Hindawi
Complexity
Volume 2020, Article ID 6695026, 10 pages
https://doi.org/10.1155/2020/6695026

Research Article

Controllability and Optimization of Complex Networks Based on Bridges

Lifu Wang, Guotao Zhao, Zhi Kong, and Yunkang Zhao

School of Control Engineering, Northeastern University at Qinhuangdao, Qinhuangdao 066004, China

Correspondence should be addressed to Zhi Kong; kongzhi2004916@163.com

Received 21 October 2020; Revised 27 November 2020; Accepted 30 November 2020; Published 9 December 2020

Academic Editor: Hocine Cherifi

In a complex network, each edge has different functions on controllability of the whole network. A network may be out of control due to failure or attack of some specific edges. Bridges are a kind of key edges whose removal will disconnect a network and increase connected components. Here, we investigate the effects of removing bridges on controllability of network. Various strategies, including random deletion of edges, deletion based on betweenness centrality, and deletion based on degree of source or target nodes, are used to compare with the effect of removing bridges. It is found that the removing bridges strategy is more efficient on reducing controllability than the other strategies of removing edges for ER networks and scale-free networks. In addition, we also found the controllability robustness under edge attack is related to the average degree of complex networks. Therefore, we propose two optimization strategies based on bridges to improve the controllability robustness of complex networks against attacks. The effectiveness of the proposed strategies is demonstrated by simulation results of some model networks. These results are helpful for people to understand and control spreading processes of epidemic across different paths.

1. Introduction

Many natural and manmade systems can be modeled as complex networks which consist of nodes and edges. For example, electric power networks can be regarded as complex networks formed by a large number of substations connected by transmission lines; citation networks can be regarded as complex networks composed by a large number of scholars contact through mutual citation of articles; in addition, biochemical networks, food webs, social networks, etc. all exist in form of complex networks. The basic research of complex networks is to understand the static structure and dynamic characteristics of networks [1], such as the construction of networks, the topological characteristics of networks, the community structure [2], and synchronization of networks [3, 4]. Extensive research on complex networks has enriched our understanding of real-world networks. The ultimate goal of research on complex networks is to control them, that is to say, how to control the entire network by controlling appropriate nodes. Classical Control Theory has been well applied to complex networks. Liu et al. [5] proposed a framework for computing the controllability of complex networks, which is named "structure controllability." The maximum matching of directed graphs [6] is used to find the minimal driver nodes to control the whole directed networks. Yuan et al. [7] proposed another controllability calculation framework called "exact controllability," which is applicable to complex networks of arbitrary structures. And the framework solves the problem that structure controllability is only applicable to directed networks.

With further studies of complex networks, the works on invulnerability of networks have become increasingly important [8]. Complex network failures caused by attacking or corrupting certain edges and nodes would lead networks out of control. For instance, failure of a station or a road may cause large-scale traffic congestion. Failure web sites or lines of the World Wide Web (www) may lead to Internet collapse. Cascading failures in a power grid could be triggered by the failure of a few transmission lines or substations [9], which eventually affect large portions of a grid. Chen et al. [10] studied the impact on controllability when nodes of

networks were attacked. Kashyap and Ambika [11] explored the change of controllability after edge with the highest betweenness breakdown. Pu and Cui [12] discussed the case where the longest simple path in networks was attacked. Their research studies demonstrate that random failures have little effect on controllability, while attacking nodes based on degree, attacking edges based on betweenness, and attacking the longest simple paths are intensely effective on controllability [13]. Thomas et al. [14] found that controlling a scale-free network is significantly more difficult than that of a random network. Quite a few nodes fail can also undermine the control of scale-free networks. Furthermore, Chen et al. [15] investigated the cascading failure and the controllability of complex networks under random failures and malicious attacks. In addition, the research studies on robustness of interdependent networks have gradually attracted scholars' attention [16]. The nodes in the dependent network interact with another layer of network, so the related properties are different from single layer networks.

