (to remember this more easily, we can call this the cir-vival probability).

We now ask, what is the degree distribution after the attack? If we were to randomly pick a node from the network after the attack, the probability to pick a node that had k links before the attack is p_k. Each of these links has a chance c to survive the attack. We can also describe the survival in terms of a probability distribution. A link that was one link before the attack is still one link after the attack, with probability c, and it is zero links with probability $1 - c$. So the degree of a randomly-picked node, after the attack, is computed as a sum over a random number of random variables. This is exactly the sort of calculation that is covered by the "dice of dice" rule from **Section 2**.

To apply the dice-of-dice rule, we need to describe the attack by a generating function,

$$A = (1 - c)x^0 + cx^1 = 1 + (x - 1)c, \tag{33}$$

which means 1 with probability c and 0 with probability $1 - c$. Using the dice-of-dice rule we can then write the degree generating function after the attack as

$$G_{\text{a}} = G(A). \tag{34}$$

This equation is a powerful tool, allowing us to derive some results very quickly. For example, we can compute the mean degree after the attack as

$$z_{\text{a}} = G_{\text{a}}'(1) = G'(A(1))A'(1) = cG'(1) = cz, \tag{35}$$

where we used the normalization condition $A(1) = 1$. This "norm reduction" step is a staple of generating function calculations and is one of the reasons why these calculations are often enjoyable.

Here, the result shows that removing a proportion of the links reduces the mean degree by the same proportion, regardless of the degree distribution.

Similarly, we can find the generating function of the excess degree distribution after the attack Q_a by substituting the attack function A into Q,

$$Q_a = Q(A). \tag{36}$$

Using generating functions, we can prove this rule in a single line,

$$Q_a = \frac{G_a'}{G_a'(1)} = \frac{G'(A)A'}{G'(A(1))A'(1)} = \frac{G'(A)}{G'(A(1))} = Q(A), \tag{37}$$

where we used $A'(x) = A'(1)$, a property of the attack function. The mean excess degree after the attack is

$$q_a = Q_a'(1) = Q'(A(1))A'(1) = Q'(1)c = cq. \tag{38}$$

This shows that, if we remove a proportion of the links at random, then, also the mean excess degree is reduced by the same proportion. We can use **Eq. 38** to calculate the proportion of links that need to be removed from a network to break the giant component. Suppose we have a network with excess degree q before the attack and $q_a = cq_b$ after the attack. The attack will break the giant component, if $q_a < 1$, which requires $c < 1/q$. Hence the proportion r of links we need to remove from the network to break the giant component by random link removal is

$$r = 1 - c = 1 - \frac{1}{q_b} = \frac{q-1}{q}. \tag{39}$$

For example, in the early stages of the COVID-19 pandemic, one infected person infected on average 3 other people. This number is the mean excess degree of the network in which nodes are infected people and links are contacts that have led to infections. If we had managed to remove 2/3 of the links from the transmission network through hygiene and social distancing, it would have broken the giant component on where the virus was spreading and stopped the pandemic in its tracks. Sadly, these numbers are by now woefully outdated due to the evolution of later variants, which are more transmissible.

The results we derived so far also permit a first glimpse at the stability of heterogeneous networks. Networks that contain different node degrees can have huge mean excess degrees q. Hence we can already see that breaking the giant component in such networks may require the removal of a large proportion of the links. For example, if a network has $q = 20$, removal of $r = 95\%$ of links is required to break the giant component by random link removal.

To summarize the results from this section, we can say that the network properties after random removal of a proportion $r = 1 - c$ of the links are

$$N_a = N \tag{40}$$
$$z_a = cz \tag{41}$$
$$q_a = cq \tag{42}$$
$$G_a = G(A) \tag{43}$$
$$Q_a = Q(A), \tag{44}$$

where $A = cx + (1 - c)$.

4.2 Random Node Removal

Another type of attack on networks is the random removal of nodes. To understand the effect of random node removal, it is useful to imagine it as a two-step process (**Figure 3**). In the first step, we remove just the nodes, which leaves behind the broken stubs of links, by which these nodes were connected to the rest of the network. In a second step, we prune these broken links, what may reduce the degrees of the surviving nodes.

If we remove nodes at random until only a proportion c of the original nodes survives. Already the first step, the removal of the affected nodes, reduces the size of the network. If we had N nodes before the attack, then the number of nodes after the attack is

$$N_h = cN, \tag{45}$$

where we used the label h to indicate that we are now considering the state after the first step, i.e. halfway through the attack.

Let's also consider what this first step does to nodes of degree k. The number of nodes of degree k before the attack is

$$n_k = Np_k. \tag{46}$$

Since the attack removes nodes at random, a proportion c of the nodes of degree k also survive the first step of the attack, hence

$$n_k{}^h = cn_k = cNp_k = N_h p_k. \tag{47}$$

We can use this result to compute the degree distribution, after the first step of the attack,

$$p_k{}^h = \frac{n_k{}^h}{N_h} = p_k. \tag{48}$$

This shows that the first step of the attack, the random node removal itself, does not change the degree distribution of the surviving nodes.

We are not quite done yet, as we still have to clean up the broken links left by the attack. This cleaning up is another example of a calculation that gets easier when we think in terms of endpoints. In the pruning step, a node will lose a given link if the endpoint at the other end of the link was removed in the attack. This means that an attack that removes a certain proportion of all endpoints will remove the same proportion of links from the surviving nodes. Moreover, if we remove a proportion r of the nodes at random, we also remove a proportion r of the endpoints in the system, which implies that in the pruning step we remove a proportion r of the links of the surviving nodes.

Expressed positively, we can say: if a proportion c of the nodes survive, the surviving nodes will retain a proportion c of their links. As the removal of the broken links is essentially random link removal, the same rules as before apply. Thus the mean degree and mean excess degree get reduced by a factor c.

