



Research Article

Methods to Measure the Network Path Connectivity

Yinwei Li ¹, Guo-Ping Jiang,^{2,3} Meng Wu,⁴ and Yurong Song ^{2,3}

¹School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

²School of Automation, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

³Jiangsu Engineering Lab for IOT Intelligent Robots (IOTRobot), Nanjing 210023, China

⁴School of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

Correspondence should be addressed to Yurong Song; songyr@njupt.edu.cn

Received 6 August 2020; Revised 29 September 2020; Accepted 28 October 2020; Published 11 November 2020

Academic Editor: Qingyi Zhu

Copyright © 2020 Yinwei Li et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The functionalities, such as connectivity and communication capability of complex networks, are related to the number and length of paths between node pairs in the networks. In this paper, we propose a new path connectivity measure by considering the number and length of paths of the network (*PCNL*) to evaluate network path connectivity. By comparing the *PCNL* with the typical natural connectivity, we prove the effectiveness of the *PCNL* to measure the path connectivity of networks. Because of the importance of the shortest paths, we further propose the shortest paths connectivity measure (*SPCNL*) based on the number and length of the shortest paths. Then, we use edge-betweenness-based malicious attacks to study the relationship between the *SPCNL* and network topology in five types of networks. The results show that the *SPCNLs* of the networks have a significant corresponding relationship and similar changing trend with their network topology heterogeneities with the increase of the number of deleted edges. These findings mean that the *SPCNL* is positively correlated with the heterogeneity of the network topology, which provides a new perspective for designing complex networks with high path connectivity.

1. Introduction

Complex networks such as power grids, transportation networks, and telecommunication networks provide the flow of current, products, and information essential to develop the economy and protect social security. Vast information collected from the wireless sensor networks has brought great convenience to the production and life of human society [1, 2]. Therefore, it is important to ensure that such networks continue to function properly for the normal operation of society. However, more and more attacks on and failures of complex networks have caused huge losses to people's production and lives. As some rare occurrences in the past have shown, complex networks are still vulnerable to diverse attacks [3–6]. To prevent these losses, it is necessary to design robust networks to combat these malicious attacks.

The node connectivity of a network is an important property concerning the ability of the network to maintain its functionality after being attacked by the removal of nodes

or edges from the network [7, 8]. Albert et al. [9] studied the changes of the maximal connected component (*MCC*), i.e., the size of the largest connected subgraph in the remaining network, after a small fraction of the nodes are removed from an exponential network and scale-free network under random attacks and targeted attacks, respectively. They found that scale-free networks display surprising connectivity against random attacks but are extremely vulnerable to targeted attacks, while the exponential networks do not exhibit this property. Schneider et al. [10] introduced a new connectivity measure and used it to devise a method to reconstruct networks against malicious attacks. Their results showed that networks with an “onion-like” structure have significantly high robustness against malicious targeted attacks. Louzada et al. [11] proposed a new measure based on communication efficiency and outlined a procedure to modify any given network to enhance its connectivity via an optimization approach using simulated annealing. Their results showed that high assortativity and the onion-like

structure are the characteristics of networks with high node connectivity. Zeng and Liu [12] proposed a link-robustness index to measure the node connectivity of a network by different malicious attack strategies.

The above robustness measures are mainly considered from the view of node connectivity. In fact, the number of paths in the network is also a very important connectivity index. Path diversification in networks is an important mechanism that can be used to select multiple paths between a given node pair to achieve maximum flow robustness. Multipath routing is one way of improving the robustness of the transmitted information [13, 14]. Multi-path selection, control, and other related algorithms have been widely studied against various malicious attacks [15–17]. Therefore, networks with a large number of paths can provide a solid physical path foundation for these algorithms. Furthermore, the shortest paths, where the length of the shortest path is the smallest of all paths between two nodes, are the most efficient for the transmission of flow, for example, electrical current, transportation, and communication packets in complex networks from a source node to a termination node. Therefore, the number of shortest paths is also an important topological index for the functionality of a network. Many classical routing algorithms and robustness measures are designed for networks according to the shortest paths [6, 18–24].

For a source node and a termination node, there may be several paths between them. When one path is broken, the two nodes can still be connected through other alternative paths. Therefore, the greater the number of paths is, the higher the path connectivity between the two nodes is. With the same number of paths, the shorter the path length, the higher the network efficiency. Therefore, we propose a new measure (*PCNL*) in this paper to evaluate the network path connectivity by considering the number and length of the paths. The shortest paths between two nodes are of particular importance for a network to provide the fastest and strongest interaction. We also propose the shortest path connectivity (*SPCNL*) by only considering the number and length of the shortest paths simultaneously. We study the *SPCNL* of *BA* networks and *ER* networks for four groups with different network sizes, where each group has the same average degree. We find that the *BA* networks have the higher *SPCNL*. Furthermore, we use Monte Carlo simulations to analyze the path connectivity of the above networks and three other types of networks, which are generated from the *BA* networks by edge rewiring algorithm, against edge-betweenness-based malicious attacks. The results demonstrate that the *SPCNL* is positively correlated with the heterogeneity of the network topology.

The rest of the paper is arranged as follows. Section 2 summarizes the related work. In Section 3, we show the effect of the number and length of the paths on the path connectivity and propose the new network path connectivity measure. In Section 4, we study the *SPCNL* of *BA* networks and *ER* networks for four groups with different network sizes. In Section 5, we study the *SPCNL* of *BA* networks, *ER* networks, and three types of networks against edge-betweenness-based malicious attack. We finally give some conclusions in Section 6.

2. Related Work

For any two nodes in a connected network, there may be several paths between them. Therefore, the number of the paths has a great impact on the measurement of network connectivity. Oyama and Morohosi [22] proposed a quantitative method for evaluating the stable connectivity of the network-structured system by shortest-path-counting methods. Morohosi [23] proposed a connectivity measure based on the shortest path length distribution and used Monte Carlo methods for the computation of the measure to find the robustness properties of networks. Kobayashi et al. [24] proposed a quantitative robustness measure of a network. They defined the connectivity function and estimated expected edge deletion and node deletion connectivity functions when an arbitrary number of edges or nodes are deleted from the original network by the Monte Carlo method. The above studies set the number of the shortest path between two nodes as one and ignored the fact that there may be multiple shortest paths between two nodes. In reality, the number and length of the shortest paths will have a great impact on the measurement of network connectivity (Section 3).