Moreover, how to optimize complex networks to improve the invulnerability has also made great progress. Hou et al. [17] proposed a method to optimize controllability of directed networks by changing the direction of a small number of edges while keeping the total number of connected edges constant. Xiao et al. [18] proposed a dynamic optimization method to improve the robustness of arbitrary structural networks against target attacks, and the method only exchanges edges but does not change the nodes' degree. Li and Lu [19] proposed an optimization method based on genetic algorithm, which is applicable to any structural network. Iudice et al. [20] takes into account the physical and economic constraints in practical applications and converts the optimization problem into an integer linear programming problem. Zhang and Liu et al. [21, 22] proposed optimization methods through redundant design to improve invulnerability. Yan et al. [23] applied congruence theory to the construction of complex networks and revealed the characteristics and properties of multiple congruence networks. The study demonstrates that multiple congruence networks are more robust than typical complex networks. Lou et al. [24] proposed a new complex networks model with high robustness by using the feedback thought of control theory.

Bridges are a kind of key edges whose removal will disconnect a network and increase the number of connected graphs [25]. Bridges play an important role in ensuring the connectivity of networks, such as protein interaction networks, communication networks, and infrastructure networks. However, little attention has been paid to the importance of bridges on controllability of complex networks. Therefore, we investigated the effects of removing bridges on controllability of network. Then, we propose two optimization strategies based on bridges to improve controllability robustness of complex networks against attacks.

2. Controllability of Complex Networks

Consider a linear time-invariant dynamic network system with N nodes whose dynamic equation is expressed as

$$\dot{x}(t) = Ax(t) + Bu(t), \tag{1}$$

where $x(t) = (x_1(t), x_2(t), \ldots, x_N(t))^T$ is the state of nodes in complex network, $x_j(t)$ is the state of node j at time t; $A \in R^{N\times N}$ is the adjacency matrix of complex network, where $a_{ij} = 0$ means that there is no connection from node j to node i, that is, the node j does not affect node i, $a_{ij} \neq 0$ means the strength of node j affects node i, and the positive or negative of a_{ij} indicates whether the effect is positive or negative; $u(t) = (u_1(t), u_2(t), \ldots, u_M(t))^T$ is input signal, where $u_j(t)$ means the external input applied to node j; $B \in R^{N\times M}$ is input matrix, b_{ij} indicates the connection between input signal and node i.

The system described by equation (1) is controllable if it can be driven from any initial state $x(t_0)$ to any desired final state $x(t_f)$ within finite time $[t_0, t_f]$. According to Kalman rank condition, it is possible if and only if the controllability matrix

$$W = \left[B, AB, A^2B, \ldots, A^{N-1}B\right] \in R^{N\times NM} \tag{2}$$

has full rank, that is, rank $(W) = N$, where W is controllability matrix.

According to Kalman rank condition, for a given complex network, the adjacency matrix A is determined, and the way to make the network fully controllable is to find an appropriate input matrix B to satisfy Kalman rank condition. Obviously, if external inputs are applied to every node in the network, it must be fully controllable, but it is unrealistic for a complex network with thousands of nodes. The solution to controllability problem is to select nodes as little as possible to control networks, that is, to find a suitable matrix B which consists of minimum number of columns to satisfy Kalman rank condition. However, complex networks have thousands of nodes, and the computational complexity of Kalman rank condition is $2^N - 1$, which needs great amount of calculation. At the same time, the weight between nodes in the real world is largely unknown or uncertain. To overcome these difficulties, Liu et al. [5] introduced a framework called 'structural controllability' to solve the problem. Structural controllability framework integrates the matching theory of graph with traditional structural controllability, which states that the minimal number of driver nodes needed to fully control a network is determined by the maximum matching of networks, where the unmatched nodes are exactly needed to control. The number of drive nodes is represented by N_D.

Liu et al.'s framework [5] offers an efficient method to determine the minimum number of driver nodes for directed complex networks. However, the structural controllability is only applicable to directed networks characterized by structural matrices, in which all links are represented by independent free parameters. This requirement may be violated if exact link weights are given or by the symmetric characteristic of undirected networks. To overcome the limitations, Yuan et al. [7] proposed an exact controllability framework based on the Popov–Belevitch–Hautus (PBH) condition. The exact controllability is applicable to arbitrary complex networks, such as directed networks, undirected networks, weighted networks, unweighted networks, self-loop networks, and nonself-loop

networks. The specific content is that the minimum number of drive nodes N_D to fully control complex network (1) is determined by the maximum geometric weight of its adjacency matrix A:

$$N_D = \max_i\{\mu(\lambda_i)\}, \tag{3}$$

where $\mu(\lambda_i)$ is the geometric multiplicity of eigenvalue λ_i ($i = 1, 2, 3, \ldots, N$) of the adjacency matrix A. For large sparse complex networks, the exact controllability framework gives a method that only needs the rank of A to determine the number of driven nodes, that is,

$$N_D = \max\{1, N - \text{rank}(A)\}. \tag{4}$$

Controllability of complex networks is defined by the ratio of the minimum number of drive nodes required to fully control the networks to the total number of nodes, recorded as

$$n_D = \frac{N_D}{N}. \tag{5}$$

Its size reflects the degree of difficulty to control complex networks. The smaller the value is, the smaller the proportion of drive nodes required to control the network to the total number of nodes and the easier to control a network. Conversely, the network is less likely to be controlled.

3. Controllability of Complex Networks Based on Bridges

Bridge removal will break the connection and affect the functionality of a complex network. Aiming at this phenomenon, the concept of bridge removal is introduced into the problem of controllability of complex networks, and the influence of bridges removal on controllability is studied.

3.1. Process of Bridge Removal. A bridge is an edge of a network whose removal disconnects the network, i.e., it increases the number of connected components. Therefore, bridge removal will give rise to changes of control signal flow, which will lead to the changes of driver nodes to achieve complete control of the network. In order to study the influence of bridges on controllability of network, we perform the following steps:

(i) Step 1: search all edges with depth first search algorithm to find bridges in a network.

(ii) Step 2: select one of the bridges that its removal will disconnect most number of nodes from the connected component as the targeted bridge, attacking the targeted edge and updating the adjacency matrix of the network.

(iii) Step 3: calculate and record the controllability after removing the bridge.

(iv) Step 4: check whether the complex network still contains bridge(s). If there are bridge(s) in the network, return to step 2, otherwise, end the process.

This is an iterative process of deleting edges, as shown in Figure 1. Specific bridge is attacked in step 2. Then, calculate the controllability after bridge removal. Step 4 checks if the network still contains bridges. If bridges are still included, continue to iteratively delete until the network no longer contains bridges.

As comparison, we select some classic edge attack strategies based on betweenness, degree, and random failure to explore the impact of bridge removal on networks.

Edge attack based on betweenness has been studied earlier in complex networks [12]; betweenness is a global feature that measures the role and influence of edges in entire complex networks. Intuitively, if an edge is passed by a multitude of shortest paths, it indicates that the edge is important in the network. Betweenness is defined as the ratio of the number of shortest paths passing through the edge e_{ij} to the total number of shortest paths, that is, $B_{ij} = r_{ij}/r$, where r *is* the number of shortest paths of network and r_{ij} is the number of shortest paths passing the edge e_{ij}. The strategy of edge attack based on betweenness: firstly, sort all edges in descending order by B_{ij} and then delete the edge with highest B_{ij} in each step.

Nodes with higher degree play an important role in ensuring functions of the network, so it is necessary to believe that edges connected to nodes with higher degree are more important. Degree of edges is defined as the product of degree of nodes on both sides of a link [13], that is, $Ed_{ij} = k_i \times k_j$, where k_i and k_j are degree of nodes connected with the edge e_{ij}. The strategy of edge attack based on degree: firstly, sort all edges in descending order by their Ed_{ij} and then delete the edge with highest Ed_{ij} in each step.

The structure and interaction between nodes of complex networks are not the same, and bridges is an overall attribute; its distribution in networks is not the same, so the number of bridges in different networks is also different. In order to be able to effectively compare, the other three edge attack strategies should have the same number of failed edges as bridge removal.

3.2. Comparing Controllability on Edge Attack

3.2.1. ER Networks. In order to verify the influence of bridges removal on controllability, a series of comparative experiments on edge attack based on betweenness, degree, and random attack were conducted. Without loss of generality, we firstly generate ER networks with 800 nodes and average degree $<k> = 3$. As shown in Figure 2(a), n_D increases with the proportion of increasing edges attack, indicating that the controllability of the network decreases. By comparing, we can find bridge removal has a greater impact on controllability than other edge attack modes. This is because the disconnection of bridges leads to the break of control chain. The decomposed subgraph needs to add driver nodes to ensure that the network is controllable.