In summary, random removal of a proportion $r = 1 - c$ of the nodes affects the network properties as follows:

$$N_a = cN \tag{49}$$

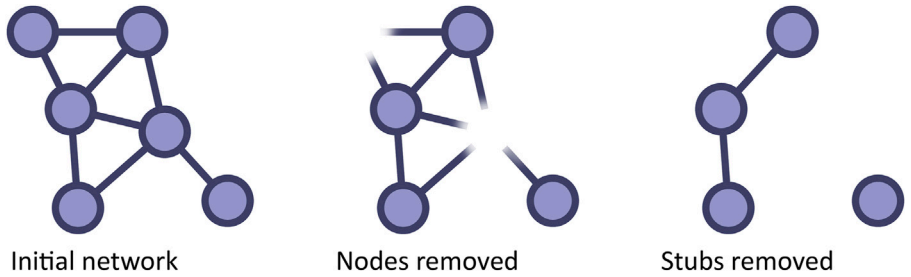


FIGURE 3 | Node removal in a two-step process. Understanding the effect of node removal becomes easier if we picture node removal as a two-step process. Starting from an initial network (left, degrees: 1,2,2,3,4,4) the first step removes the target nodes (here a node of degree 2 and a node of degree 4), but the broken links are kept in the network (center, node degrees 1,2,3,4). In the second step, the broken links are pruned (right, 0,1,1,2). In this example, the mean degree after the first step is $z_h = (1 + 2 + 3 + 4)/4 = 2.5$.

$$z_a = cz \tag{50}$$
$$q_a = cq \tag{51}$$
$$G_a = G(A) \tag{52}$$
$$Q_a = Q(A), \tag{53}$$

where $A = cx + (1 - c)$.

It is interesting to note that random node removal and random link removal affect the network in very similar ways, which allows us to multiply up the effects of different attacks.

For example, if we vaccinate half the population with a vaccine that is 90% effective and then also avoid 1/3 of all contacts. We reduce the network mean excess degree, consequently, the remaining vulnerable network is $0.9 \cdot 0.5 \cdot (2/3) = 0.3$ of its original value. What would certainly, have broken the giant component spread of the SARS-CoV-2 wild-type, but insufficient to break the giant component spread for later variants.

4.3 Targeted Node Removal

The previous section showed that heterogeneous networks, characterized by high values of q, are hard to break by random node removal because we need a proportion of $r = (q - 1)/q$ nodes to break the giant component.

Perhaps we can do better with targeted attacks? The low-dimensional intuition of our daily experience suggests that we can do perhaps much better by attacking naturally existing bottlenecks in the network. A COVID-19 example of this strategy is, for example, trying to stop the virus at national borders; a strategy that has had mixed success.

When it comes to random networks, our real-world intuition can be misleading: Unless we consider networks of low mean degree, which are fragile in any case, bottlenecks arise only as a result of the low-dimensional embedding of networks, for example, due to geographical constraints [38]. The configuration model networks considered here are genuinely high-dimensional structures and thus generally lack strong bottlenecks. While it is possible to fine-tune an attack to split a strongly geographically embedded network, e.g. the road network, trying to find a similarly optimized attack in a random network is pointless.

Even in the absence of bottlenecks, we can still maximize the impact of our attack by targeting highly-connected nodes. As in the case of random node removal, we implement the attack in two steps, where the first step removes only the directly affected nodes but leaves the rest of the degree distribution unchanged. Then the leftover stubs will be removed in a second step.

An important decision is how we encode the targeted removal mathematically. Here, we define r_k as the probability that a randomly-picked node from the original network has degree k *and* is subsequently removed in the attack. Most other papers encode targeted attacks in terms of ρ_k, the removal risk of a node of degree k which is related to r_k via

$$\rho_k = \frac{r_k}{p_k}. \tag{54}$$

While the definition of r_k seems more complicated, we will see below that it leads to particularly nice results.

In actual calculations, r_k is quite intuitive as it follows the same intuition as the degree distribution. Suppose, for example, the degree distribution of our network was 0.5, 0.25, 0.25, such that half the nodes were of degree zero. If we wanted to remove 60% of the nodes of degree 2, then r_k would be 0, 0, 0.15.

Having familiarized with the r_k, let us now consider a degree targeted attack on a general network. As this first step in our calculation, we calculate some properties that quantify the effect of the attack. For this purpose, it is convenient to define the generating function of r_k as

$$R = \sum_{k=0}^{\infty} r_k x^k. \tag{55}$$

In contrast to the generating functions used so far, the norm of r_k is not 1 but, the proportion of nodes removed in the attack, i.e.

$$r = 1 - c = \sum_{k=0}^{\infty} r_k = R(1), \tag{56}$$

where r and c are again the removed and surviving proportions of the nodes.

A second important property is $\tilde{r}$ the proportion of endpoints that are removed directly in the first step of the attack Recall that

$G'(1) = z$ is the mean degree of the nodes in the network. Hence $NG'(1)$ is the number of all endpoints in the network. Analogously, $NR'(1)$ is the number of endpoints that are removed in the first step of the attack. Hence we can compute $\tilde{r}$ as the ratio

$$\tilde{r} = \frac{R'(1)N}{G'(1)N} = \frac{R'(1)}{z}. \tag{57}$$

We can now also defined the proportion of surviving endpoints after the first step

$$\tilde{c} = 1 - \tilde{r}. \tag{58}$$

Let's also have a look at the second derivative of R. For the degree generating G the quantity $G''(1)/z$ is the mean excess degree q. So by analogy we may call

$$\delta = \frac{R''(1)}{z}, \tag{59}$$

the *removed excess degree* by analogy.

We can now write the degree distribution after the first step (removal of targeted nodes). It is helpful to first write the number of nodes of degree k after the removal

$$n_k{}^{\mathrm{h}} = Np_k - Nr_k = N(p_k - r_k), \tag{60}$$

where we have again used h to denote properties after the first step of the attack. To find the degree distribution after the removal, we have to divide by the remaining number of nodes, which we can write as Nc. Hence,

$$p_k{}^{\mathrm{h}} = \frac{N(p_k{}^{\mathrm{b}} - r_k)}{cN} = \frac{p_k - r_k}{c}. \tag{61}$$

The corresponding generating function is

$$G_{\mathrm{h}} = \sum_{k=0}^{\infty} \frac{p_k - r_k}{c} x^k = \frac{G - R}{c}. \tag{62}$$