If the source and destination of a path are the same nodes, the path is called as closed path. The number of closed paths is an important index for complex networks. Wu et al. [25] proposed a connectivity measure by considering the number and length of the closed paths simultaneously. The connectivity measure was defined as follows:

$$S = \sum_{l=0}^{\infty} \frac{n_l}{l!} = \sum_{i=1}^N \sum_{l=0}^{\infty} \frac{\lambda_i^l}{l!} = \sum_{i=1}^N e^{\lambda_i}, \quad (1)$$

where n_l is the number of closed paths with length l and λ_i is the eigenvalue of the adjacency matrix for a network. The authors scaled equation (1) and denoted it by

$$\bar{\lambda} = \ln \left(\frac{1}{N} \sum_{i=1}^N e^{\lambda_i} \right), \quad (2)$$

where N is the number of nodes in a network. They call equation (2) the natural connectivity (Na_C). The authors considered the influence of the number and length of closed paths on the connectivity measure simultaneously. However, the traffic or information in a network is mainly transmitted between two different nodes, not the node itself. Therefore, the number of closed paths from node to node itself may not accurately reflect the path connectivity of the networks. Moreover, to obtain this measure in the form of a graph spectrum, the authors scale the contribution of closed walks by the factorial of the closed path length. The factor of the factorial of the closed path length will lead to inaccurate measurement of network connectivity. In Section 3, we will give an example to demonstrate this problem.

3. Path Connectivity Measure

Given an undirected simple graph $G = (V, E)$, V is the set of nodes and E is the set of edges. A path is a sequence of vertices $P = v_1, v_2, \dots, v_k$, where $v_i \in V$, $i = 1, 2, \dots, k$. P is also

called a path from v_1 to v_k . The length of a path is defined as the number of edges it contains. Therefore, the length of path P is $k - 1$. The distance between two nodes is defined as the length of the shortest path between the two nodes. The maximum distance between any two nodes in a network is called the diameter (D) of the network. The average path length (Avg_L) of a network is defined as the average distance between any two nodes. Path connectivity refers to the ability of a network to make the paths with the same length connected under disturbances caused by paths change. An intuitive notion of path connectivity can be interpreted as the redundancy of paths between nodes. The greater the number of paths is, the less the risk of disconnection is when the paths between nodes are broken by the removal of edges.

Figure 1 shows the three path scenarios between node i and node j , and the length of all paths is l . Figure 1(a) shows that there is only one path between node i and node j , but Figures 1(b) and 1(c) show that there are n paths between node i and node j . Letting the probability that an edge is removed be p , one can obtain the probabilities that the paths with length l between node i and node j are disconnected for the three path scenarios in Figure 1 as follows:

$$\begin{cases} 1 - (1 - p)^l, & \text{for Figure 1 (a),} \\ 1 - (1 - p)^{l-2} \left(1 - (1 - (1 - p)^2)^n\right), & \text{for Figure 1 (b),} \\ (1 - (1 - p)^l)^n, & \text{for Figure 1 (c),} \end{cases} \quad (3)$$

where $l > 2$. When $l = 2$, it is noted that Figures 1(b) and 1(c) become the same scenarios. From equation (3), one can deduce the probability q that all paths with length l and number n between node i and node j are disconnected belongs to the following range:

$$q \in \left[1 - (1 - p)^{l-2} \left(1 - (1 - (1 - p)^2)^n\right), (1 - (1 - p)^l)^n\right], \quad l > 2. \quad (4)$$

Note that q decreases with the increase of n or the decrease of l . One can intuitively understand that the more alternative and disjoint paths there are, the stronger the connectivity and the function of communication or transmission between the two nodes are. Therefore, one can consider the number of paths as a measure for the path connectivity of the networks. For simplicity, we do not distinguish the two scenarios of Figures 1(b) and 1(c) in this paper. Considering the influence of path length on network path connectivity, we propose a path connectivity measure between a pair of nodes based on the number and length of the paths in a connected network as follows:

$$R_p^{ij} = \sum_{l=|p_{ij}|}^{L_{ij}} \frac{n_l^{ij}}{l}, \quad i \neq j, \quad (5)$$

where L_{ij} is the length setting for the paths between node i and node j , $|p_{ij}|$ is the length of the shortest paths, and n_l^{ij} is the number of paths with length l . R_p^{ij} represents the path connectivity ability between node i and node j . The greater

the R_p^{ij} is, the stronger the robustness of connectivity and the function of communication between node i and node j are. It is noted that different settings of L_{ij} will produce different R_p^{ij} . One can set L_{ij} according to the actual situation of the networks, for example, the restriction distance in network transmission and the diameter D limitation of a network. For a connected network, it has $N(N - 1)/2$ node pairs. One can obtain the mean value of the R_p^{ij} of all node pairs as follows:

$$S_p = \frac{2}{N(N - 1)} \sum_{(i \neq j) \in V} R_p^{ij}. \quad (6)$$

We call S_p the path connectivity based on the number and length of paths ($PCNL$). One can use S_p to measure the path connectivity of a network. S_p can change monotonically as edges are added or deleted. To prove this, given a network G^0 , let G^1 be the network after adding an edge between node i and node j . Let $R_p^{ij}(0)$ be the path connectivity of G^0 and $R_p^{ij}(1)$ be the path connectivity of G^1 between node i and node j . $S_p(0)$ and $S_p(1)$ are the $PCNL$ s of G^0 and G^1 , respectively. For the same $L_{ij} = K$, one can obtain $R_p^{ij}(0)$ and $R_p^{ij}(1)$ from equation (5) as follows:

$$\begin{aligned} R_p^{ij}(0) &= \sum_{l=|p_{ij}(0)|}^{L_{ij}=K} \frac{n_l^{ij}(0)}{l}, \quad i \neq j, \\ R_p^{ij}(1) &= \sum_{l=1}^{|p_{ij}(0)|-1} \frac{n_l^{ij}(1)}{l} + \sum_{l=|p_{ij}(0)|}^{L_{ij}=K} \frac{n_l^{ij}(1)}{l}, \quad i \neq j, \end{aligned} \quad (7)$$

where $|p_{ij}(0)|$ is the length of the shortest path between node i and node j in G^0 . For the same l , $n_l^{ij}(1) \geq n_l^{ij}(0)$. Therefore, one can obtain $R_p^{ij}(1) > R_p^{ij}(0)$. For any other node pair (m, n) , one can deduce that

$$\begin{aligned} R_p^{mn}(1) &\geq R_p^{mn}(0), \quad (m, n) \neq (i, j), \\ S_p(1) &= R_p^{ij}(1) + \sum_{m,n} R_p^{mn}(1), \quad (m, n) \neq (i, j), \\ S_p(0) &= R_p^{ij}(0) + \sum_{m,n} R_p^{mn}(0), \quad (m, n) \neq (i, j). \end{aligned} \quad (8)$$

Thus, $S_p(1) > S_p(0)$.