Using this function, we compute the excess degree generating function after the first step using the relationship $Q = G'/G'(1)$, which implies

$$Q_{\mathrm{h}} = \frac{G_{\mathrm{h}}'}{G_{\mathrm{h}}'(1)} = \frac{G' - R'}{G'(1) - R'(1)} = \frac{G' - R'}{z\tilde{c}}, \tag{63}$$

where we used **Eq. 57** to replace

$$G'(1) - R'(1) = z - z\tilde{r} = z(1 - \tilde{r}) = z\tilde{c}. \tag{64}$$

Let's turn to the second step of the attack and remove the remaining stubs of the broken links. We proceed as in the previous case and define the generating function for the probability that a link remains intact

$$\tilde{A} = \tilde{c}x + 1 - \tilde{c}, \tag{65}$$

and then use the dice-of-dice rule to find the degree and excess degree generating function after the attack

$$\begin{aligned} G_{\mathrm{a}} &= G_{\mathrm{h}}(\tilde{A}) = \frac{G(\tilde{A}) - R(\tilde{A})}{c} \\ Q_{\mathrm{a}} &= Q_{\mathrm{h}}(\tilde{A}) = \frac{G'(\tilde{A}) - R'(\tilde{A})}{z\tilde{c}}. \end{aligned} \tag{66}$$

At this point, we already have the generating functions that we need for giant component calculations, but, for completeness, let's also compute the mean degree and mean excess degree after the attack:

$$z_{\mathrm{a}} = G_{\mathrm{a}}'(1) = \frac{\tilde{A}'(1)}{c}\left(G'(\tilde{A}(1)) - R'\tilde{A}(1)\right) = \frac{\tilde{c}}{c}\left(G'(1) - R'(1)\right) = \frac{z\tilde{c}^2}{c}, \tag{67}$$

$$q_{\mathrm{a}} = Q_{\mathrm{a}}'(1) = \frac{\tilde{A}'(1)}{\tilde{c}} \frac{G''(1) - R''(1)}{z} = q - \delta. \tag{68}$$

The second of these equations justifies why we call δ the removed excess degree. The simplicity of this equation is surprising and probably hints at some deeper insights that may yet be gained.

In summary, some network properties after a degree-targeted attack described by the attack generating function R are

$$N_{\mathrm{a}} = cN \tag{69}$$

$$z_{\mathrm{a}} = z\frac{\tilde{c}^2}{c} \tag{70}$$

$$q_{\mathrm{a}} = q - \delta \tag{71}$$

$$G_{\mathrm{a}} = \frac{G(\tilde{A}) - R(\tilde{A})}{c} \tag{72}$$

$$Q_{\mathrm{a}} = \frac{G'(\tilde{A}) - R'(\tilde{A})}{z\tilde{c}}, \tag{73}$$

where $\tilde{A} = \tilde{c}x + (1 - \tilde{c})$, $\tilde{c} = 1 - R'(1)/z$, $c = 1 - R(1)$ and $\delta = R''(1)/z$.

4.4 Viral Attacks

Another interesting class of attacks that we can treat with the same mathematics are "viral" attacks that propagate across the same network that they are attacking. Real-world examples include computer viruses and certain infrastructure disruptions such as traffic gridlock and cascading line failure in power grids, but also viral advertising campaigns, etc. Even vaccinations could be turned into viral attacks on an epidemic if we let recipients of the vaccination nominate further recipients.

When dealing with viral attacks, one potential pitfall is to confuse ourselves by thinking too much about the dynamic nature of the attack. Network science has good methods for dealing with dynamics, but in this paper, we aim to study attacks from a purely structural angle. We will therefore consider the state of the network after the attack has stopped spreading because it can't reach any more nodes.

If the attack can spread across every link in the network, it will eventually reach every node in the entire component. It is more interesting to consider an attack that can only spread across a certain portion of the links, chosen randomly. For example, only some roads may have enough traffic flowing along them to allow gridlock to spread. In the following, we call such links that can propagate the attack as *conducting links*.

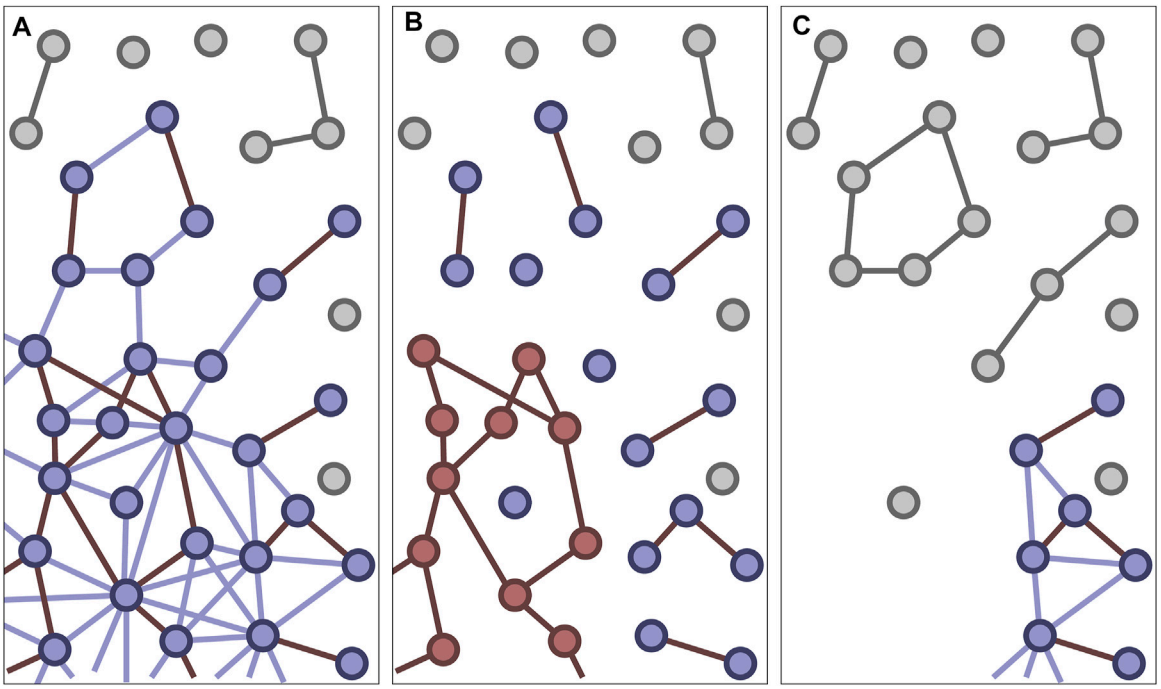


FIGURE 4 | Illustration of a viral attack. Before the attack **(A)** some proportion of the nodes and links is in the giant component (colored), whereas others are in small components (grey). We consider a situation where only a small fraction of the links conduct the attack (dark red links, only marked in giant component). To assess the impact of a viral attack **(B)**, we remove all non-conducting links and compute the size of the giant conducting component (red nodes). After the attack **(C)** all nodes in the giant conducting component and their links have been removed from the original network. The giant component in the remaining network is now smaller as some of its nodes have been destroyed and others have become separated into small components.

Now the attack will infect all nodes that it can reach by a path of conducting links. In other words, the attack reaches the entire component in a different version of the network where we count only the conducting links. Because the non-conducting are now ignored, the components in the network of conducting are smaller than the components in our original network, potentially allowing some nodes to escape the attack.

Considering a proportion w of the links as non-conducting is analogous to a link removal attack on the viral attack. Hence if the non-conducting links are distributed randomly, then we can re-purpose our treatment of random link removal to study how many nodes will be affected by the viral attack. For example, we can see immediately that in a network with mean excess degree q, there is a giant component in the network of conducting links if $(1 - w)q > 1$. Otherwise, a viral attack starting from one node can only spread to a very small number of nodes.

From now on, we refer to the nodes and links that are part of the giant component in the network of conducting links as the *giant conducting component*.

Furthermore, we can use the results of the random-link-removal attack to compute the number of nodes that are affected by a viral attack. For this purpose, we need to construct a pruning function corresponding to the removal of the non-conducting proportion w of the links,

$$A = (1 - w)x + w, \tag{74}$$

which then allows us to compute the giant conducting component size by solving

$$v_c = Q(A(v_c)), \tag{75}$$

$$s_c = 1 - G(A(v_c)). \tag{76}$$

This component size is the proportion of nodes that are removed if an attack starts in the giant conducting component. It is also the probability that a randomly chosen initial spreader will be part of the giant conducting component and hence cause such a large cascade. Otherwise, the initial spreader will be located in a small component of the conducting network and, the attack will only affect a small number of nodes.

A typical question that arises in the context of viral attacks is if the giant component of the original network can survive a viral attack of a given scale. Thinking about this question becomes much easier if we start in the middle and consider a network in which a certain proportion of links y is *not* in the giant conducting component (**Figure 4**), either because they are not conducting, or because they are conducting but part of a smaller component.

We start by constructing the attack generating function R in analogy to our treatment of targeted attacks. If an attack starts in the giant conducting component, it will reach every link except the proportion y. Hence a node of degree k will *not* be affected by the attack with probability y^k. Conversely, nodes of degree k will be affected by the attack with probability $1 - y^k$. Hence the

probability that a randomly picked node has degree k and is affected by the attack is

$$r_k = p_k(1 - y^k). \tag{77}$$

Hence the generating function for the node removal is

$$R = \sum_{k=0}^{\infty} p_k(1 - y^k)x^k = G - G(xy). \tag{78}$$

We can now reuse some results from our treatment of degree-targeted attacks. The proportion of nodes affected by the attack is

$$r = R(1) = 1 - G(y). \tag{79}$$

The proportion of removed endpoints is

$$\tilde{r} = \frac{R'(1)}{z} = \frac{G'(1) - yG'(y)}{z} = 1 - \frac{yG'(y)}{z}, \tag{80}$$

and the reduction in excess degree due to the attack is

$$\delta = \frac{R''(1)}{z} = q - \frac{y^2G''(y)}{z}. \tag{81}$$

Hence, after the attack the proportion of remaining nodes is

$$c = 1 - r = G(y). \tag{82}$$

The proportion of surviving endpoints is

$$\tilde{c} = 1 - \tilde{r} = \frac{yG'(y)}{z}, \tag{83}$$

and the remaining excess degree of the network is

$$q_a = q - \delta = \frac{y^2G''(y)}{z}. \tag{84}$$

We can now construct the pruning function

$$\tilde{A} = \tilde{c}x + \tilde{r}. \tag{85}$$

Using **Eq. 66** we can write the generating functions after the attack

$$G_a = \frac{G(\tilde{A}) - R(\tilde{A})}{c} = \frac{G(\tilde{A}y)}{G(y)} \tag{86}$$

$$Q_a = \frac{G'(\tilde{A}) - R'(\tilde{A})}{z\tilde{c}} = \frac{G'(\tilde{A}y)}{G'(y)}, \tag{87}$$

from which we can compute the giant component size in the usual way.

So far, all of these results are expressed in terms of y. Let's explore how y (the proportion of links that are not in the giant conducting component) is related to the more intuitive w (the proportion of non-conducting links). We start by noting that we have two ways to compute the number of nodes removed in the attack on the giant conducting component. We can compute it from our calculation of the giant conducting component size in **Eq. 76**. Otherwise we can compute it via **Eq. 79** from the attack function R. Combining these two equations we get,

$$G(A(v_c)) = G(y), \tag{88}$$

since G is a rising function, this implies

$$y = A(v_c), \tag{89}$$

which we can compute from w using **Eqs 74** and **75**.

In summary, after a viral attack that can spread across a proportion $1 - w$ of the links in the network, will result in a large outbreak with a probability of $1 - G(y)$, and if it does, will affect the network as follows:

$$N_a = G(y)N \tag{90}$$

$$z_a = \frac{(yG'(y))^2}{zG(y)} \tag{91}$$

$$q_a = \frac{y^2G''(y)}{z} \tag{92}$$

$$G_a = \frac{G(\tilde{A}y)}{G(y)} \tag{93}$$

$$Q_a = \frac{G'(\tilde{A}y)}{G'(y)}, \tag{94}$$

where $y = A(v_c)$, $A = (1 - w)x + w$, and v_c is the solution of $v_c = Q(A(v_c))$.

5 EXAMPLES AND GENERAL RESULTS

The results reviewed in the sections above provide us with a powerful toolkit. We now illustrate this toolkit in a series of examples.

5.1 Robustness to Random Attacks

Let us start with a three-regular graph, where every node has exactly 3 links. This network is interesting because the property of all networks that suffer random attacks on the three-regular graph can be computed analytically, highlighting it as a great example for teaching.