Figure 2 shows two networks with the same degree distribution. Table 1 shows the characteristic parameters of the two networks, where Tri_num denotes the number of triangles in a network, r denotes the correlation coefficient, D denotes the diameter, and Avg_L denotes the average shortest path length. We denote P_num as the sum of the number of the shortest paths and denote Na_C as the natural connectivity. We obtain the $PCNL$ s of the two networks by setting $L_{ij} = 6$. For *network A*, if we remove node 1 or 2, *network A* will become disconnected. If we remove the edge between node 1 and node 2, the paths in *network A* will change dramatically. For example, D of *network A* increased dramatically from 4 to 7. For *network B*, the removal of any node cannot make it disconnected. In addition, it is intuitive that the removal of any edge will not change the paths of the

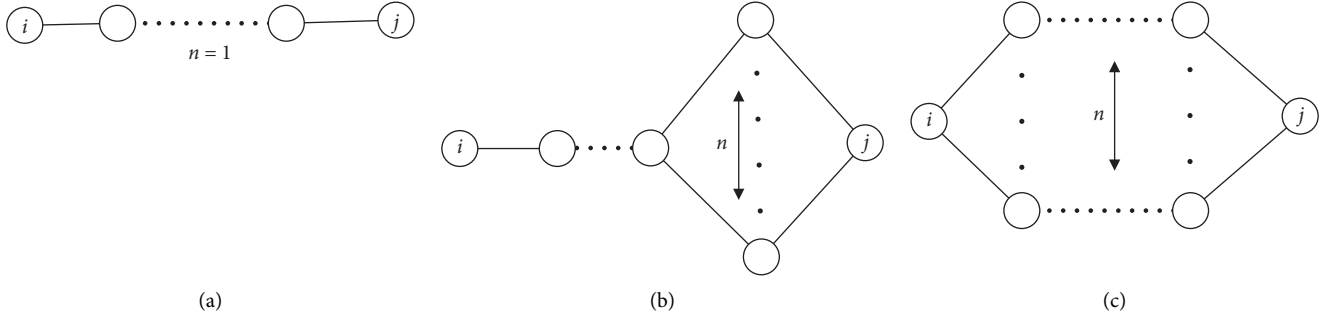
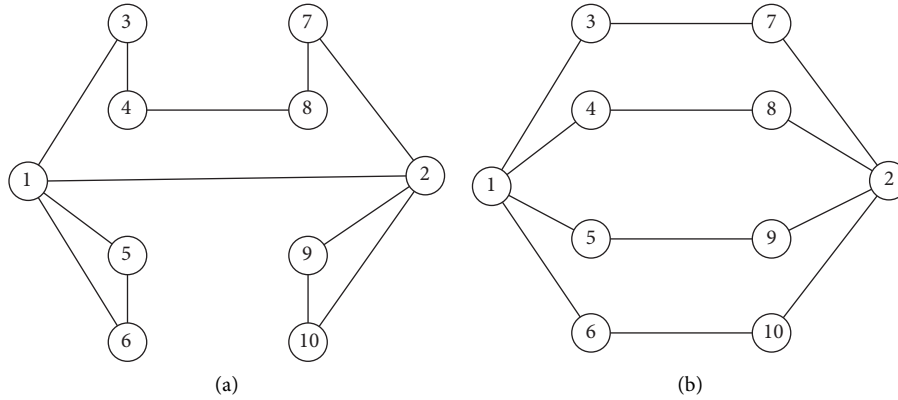
FIGURE 1: Three path scenarios between node i and node j .FIGURE 2: Two networks with the same degree distribution. (a) *Network A*. (b) *Network B*.

TABLE 1: Characteristic parameters for network A and network B.

	r	Tri_num	D	Avg_L	P_num	$PCNL$	Na_C
Network A	-0.1250	2	4	2.2444	52	1.0230	1.1062
Network B	-0.5000	0	3	2.0222	60	1.3407	1.0031

network significantly. Therefore, it is obvious that the node connectivity and path connectivity of *network B* are better than those of *network A*. However, according to Na_C , we draw the opposite conclusion (Table 1). This shows that Na_C has limitation in evaluating path connectivity of the network. From equation (1), one can find that a closed walk of length $l=2$ corresponds to an edge. Because the degree distributions of two networks are identical, the contribution of $l=2$ to their Na_C is the same for the two networks. For $l=2, 3, 4,$ and 5 in *network A*, one can obtain S from equation (1) as follows:

$$\begin{aligned}
 SA(3) &= \frac{12}{2!} = 6.000, \\
 SA(3) &= \frac{2}{3!} = 0.333, \\
 SA(4) &= \frac{13}{4!} = 0.541, \\
 SA(5) &= \frac{10}{5!} = 0.083.
 \end{aligned} \tag{9}$$

One can find that the factor of the factorial of the closed path length sharply reduces the contribution of path lengths greater than 2 to Na_C . The effect of path length on Na_C is amplified by the factorial. From equation (1), one can find that a closed walk of length $l=3$ represents a triangle. There are two triangles in *network A* and zero in *network B*. This may be because the Na_C of *network A* is larger than that of *network B*. Therefore, one can infer that Na_C has too strong a correlation with the short closed path lengths of the networks. This will lead to inaccurate measurement of path connectivity by Na_C . From Table 1, one can see that the $PCNL$ of *network B* is larger than that of *network A*. This shows the effectiveness of the $PCNL$ to measure the path connectivity of networks.