Since all nodes in this network have degree three, the degree generating function before the attack is

$$G = x^3, \tag{95}$$

and the corresponding excess degree generating function is

$$Q = \frac{G'}{z} = x^2, \tag{96}$$

which confirms that, if we follow a random link, we expect to find exactly two additional links at the destination, as it should be.

Because the mean excess degree is only $q = 2$, we can break the giant component already by removing half the links at random, but let's see what happens when we start removing nodes or links at random. Using **Eqs 34** and **36** we know that the generating functions after the attack will be

$$G_a = G(A) = (cx + r)^3, \tag{97}$$

$$Q_a = Q(A) = (cx + r)^2. \tag{98}$$

To find the giant component size we use **Eq. 28** and

$$v = Q_a(v) = (cv + r)^2. \tag{99}$$

This is a quadratic polynomial and can be factorized straight forwardly. Alternatively, we can guess that $v = 1$ will be a solution and then factor $v - 1$ out by polynomial long division. Both ways lead us to

$$v = \frac{(c-1)^2}{c^2} = \frac{r^2}{c^2}, \tag{100}$$

from which we can see in a different way that the v reaches 1 (and consequently the giant component breaks) when we have removed half the links at random (i.e. $r = c$). Let's focus instead on finding the giant component size when it exists. Again following **Eq. 28** we compute

$$\begin{aligned} s &= 1 - G_a(v) = 1 - (cv + r)^3 = 1 - v(cv + r) = 1 - v(r + c)r/c \\ &= 1 - vr/c = 1 - r^3/c^3. \end{aligned} \tag{101}$$

This result shows that the regular graph is initially quite tough. Before we start removing nodes or links, the giant component contains all nodes. For a small attack, the reduction in giant component size initially scales like r^3 and hence removing a small proportion of the nodes and/or links has almost no effect on the size of the giant component in the remaining network. But, once a significant proportion of nodes/links have been removed, the impact on the giant component accelerates and quickly leads to its destruction.

Let us compare these results from the regular graph with a network where three-quarters of the nodes have degree 1 and one quarter has degree 9. This network also has a mean degree $z = 3$, but its mean excess degree is $q = 6$. The generating functions before the attack are

$$G(x) = \frac{3x + x^9}{4}, \tag{102}$$

$$Q(x) = \frac{1 + 3x^8}{4}. \tag{103}$$

To find the size of the giant component before the attack, we solve

$$v = \frac{1}{4} + \frac{3v^8}{4}. \tag{104}$$

While we could solve this equation numerically, an insightful shortcut is to note that the solution must be very close to $v = 1/4$. Using this approximate solution, we can then compute the giant component size as follows:

$$s = 1 - \frac{3v + v^9}{4} = 1 - v\left(\frac{9 + (4v - 1)}{12}\right), \tag{105}$$

where we used $v^8 = (4v - 1)/3$ to avoid the inaccuracy from raising a numerical approximation to the 9th power. We can see that the factor in the bracket is approximately 0 and hence $s = 1 - 3v/4$ = 1–3/16 = 0.8125, which is the correct result up to 4 digits of accuracy.

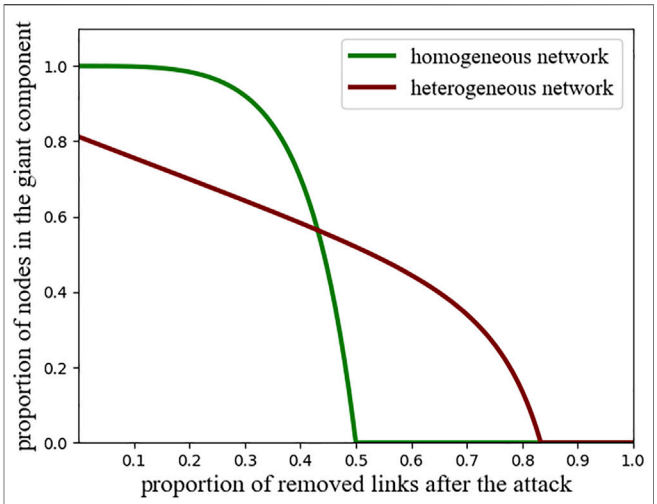


FIGURE 5 | Robustness of homogeneous and heterogeneous networks to random damage. Plotted is the proportion of nodes in the giant component versus removed links after the attack for a homogeneous (green, **Eq. 101**) and heterogeneous (red, **Eq. 108**). The homogeneous networks resist small attacks better whereas, the heterogeneous network survives a higher proportion of removal (Random node removal is described by the same curves, in this case, the proportion of the giant component refers to the proportion of remaining nodes).

The result shows that, in this heterogeneous network, the giant component contains only about 81% of the nodes, even before the attack. Conversely, we know that for a network with $q = 6$ removal of $5/6 \approx 83\%$ of the network is necessary to break the giant component.

To study the effect of the attack in more detail we have to solve

$$v = Q_a(v) = Q(A(v)) = \frac{1 + 3(cv + r)^8}{4}, \tag{106}$$

which we now solve numerically. For teaching (or even a quick implementation on a computer), it is interesting to note that equations of this form can be quickly solved by iteration, i.e. we interpret the equation as an iteration rule

$$v_{n+1} = Q_a(v) = Q(A(v)) = \frac{1 + 3(cv_n + r)^8}{4}. \tag{107}$$

Starting from an initial estimate, say $v_0 = 1/4$, the iteration converges in a few steps due to the high exponent. Once we have obtained the value of v for a given value of r, we can compute the corresponding giant component size as

$$s = 1 - G(\tilde{A}(v)), \tag{108}$$

the result is shown in **Figure 5**. Although the figure confirms that the giant component persists until 5/6 of the nodes or links have been removed, it also shows that for moderate attacks, the homogeneous topology has a giant component that is larger in absolute terms and also initially less susceptible to attacks.

This leads us to an important take-home message. We can say, homogeneous networks are like glass: They are very hard when hit lightly but, strong impacts shatter them. Heterogeneous networks are like foam: Parts can be disconnected even without an attack, and it is easy to tear bits off, but it is very tedious to destroy the giant component in its entirety.

5.2 Targeted Attack on a Heterogeneous Network

Let us now consider a targeted attack on the heterogeneous network from the previous section. For a simple start, we explore what happens when we remove half of the nodes of degree 9, i.e. we are only removing 1/8 of the total number of nodes in the network. In this case, the generating function for the targeted attack is

$$R = \frac{1}{8}x^9, \tag{109}$$

and hence we can compute

$$r = R(1) = \frac{1}{8} \qquad s = 1 - r = \frac{7}{8}, \tag{110}$$

$$\tilde{r} = \frac{R'(1)}{z} = \frac{9}{24} \qquad \tilde{s} = 1 - \tilde{r} = \frac{5}{8}, \tag{111}$$

$$\delta = \frac{R''(1)}{z} = 3. \tag{112}$$

We can now use the formulas derived above to compute the mean degree and the mean excess degree after the attack

$$z_a = z\frac{\tilde{c}^2}{c} = \frac{75}{56} \qquad q_a = q - \delta = 3. \tag{113}$$

So, in this case, removing 1/8 of the nodes already halves the excess degree. We can also ask what proportion p of the nodes we need to remove if we only target nodes having initially degree 9. We can consider the attack $R = rx^9$. Since we need $q_a = 1$ to break the giant component and start with $q = 6$,

$$\delta = 5 = \frac{R''(1)}{z} = 24r. \tag{114}$$

Hence, we can break the giant component by removing $r = 5/24$ of the nodes, which is a little bit more than 20%.

We can also compute the size of the giant component after a proportion r of the nodes is removed in an attack that targets only the high degree nodes. Considering again $R = rx^9$, we first compute the proportion of surviving endpoints using **Eq. 57**

$$\tilde{c} = 1 - \frac{9r}{3} = 1 - 3r, \tag{115}$$

and the pruning function

$$\tilde{A} = (1 - 3r)x + 3r. \tag{116}$$

Which allows us to write the self-consistency condition for v as

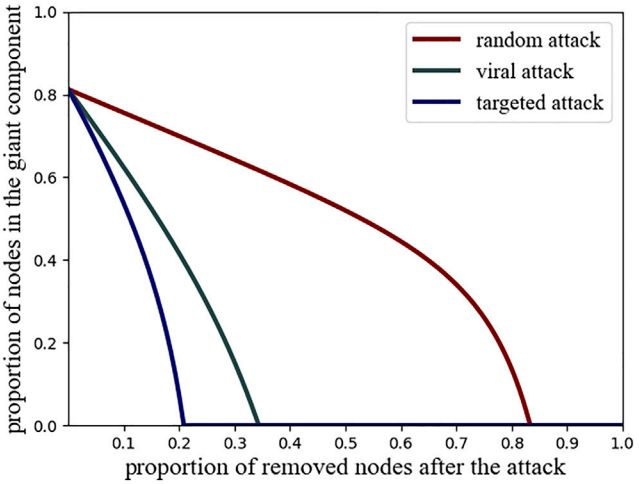


FIGURE 6 | Effect of different types of attacks on heterogeneous networks. Shown is the giant component size of the heterogeneous example network after a random attack (red, **Eq. 108**), a viral attack (green, **Eq. 128**) and an optimal degree-targeted attack (blue, **Eq. 118**). Targeting the nodes of highest degree destroys the giant component very quickly. The viral attack is almost as efficient in destroying the network, while requiring much less information on the node degrees.

$$v = Q_a(v) = \frac{G'(\tilde{A}(v)) - R'(\tilde{A}(v))}{z\tilde{c}} = \frac{1 + 3(1 - 4r)((1 - 3r)v + 3r)^8}{4(1 - 3r)}, \tag{117}$$

and the giant component size as

$$s = 1 - G_a(v) = 1 - \frac{G(\tilde{A}(v)) - R(\tilde{A}(v))}{c} = 1 - \frac{3\tilde{A}(v) + (1 - 4r)\tilde{A}(v)^9}{4(1 - r)}. \tag{118}$$

This again can be solved by numerical iteration or parametrically. A comparison between the effect of the targeted and the random attack on the heterogeneous network is shown in **Figure 6**. This illustrates the fragility of heterogeneous networks to targeted attacks [4, 39]. By contrast, the effect of a targeted attack on a homogeneous network is the same as a random attack, as it contains only nodes of the same degree.

5.3 Viral Attack on a Heterogeneous Network

For our final example, we study a viral attack on the heterogeneous example network. For illustration, we consider the case where 80% of the links are non-conducting, i.e. w = 0.8.

Following **Eq. 74**, we can prune the none conducting links from the network by the pruning function

$$A = 0.2x + 0.8, \tag{119}$$

and hence the generating functions of the conducting network are

$$G_a = G(A) = \frac{3(0.2x + 0.8) + (0.2x + 0.8)^9}{4} \tag{120}$$

$$Q_a = Q(A) = \frac{1 + 3(0.2x + 0.8)^8}{4}. \tag{121}$$

We find the giant conducting component solving **Eq. 75** by iteration:

$$v = Q_a(v), \tag{122}$$

which yields $v \approx 0.735$, and then compute the conducting component size from **Eq. 76**,

$$s_c = 1 - G_a(v) \approx 0.136. \tag{123}$$

This tells us that an attack that starts from a randomly-selected node will lead to a large outbreak with a 13.6% probability, and if it does, it will remove 13.6% of the nodes.

To explore the effect that the removal has on the remaining network, we compute y using **Eq. 89**,

$$y = A(v) \approx 0.947, \tag{124}$$

so almost 95% of links are not in the giant conducting component.

Now that we know y, we can use **Eq. 83** to compute the proportion of surviving endpoints after the attack,

$$\tilde{c} = \frac{yG'(y)}{z} = \frac{3y + 9y^9}{12} \approx 0.697, \tag{125}$$

and the proportion of removed endpoints,

$$\tilde{r} = 1 - \tilde{c} \approx 0.303. \tag{126}$$

We can now construct our pruning function, $\tilde{A}$, for the viral attack itself (**Eq. 85**) and then compute the giant component size by first solving

$$v = Q_a(v) = Q(\tilde{A}(v)), \tag{127}$$

which yields $v \approx 0.252$. And then computing the remaining giant component size as

$$s = 1 - G_a(v) \approx 0.640. \tag{128}$$

In summary, we have studied an example where only 20% of the links actually conduct the attack. With so few links, there is only a 13% chance that it causes a significant outbreak. However, while such an outbreak, if it occurs, removes only 13% of the nodes, it preferentially hits the nodes of high degree and, as a result, only 64% of the nodes in the surviving network remain in the giant component.