Next, we take the $PCNL$ ($L_{ij}=6$) as an objective function to optimize *network A* by the degree-preserving rewiring algorithm [26], which can keep the degree distribution of the network unchanged after rewiring the network. Figure 3 shows the process of network optimization by degree-preserving rewiring. One can find that *network B* can be obtained from *network A* with the optimization of the $PCNL$. However, one cannot obtain this optimization result through Na_C . This shows that the performance of the $PCNL$ for evaluating the path connectivity is better than that of Na_C .

For the $PCNL$, it is noted that the length setting $L_{ij}=K$ needs to be greater than the network diameter D ; otherwise, the path information of node pairs that their distance is greater than K will be neglected. From equation (3), one can find that

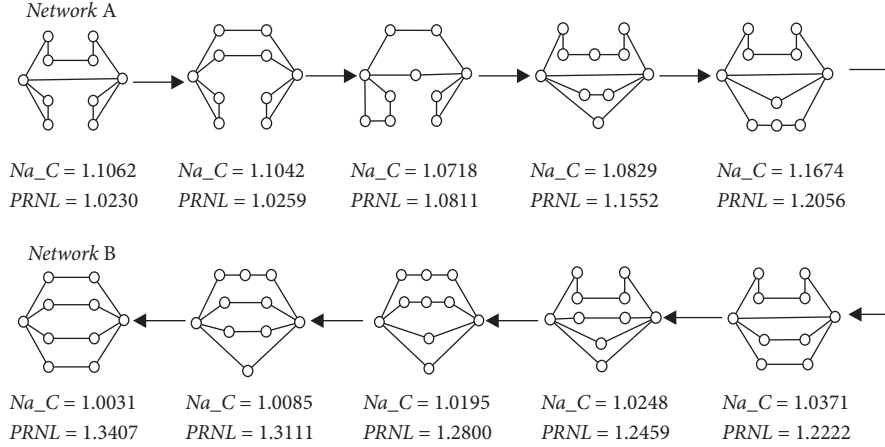


FIGURE 3: Process of network optimization by degree-preserving rewiring.

the complexity of the PCNL will increase with the increase of L_{ij} . Considering the influence of shortest paths on network functionality [6, 18–24] and the complexity of the PCNL, we set $L_{ij} = |p_{ij}|$ to calculate the shortest path connectivity of a network. Then, equations (5) and (6) are shown as follows:

$$R_{sp}^{ij} = \frac{n_l^{ij}}{l = |p_{ij}|}, \quad i \neq j, \quad (10)$$

$$S_{sp} = \frac{2}{N(N-1)} \sum_{(i \neq j) \in V} R_{sp}^{ij},$$

where $|p_{ij}|$ is the length of the shortest paths and n_l^{ij} is the number of paths with length l between node i and node j . R_{sp}^{ij} represents the shortest path connectivity ability between node i and node j . S_{sp} is the mean value of the R_{sp}^{ij} of all node pairs. We call S_{sp} the path connectivity based on the number and length of shortest paths (SPCNL). Note that S_{sp} may not change monotonically as edges are added or deleted. The reason is that, when one adds or deletes an edge in a network, the number of shortest paths in the network may decrease or increase. Therefore, it is possible to reduce or improve the SPCNL of a network by adding or deleting an edge. One can also find similar examples, and many researches studies have also obtained similar results [27]. For example, when drivers choose the shortest path independently, opening some new road sections may lead to overall traffic network congestion and capacity decline. Although the complexity of SPCNL is much lower than that of PCNL, it contains the shortest path information between all node pairs. According to equations (5) and (6), the contribution of the shortest path to PCNL is relatively larger than that of other paths. Therefore, we can use SPCNL to evaluate the path connectivity of a network.

4. Relationship between Path Connectivity and Network Topologies

Some natural questions arise: what is the relation between path connectivity and network topologies? How can we obtain a network with high path connectivity under a given

average degree or degree distribution? We will try to answer these questions in this section. We first generate *BA networks* (heterogeneous networks) [28] and *ER networks* (homogeneous networks) [29] with sizes of 1000, 2000, 3000, and 4000. For *BA networks* and *ER networks*, we generate ten networks of each size, respectively. All networks have the same average degree $\langle k \rangle \approx 6$. Figure 4 shows the average value of each of the ten networks for *BA networks* and *ER networks*, respectively. From Figure 4(a), one can see that the SPCNLs of the *BA networks* are the larger than those of *ER networks*. Figures 4(c) and 4(d) show that this is because the P_nums of *BA networks* are greater than those of *ER networks* and the Avg_Ls of *BA networks* are smaller than those of *ER networks*. From Figure 4(c), under the same average degree, one can see that the *BA networks* can generate the many shortest paths than *ER networks*. In Figure 4(b), one can see that Na_Cs of *BA networks* are far greater than those of *ER networks*. One can infer that the reason is that the Avg_Ls of *BA networks* are smaller than those of *ER networks* (Figure 4(d)). From Figures 4(b) and 4(d), one can obtain that the effect of path length on Na_C is amplified. By the results shown in Figure 4, one can answer the questions at the beginning of this section, namely, under the same average degree condition, the heterogeneous networks have the larger number of shortest paths and the stronger path connectivity than homogeneous networks.