Repeating the calculation for different values of w reveals that the viral attack is an intermediate case between random and optimal degree targeted attacks (**Figure 6**). In heterogeneous networks, they are almost as damaging as the optimal degree targeted attack while not requiring the attacker to know the complete degree sequence of the network.

6 CONCLUSION AND DISCUSSION

In this paper, we revisited the well-known topic of attacks on networks. We aimed to present this topic in a consistent and didactic way and show that the effect of four types of attacks (random removal of links, random removal of nodes, degree-targeted removal of nodes, and viral attacks) can be summarized in compact equations. In many cases these equations, can be solved with pen and paper.

Our examples illustrate some important and widely-known take-home messages about the robustness of networks. As these are sometimes misconstrued in the wider literature, let us try to restate these messages clearly:

- Networks with homogeneous degree distributions are like glass, they are incredibly hard when attacked lightly, but heavier attacks can shatter them easily.
- Networks with heterogeneous degree distributions are like foam. Random attacks can quickly detach parts of the giant component. However, shedding the weakest parts enables the giant component to survive significant damage.
- Degree-targeted attacks are relatively pointless against homogeneous networks as the variation in node degrees is low.
- Degree-targeted attacks against heterogeneous networks are devastating and can quickly destroy the giant component.
- Propagating/viral/cascading attacks that spread across the network itself are almost as dangerous as degree targeted attacks as they hit high-degree nodes with high probability.

We emphasize that these are only the most basic insights into configuration-model type networks, and thus strictly hold only in the absence of additional organizing principles such as strong embedding in physical space or the presence of degree correlations and short cycles. Several other papers have extended the theory reviewed here to alleviate these constraints. Notable results include the positive effect of positive degree correlations, which can make the network much more robust against targeted attacks [16, 17], and the effect of clustering of short cycles, i.e., network clustering [18, 19].

For the class of random and degree-targeted attacks, we showed that the effect of these attacks on the mean and mean excess degree can be captured by very simple equations that can be derived relatively straight-forwardly. Moreover, we pointed out a case (the three-regular-graph) for which the giant component size after all types of attacks can be computed analytically in closed form. For other networks, numerical solutions are needed, but they can be solved by quick numerical iteration on a calculator, rather than requiring full-scale numerics.

In this paper, we have often referred to the example of vaccination campaigns, and hence a scenario where we want the attack to succeed. However, many of the insights gained can also be applied to make networks more robust against attacks. Many of the conclusions that have been drawn have been discussed abundantly in the literature. Instead of reiterating these, let us point out some issues that have gained

comparatively less attention. While it is widely known that the giant component in scale-free networks is highly robust, the results from our examples show that more homogeneous networks are robust in a different way: They resist weaker attacks exceptionally well and are also much less susceptible to targeted and viral attacks. It is interesting to reflect on the stability of homogeneous networks against small-scale attacks and damage in a business context. For private businesses, catastrophic events that cause large-scale damage are often not a primary concern, as government actors are expected to intervene in the case of such an event. In comparison, small-damage events typically arrive at a higher rate and will have to be dealt with by the network operator on their own. In this light operating, a very homogeneous network might be in the interest of a business that operates it. However, for governments and the general public optimizing networks in this way, may be detrimental as it leads to low disaster resilience.

The example illustrates a deeper insight into the nature of network robustness: By adjusting topological properties, we can make networks more resilient against certain types of attacks and damage (cf. [20]). However, unless we increase the overall connectivity, this resilience is usually gained at the cost of increasing vulnerabilities to other attacks. In the real world, where increasing connectivity often comes at a steep price, we can still optimize the robustness by shaping the network such that it can optimally withstand the most likely types of damage. However, care must be taken to make sure we also understand the downsides of such optimization.

Perhaps a more important conclusion from the present work is that the physics of attacks on networks is a rewarding field of study. The authors greatly enjoyed revisiting the relevant calculations, and the results highlighted here provide a flexible toolkit that, in our opinion, still has large potential to be more widely used in a broad range of fields. We hope that readers likewise find this review of the foundations of network robustness helpful and will carry this topic into university curricula and new fields of application.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

FUNDING

This work was funded by the Ministry for Science and Culture of Lower Saxony (HIFMB project) and the Volkswagen Foundation (Grant Number ZN3285).

SUPPLEMENTARY MATERIAL

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fphy.2022.823564/full#supplementary-material

REFERENCES

1. Albert R, Jeong H, Barabási A-L. Error and Attack Tolerance of Complex Networks. *Nature* (2000) 406:378–82. doi:10.1038/35019019
2. Newman ME, Strogatz SH, Watts DJ. Random Graphs with Arbitrary Degree Distributions and Their Applications. *Phys Rev E Stat Nonlin Soft Matter Phys* (2001) 64:026118. doi:10.1103/PhysRevE.64.026118
3. Molloy M, Reed B. The Size of the Giant Component of a Random Graph with a Given Degree Sequence. *Combinator Probab Comp* (1998) 7:295–305. doi:10.1017/S0963548398003526
4. Albert R, Albert I, Nakarado GL. Structural Vulnerability of the north American Power Grid. *Phys Rev E Stat Nonlin Soft Matter Phys* (2004) 69:025103. doi:10.1103/PhysRevE.69.025103
5. Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of Failures in Interdependent Networks. *Nature* (2010) 464:1025–8. doi:10.1038/nature08932
6. Cohen R, Erez K, Ben-Avraham D, Havlin S. Breakdown of the Internet under Intentional Attack. *Phys Rev Lett* (2001) 86:3682–5. doi:10.1103/physrevlett.86.3682
7. Doyle JC, Alderson DL, Li L, Low S, Roughan M, Shalunov S, et al. The "robust yet Fragile" Nature of the Internet. *Proc Natl Acad Sci U.S.A* (2005) 102:14497–502. doi:10.1073/pnas.0501426102
8. Dunne JA, Williams RJ, Martinez ND. Network Structure and Biodiversity Loss in Food Webs: Robustness Increases with Connectance. *Ecol Lett* (2002) 5:558–67. doi:10.1046/j.1461-0248.2002.00354.x
9. Pastor-Satorras R, Vespignani A. Immunization of Complex Networks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2002) 65:036104. doi:10.1103/PhysRevE.65.036104
10. Cohen R, Havlin S, Ben-Avraham D. Efficient Immunization Strategies for Computer Networks and Populations. *Phys Rev Lett* (2003) 91:247901. doi:10.1103/physrevlett.91.247901
11. Newman ME. Spread of Epidemic Disease on Networks. *Phys Rev E Stat Nonlin Soft Matter Phys* (2002) 66:016128. doi:10.1103/PhysRevE.66.016128
12. Boss M, Elsinger H, Summer M, Thurner S. Network Topology of the Interbank Market. *Quantitative finance* (2004) 4:677–84. doi:10.1080/14697680400020325
13. Gai P, Kapadia S. Contagion in Financial Networks. *Proc R Soc A* (2010) 466:2401–23. doi:10.1098/rspa.2009.0410
14. Haldane AG, May RM. Systemic Risk in Banking Ecosystems. *Nature* (2011) 469:351–5. doi:10.1038/nature09659
15. Shao C, Ciampaglia GL, Varol O, Yang KC, Flammini A, Menczer F. The Spread of Low-Credibility Content by Social Bots. *Nat Commun* (2018) 9:4787–9. doi:10.1038/s41467-018-06930-7
16. Newman MEJ. Assortative Mixing in Networks. *Phys Rev Lett* (2002) 89:208701. doi:10.1103/PhysRevLett.89.208701
17. Vázquez A, Moreno Y. Resilience to Damage of Graphs with Degree Correlations. *Phys Rev E* (2003) 67:015101. doi:10.1103/PhysRevE.67.015101
18. Berchenko Y, Artzy-Randrup Y, Teicher M, Stone L. Emergence and Size of the Giant Component in Clustered Random Graphs with a Given Degree Distribution. *Phys Rev Lett* (2009) 102:138701. doi:10.1103/PhysRevLett.102.138701
19. Newman MEJ. Random Graphs with Clustering. *Phys Rev Lett* (2009) 103:058701. doi:10.1103/PhysRevLett.103.058701
20. Priester C, Schmitt S, Peixoto TP. Limits and Trade-Offs of Topological Network Robustness. *PLoS ONE* (2014) 9:e108215. doi:10.1371/journal.pone.0108215
21. Motter AE, Lai Y-C. Cascade-based Attacks on Complex Networks. *Phys Rev E* (2002) 66:065102. doi:10.1103/PhysRevE.66.065102
22. Watts DJ. A Simple Model of Global Cascades on Random Networks. *Proc Natl Acad Sci U.S.A* (2002) 99:5766–71. doi:10.1073/pnas.082090499
23. Baxter GJ, Dorogovtsev SN, Goltsev AV, Mendes JFF. Bootstrap Percolation on Complex Networks. *Phys Rev E* (2010) 82:011103. doi:10.1103/PhysRevE.82.011103

24. Leicht EA, D'Souza RM. Percolation on Interacting Networks. *ArXiv: 0907.0894* (2009).
25. Bianconi G, Ziff RM. Topological Percolation on Hyperbolic Simplicial Complexes. *Phys Rev E* (2018) 98:052308. doi:10.1103/PhysRevE.98.052308
26. Artime O, De Domenico M. Percolation on Feature-Enriched Interconnected Systems. *Nat Commun* (2021) 12:2478. doi:10.1038/s41467-021-22721-z
27. Newman MEJ. The Structure and Function of Complex Networks. *SIAM Rev* (2003) 45:167–256. doi:10.1137/S003614450342480
28. Callaway DS, Newman MEJ, Strogatz SH, Watts DJ. Network Robustness and Fragility: Percolation on Random Graphs. *Phys Rev Lett* (2000) 85:5468–71. doi:10.1103/physrevlett.85.5468
29. Cohen R, Havlin S. *Complex Networks: Structure, Robustness and Function*. Cambridge, UK: Cambridge University Press (2010).
30. Newman M. *Networks*. Oxford, UK: Oxford University Press (2018).
31. Latora V, Nicosia V, Russo G. *Complex Networks*. Cambridge: Cambridge University Press (2017).
32. Wilf HS. *Generatingfunctionology*. Boca Raton, FL, USA: CRC Press (2005).
33. Erdös P. Graph Theory and Probability. *Can J Maths* (1959) 11:34–8.
34. Erdos P, Rényi A. On the Evolution of Random Graphs. *Publ Math Inst Hung Acad Sci* (1960) 5:17–60. doi:10.1515/9781400841356.38
35. Erdős P, Rényi A. On the Strength of Connectedness of a Random Graph. *Acta Mathematica Hungarica* (1961) 12:261–7.
36. Molloy M, Reed B. A Critical point for Random Graphs with a Given Degree Sequence. *Random Struct Alg* (1995) 6:161–80. doi:10.1002/rsa.3240060204
37. Newman MEJ, Watts DJ, Strogatz SH. Random Graph Models of Social Networks. *Proc Natl Acad Sci U.S.A* (2002) 99:2566–72. doi:10.1073/pnas.012582999
38. Newman M. *Networks: An Introduction*. Oxford: Oxford University Press (2010).
39. Peixoto TP, Bornholdt S. Evolution of Robust Network Topologies: Emergence of central Backbones. *Phys Rev Lett* (2012) 109:118703. doi:10.1103/PhysRevLett.109.118703

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Advantages of publishing in Frontiers

OPEN ACCESS
Articles are free to read for greatest visibility and readership

FAST PUBLICATION
Around 90 days from submission to decision

HIGH QUALITY PEER-REVIEW
Rigorous, collaborative, and constructive peer-review

TRANSPARENT PEER-REVIEW
Editors and reviewers acknowledged by name on published articles

Frontiers
Avenue du Tribunal-Fédéral 34
1005 Lausanne | Switzerland

Visit us: www.frontiersin.org
Contact us: frontiersin.org/about/contact

REPRODUCIBILITY OF RESEARCH
Support open data and methods to enhance research reproducibility

DIGITAL PUBLISHING
Articles designed for optimal readership across devices

FOLLOW US
@frontiersin

IMPACT METRICS
Advanced article metrics track visibility across digital media

EXTENSIVE PROMOTION
Marketing and promotion of impactful research

LOOP RESEARCH NETWORK
Our network increases your article's readership