To further confirm the above conclusion, we need more networks with the same average degree and different network topologies. We use random edge rewiring for one of the ten *BA networks* to obtain a new network. Then, taking the new *BA network* as the initial network, we use the degree-preserving rewiring algorithm to generate three network sets and denote them as *Ran networks* (uncorrelated network), *Dis networks* (disassortative network), and *Ass networks* (assortative network), respectively. There are ten networks in each network set. The networks in the same network set have the same degree distribution and degree correlation coefficient. Note that all of the networks in the three sets have the identical average degree as the *BA networks* and *ER networks*. The characteristic parameters of the network sets are shown in Table 2, where $\langle k^2 \rangle$ is the mean of the sum of the squares

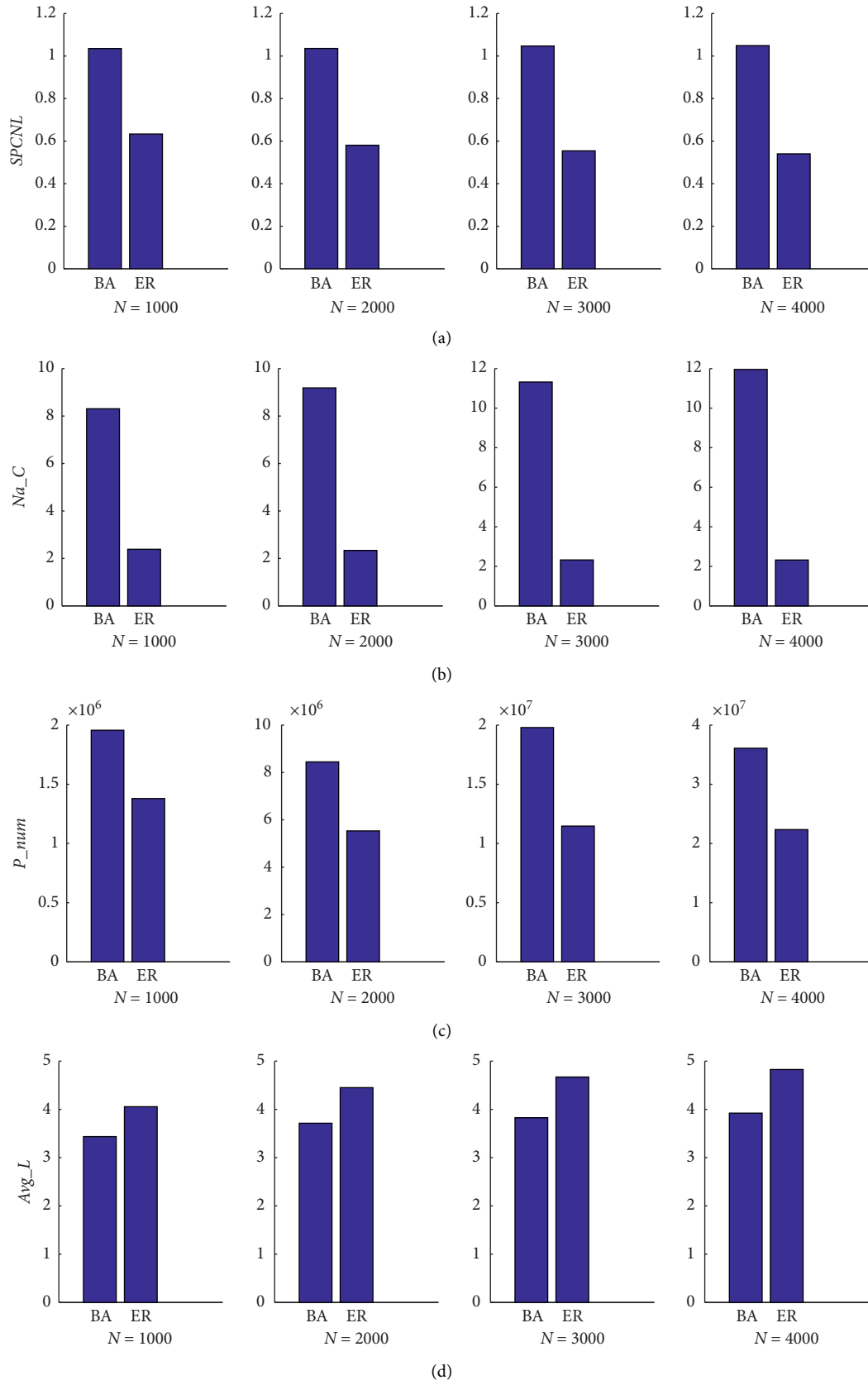
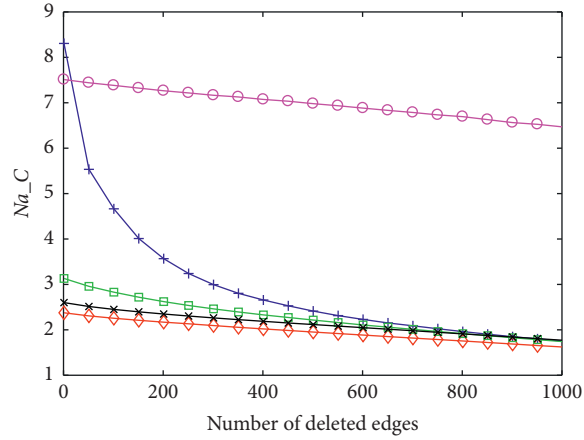


FIGURE 4: (a) The SPCNL of two types of networks, BA networks and ER networks. The average degree of all networks is 6. N is the number of nodes of the networks, 1000, 2000, 3000, and 4000, respectively. (b) The Na_C of two types of networks. (c) The P_num of two types of networks. (d) The Avg_L of two types of networks.

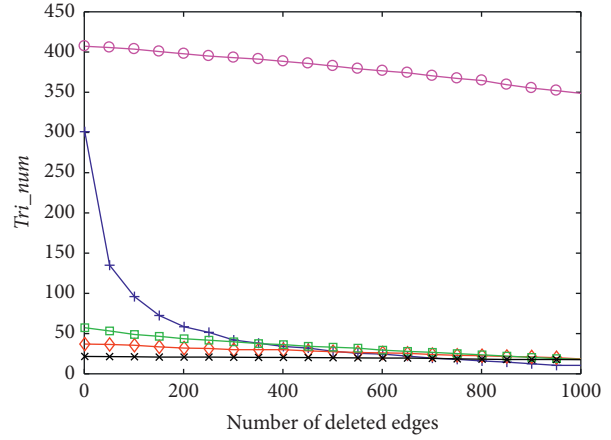
TABLE 2: Characteristic parameters for the five network sets.

	$\langle k \rangle$	$\langle k^2 \rangle$	r	Tri_num	D	Avg_L	P_num	$SPCNL$	Na_C
<i>Ran networks</i>	5.99	50.882	0.002	57.3	8	4.026	1772066	0.818	3.132
<i>Dis networks</i>	5.99	50.882	-0.560	21.6	6.4	3.917	1715478	0.787	2.600
<i>Ass networks</i>	5.99	50.882	0.600	407.2	8.7	4.284	1750788	0.777	7.510
<i>BA networks</i>	5.99	93.052	-0.076	301	6	3.437	1953483	1.034	8.306
<i>ER networks</i>	5.99	41.566	0.010	37	7	4.064	1374022	0.630	2.375



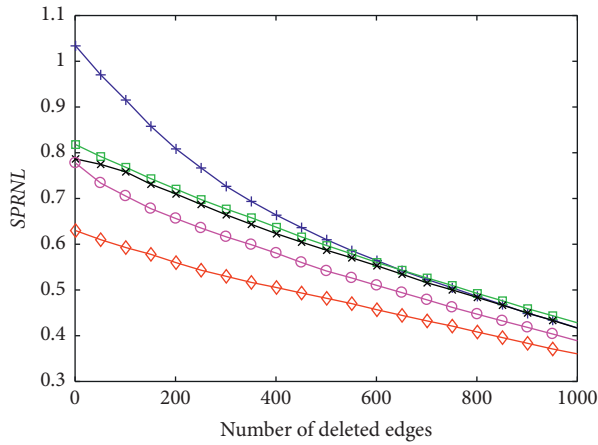
Legend for (a):
 BA networks (blue line with '+')
 Dis networks (black line with '*')
 ER networks (red line with 'o')
 Ass networks (magenta line with 'o')
 Ran networks (green line with 'x')

(a)



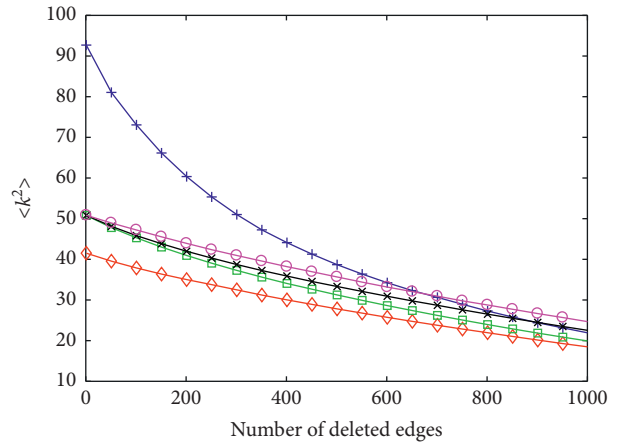
Legend for (b):
 BA networks (blue line with '+')
 Dis networks (black line with '*')
 ER networks (red line with 'o')
 Ass networks (magenta line with 'o')
 Ran networks (green line with 'x')

(b)



Legend for (c):
 BA networks (blue line with '+')
 Dis networks (black line with '*')
 ER networks (red line with 'o')
 Ass networks (magenta line with 'o')
 Ran networks (green line with 'x')

(c)



Legend for (d):
 BA networks (blue line with '+')
 Dis networks (black line with '*')
 ER networks (red line with 'o')
 Ass networks (magenta line with 'o')
 Ran networks (green line with 'x')

(d)

FIGURE 5: Continued.

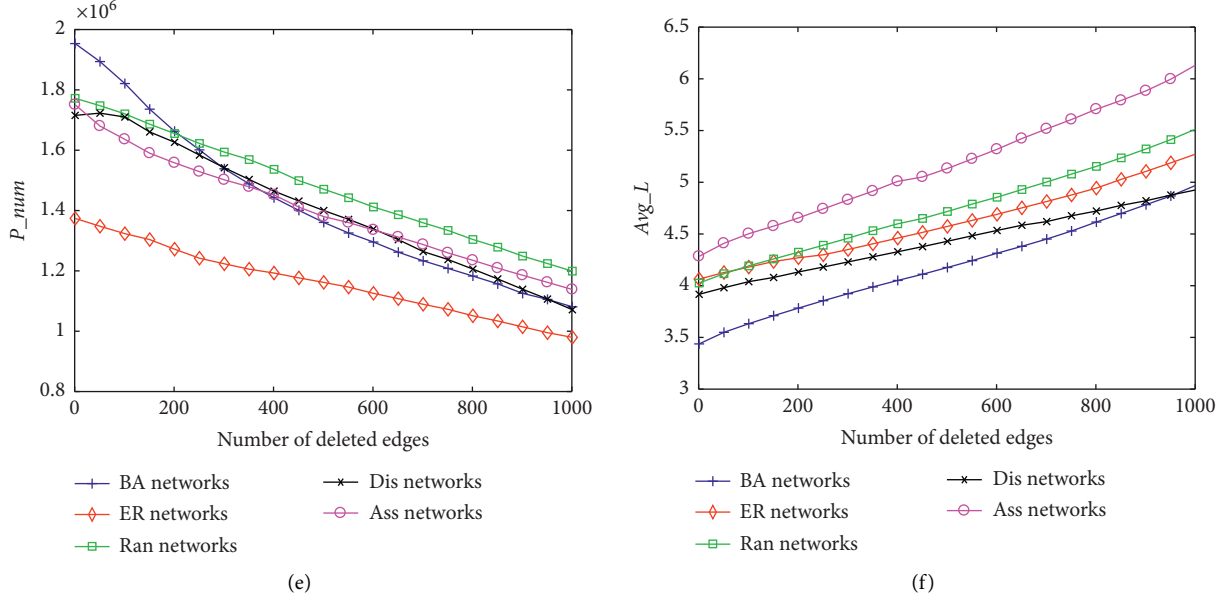


FIGURE 5: (a) Na_C is shown as a function of the number of deleted edges. (b) Tri_num is shown as a function of the number of deleted edges. (c) $SPCNL$ is shown as a function of the number of deleted edges. (d) $\langle k^2 \rangle$ is shown as a function of the number of deleted edges. (e) P_num is shown as a function of the number of deleted edges. (f) Avg_L is shown as a function of the number of deleted edges. When two nodes are disconnected, the number and length of the shortest paths between them are set to 0. Each data point is the average of the ten networks for *BA networks*, *ER networks*, *Ran networks*, *Dis networks*, and *Ass networks* under the edge betweenness-based malicious attack.

of the degrees. $\langle k^2 \rangle$ can represent the heterogeneity of a network topology. For *Ran networks*, *Dis networks*, *Ass networks*, *BA networks*, and *ER networks*, each characteristic parameter in Table 2 is the average value of the characteristic parameters of the corresponding ten networks.

In Table 2, one can see that the $\langle k^2 \rangle$ and P_num of the *BA network* are both larger than those of the other networks. This shows that the heterogeneity significantly increases the number of shortest paths in a network. One can also obtain that the $SPCNL$ of the *BA network* is larger than that of the other networks. This means that the shortest path connectivity and the function of communication of the *BA network* are better than those of the other networks. For *Ran networks*, *Dis networks*, and *Ass networks* with the identical $\langle k^2 \rangle$, they have almost the same $SPCNL$ s. Note that the $SPCNL$ of the *BA networks* with the largest $\langle k^2 \rangle$ is significantly larger than the $SPCNL$ of the *ER networks* with the smallest $\langle k^2 \rangle$. The order of $SPCNL$ is consistent with the order of $\langle k^2 \rangle$ among the *Ran networks*, *Dis networks*, *Ass networks*, *BA networks*, and *ER networks*. One can also see that the order of $SPCNL$ is inconsistent with the order of r among all the networks. These mean that the $SPCNL$ may be positively correlated with the heterogeneity of a network topology and independent of the degree correlation coefficient. One can see that the Tri_nums and NA_Cs of *Ass networks* and *BA networks* are far larger than those of the other networks, and this may suggest that NA_C is positively correlated with the Tri_nums in a network. This confirms the conclusion drawn in Section 2 that the Na_C has too strong a correlation with the short closed path lengths of the networks. Next, we will carry out edge-betweenness-based malicious attacks on these networks to further verify these conclusions in Section 5.

5. Simulations

In the actual situation, edges are more vulnerable than nodes in a network [30]. In particular, edges with high betweenness play an important role in the network path connectivity [31]. The larger the betweenness of an edge is, the greater the number of shortest paths between node pairs passing through the edge is. If the edges with high betweenness are attacked and removed from a network, the shortest paths of a network will change dramatically. To verify the above conclusion on the relation between network topology and path connectivity, we use edge-betweenness-based malicious attacks to study the $SPCNL$ and Na_C of the above five types of networks and draw some conclusions. The process edge-betweenness-based malicious attack is as follows: (1) the edge betweenness of each network is calculated; (2) the edge with the maximal betweenness is removed from the network. We repeat the process 1000 times to remove 1000 edges one by one for each network. Each data point is the average of the ten networks for *BA networks*, *ER networks*, *Ran networks*, *Dis networks*, and *Ass networks* under the edge betweenness-based malicious attack.

Figure 5(a) shows Na_C as a function of the number of deleted edges, and Figure 5(b) shows Tri_num as a function of the number of deleted edges. From Figures 5(a) and 5(b), one can see that Na_C showed a significantly corresponding relationship and similar changing trend with Tri_num . One can see that the relative changing laws of the Na_C of *Ass networks* are consistent with the changing laws of the Tri_num of *Ass networks* in that the curves both decrease slowly with the increase of the number of deleted edges. For *BA networks*, as Tri_num drops rapidly, Na_C also exhibits a

rapid decline. From Figures 5(a) and 5(b), we can obtain that NA_C is positively correlated with Tri_nums in a network. This validates the previous conclusion that the Na_C has an overly strong correlation with the short closed path lengths of the networks to limit the performance to evaluate the path connectivity.

For *Ran networks*, *Dis networks*, and *Ass networks* in Figures 5(d) and 5(e), the $\langle k^2 \rangle$ and P_num of the three types of networks have little difference with the increase of the number of deleted edges. One can also see that the $SPCNL$ of the three types of networks have little difference. Note that the $SPCNL$ of the *Ass networks* is slightly less than *Ran networks* and *Dis networks*. One can speculate the reason from the Figure 5(f) that the Avg_L of the *Ass networks* is still larger than *Ran networks* and *Dis networks* with the increase of the number of deleted edges. For *BA networks*, the $\langle k^2 \rangle$ decreases rapidly with the deletion of edges until it is close to that of the other networks. From Figure 5(c), one can see that the changing trend for the $SPCNL$ of *BA networks* is the same as that of the $\langle k^2 \rangle$. For *ER networks*, the $\langle k^2 \rangle$ is still smaller than those of the other networks in the Figure 5(d), and the same scenario for $SPCNL$ can be seen in the Figure 5(c). One can see that the $SPCNLs$ of all networks show an obviously corresponding relationship and similar changing trend with $\langle k^2 \rangle$ (see Figure 5(d)). In general, we can obtain that the $SPCNL$ is positively correlated with the heterogeneity of a network topology.

6. Conclusions

The number and length of the shortest paths are important topological indexes for the functionality of complex networks. The greater the number and the shorter the length of paths in a network, the better the path connectivity of the network is. Considering the number and length of the shortest paths, a new measure called the $PCNL$ has been proposed in this paper to assess network path connectivity. Compared with the classical natural connectivity Na_C , the effectiveness of the proposed measure has been verified. In view of the importance of the shortest paths, we further propose the $SPCNL$ based on the number and length of shortest paths. We have studied the $SPCNL$ for two types of networks, namely, the *BA networks* and *ER networks*. The results show that the *BA networks* have the larger number of shortest paths and the stronger path connectivity than *ER networks* with identical average degree. We have drawn the same conclusion with the two types of networks with different sizes. To explore the relationship between network topology and path connectivity, we have generated three types of networks with the same degree distribution but different degree correlations, namely, *Ran networks*, *Dis networks*, and *Ass networks* and carried out edge-betweenness-based malicious attacks on the above five types of networks to obtain various conclusions. In general, the results show that the NA_C is positively correlated with Tri_num and that the $SPCNL$ is positively correlated with the heterogeneity of a network topology, which provide a new perspective to design complex networks with high path connectivity.

As we all know, the measures based on finding network paths are extremely complex. If one uses these measures as an objective function to optimize the network, the computational complexity will grow larger with the increasing scale of a network. Under the same degree distribution (keep network heterogeneity unchanged), increasing the number of shortest paths and limiting path length simultaneously can effectively increase $SPCNL$. However, it is a challenge to achieve this goal by existing optimization methods. Therefore, seeking an appropriate algorithm is an important study for optimizing network by using these measures as an objective function in the future.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research has been supported by the National Natural Science Foundation of China (Grant nos. 61672298, 61873326, 61802155, and 61802201) and the Philosophy Social Science Research Key Project Fund of Jiangsu University (Grant no. 2018SJZDI142).

References

- [1] X. Liu, P. Lin, T. Liu, T. Wang, A. Liu, and W. Xu, "Objective-variable tour planning for mobile data collection in partitioned sensor networks," *IEEE Transactions on Mobile Computing*, 2020.
- [2] T. Li, A. Liu, N. N. Xiong, S. Zhang, and T. Wang, "A trustworthiness-based vehicular recruitment scheme for information collections in distributed networked systems," *Information Sciences*, vol. 545, pp. 65–81, 2021.
- [3] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Physical Review E*, vol. 69, no. 2, 2004.
- [4] K. H. Thompson and H. T. Tran, "Operational perspectives into the resilience of the U.S. Air transportation network against intelligent attacks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 4, pp. 1503–1513, 2020.
- [5] W. Liu and Z. Y. Song, "Review of studies on the resilience of urban critical infrastructure networks," *Reliability Engineering & System Safety*, vol. 193, 2020.
- [6] R. Faturechi and E. Miller-Hooks, "Measuring the performance of transportation infrastructure systems in disasters: a comprehensive review," *Journal of Infrastructure Systems*, vol. 21, no. 1, 2015.
- [7] J. Liu, M. Zhou, S. Wang, and P. Liu, "A comparative study of network robustness measures," *Frontiers of Computer Science*, vol. 11, no. 4, pp. 568–584, 2017.
- [8] J. Wu, S. Y. Tan, Z. Liu, Y. J. Tan, and X. Lu, "Enhancing structural robustness of scale-free networks by information disturbance," *Scientific Reports*, vol. 7, 2017.
- [9] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

- [10] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proceedings of the National Academy of Sciences*, vol. 108, no. 10, pp. 3838–3841, 2011.
- [11] V. H. P. Louzada, F. Daolio, H. J. Herrmann, and M. Tomassini, "Generating robust and efficient networks under targeted attacks," <https://arxiv.org/abs/1207.1291>.
- [12] A. Zeng and W. P. Liu, "Enhancing network robustness against malicious attacks," *Physical Review E*, vol. 85, no. 6, 2012.
- [13] J. P. Rohrer, A. Jabbar, and J. P. G. Sterbenz, "Path diversification for future internet end-to-end resilience and survivability," *Telecommunication Systems*, vol. 56, no. 1, pp. 49–67, 2014.
- [14] Z. Q. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "A framework for reliable routing in mobile ad hoc networks," in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies, SFO*, pp. 270–280, San Francisco, CA, USA, March 2003.
- [15] P. Key, L. Massoulié, and D. Towsley, "Path selection and multipath congestion control," *Communications of the ACM*, vol. 54, no. 1, pp. 109–116, 2011.
- [16] K. A. M. Al-Soufy and A. M. Abbas, "A path robustness-based quality of service routing for mobile ad hoc networks," in *Proceedings of 2010 IEEE 4th International Conference on Internet Multimedia Services Architecture and Application*, Bangalore, India, December 2010.
- [17] M. Schafer, J. Scholz, and M. Greiner, "Proactive robustness control of heterogeneously loaded networks," *Physical Review Letters*, vol. 96, no. 10, 2006.
- [18] A. Rego, S. Sendra, J. M. Jimenez, and J. Lloret, "Dynamic metric OSPF-based routing protocol for software defined networks," *Cluster Computing-The Journal of Networks Software Tools and Applications*, vol. 22, no. 3, pp. 705–720, 2019.
- [19] E. Katzav, M. Nitzan, D. ben-Avraham et al., "Analytical results for the distribution of shortest path lengths in random networks," *EPL*, vol. 111, no. 2, 2015.
- [20] P. Narvaez, K. Y. Kai-Yeung Siu, and H. Y. Hong-Yi Tzeng, "New dynamic algorithms for shortest path tree computation," *IEEE/ACM Transactions on Networking*, vol. 8, no. 6, pp. 734–746, 2000.
- [21] R. Meredith, N. Landsberg, A. Lopez, and R. Dutta, "Recovering an OSPF network from malicious attacks: an experimental evaluation of recovery techniques," in *Proceedings of 2018 IEEE Global Communications Conference*, IEEE, Abu Dhabi, UAE, December 2018.
- [22] T. Oyama and H. Morohosi, "Applying the shortest-path-counting problem to evaluate the importance of city road segments and the connectedness of the network-structured system," *International Transactions in Operational Research*, vol. 11, no. 5, pp. 555–573, 2004.
- [23] H. Morohosi, "Measuring the network robustness by Monte Carlo estimation of shortest path length distribution," *Mathematics and Computers in Simulation*, vol. 81, no. 3, pp. 551–559, 2010.
- [24] K. Kobayashi, H. Morohosi, and T. Oyama, "Applying path-counting methods for measuring the robustness of the network-structured system," *International Transactions in Operational Research*, vol. 16, no. 3, pp. 371–389, 2009.
- [25] J. Wu, M. Barahona, Y. J. Tan, and H. Z. Deng, "Natural connectivity of complex networks," *Chinese Physics Letters*, vol. 27, no. 7, 2010.
- [26] P. Van Mieghem, H. Wang, X. Ge, S. Tang, and F. A. Kuipers, "Influence of assortativity and degree-preserving rewiring on the spectra of networks," *The European Physical Journal B*, vol. 76, no. 4, pp. 643–652, 2010.
- [27] Y. Li, J. Wu, and A. Q. Zou, "Effect of eliminating edges on robustness of scale-free networks under intentional attack," *Chinese Physics Letters*, vol. 27, no. 6, 2010.
- [28] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.
- [29] P. Erdős and A. Rényi, "On the evolution of random graphs," *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, vol. 5, pp. 17–60, 1960.
- [30] S. He, S. Li, and H. Ma, "Effect of edge removal on topological and functional robustness of complex networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 388, no. 11, pp. 2243–2253, 2009.
- [31] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Physical Review E*, vol. 65, no. 5, 2002.