For ER networks with 800 nodes and average degree $<k> = 5$, the link is relatively more dense, the relationship between n_D and attack edge proportion p is shown in Figure 2(b), and we can find the network has a more strong

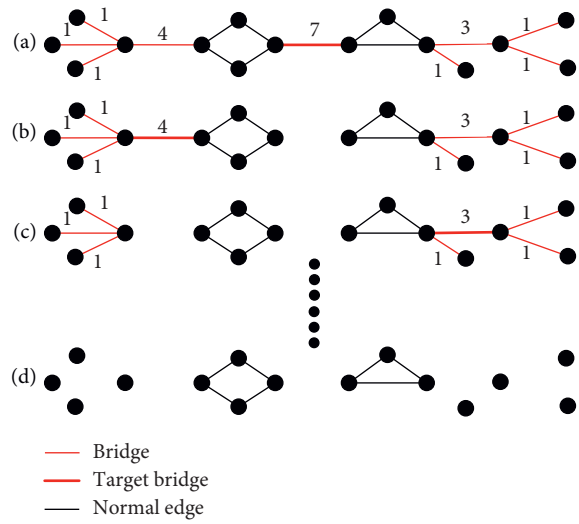

Figure 1: An example of the process of removing bridge. Bridges are shown in red, nonbridge edges are shown in black. The value next to the red edge represents the number of dropped nodes from the connected component due to removal of this edge. (a) A initial network. (b) The network after the first removal of bridge. (c) The network after the second removal of bridge. (d) The network after removal of all bridges.

controllability to resist edge attack of betweenness, degree, and random. However, only the bridge removal has a greater impact on controllability. Therefore, the effect of bridge removal on controllability is the greatest compared with other edge attack modes. And different from the average degree $<k> = 3$, under the same attack ratio, bridge removal has a significantly greater influence on controllability than other attack modes.

The connectivity of a network can be quantified by the largest connected component in the network [16]. Thus, we think the largest connected component can be used to measure the connectivity after some edges are attacked by different strategies. We define node ratio $s(q) = S/N$, where S is the number of nodes included in the largest connected component and N is the total number of nodes in network [14]. The relationship between $s(q)$ and attack edges proportion p is shown in Figure 3. It can be found that edge attack reduces the number of nodes in the largest connected component. It shows that the connectivity of the network decreases, and bridge removal has a greater damage to connectivity. At the same time, it can be found that there is some synchronization between controllability and the size of the largest connected component. When the largest connected component is reduced, the controllability is decreased, too. Therefore, controllability of complex networks is related to the connectivity of the network.

3.2.2. BA Scale-free Networks. Different from ER networks, the degree distribution of scale-free networks is heterogeneous, and there are some hub nodes of high degree in scale-free networks. And the uniformity of degree distribution has influence on controllability [3, 5]. We investigate the controllability and connectivity of scale-free networks with 800 nodes, and average degrees $<k> = 5$ and $<k> = 13$ are shown in Figures 4 and 5, respectively. Similar to ER networks, bridge removal of scale-free networks has a greater impact on controllability and connectivity than edge attack of betweenness, degree, and random.

3.3. Effect of Bridge Removal on Controllability. By comparing with edge attack of betweenness, degree, and random, we find that bridge removal has a greater impact on controllability. At the same time, the density of complex networks (that is, the average degree of networks) has impacts on the number of bridges contained in networks. Therefore, further studies are still necessary on the relationship between effect of bridge removal and average degree of complex networks. The effect is measured by the change of controllability before and after removing edges, that is,

$$\Delta n_D = n_D' - n_D, \tag{6}$$

where n_D' is the controllability measurement of complex networks after edges are removed. Δn_D reflects the change in controllability under attack. The smaller Δn_D is, the stronger the ability to maintain controllability and the better the controllability robustness of networks is. Conversely, the less the robustness of the network is.

We generate ER networks with 300, 500, and 800 nodes and various average degree $<k>$ from 2.5 to 5 and generate scale-free networks with 300, 500, and 800 nodes and various average degree $<k>$ from 4 to 16. Figure 6 shows the change of controllability Δn_D with the average degree growing after removing all bridges by the process in Section 3.1. In Figure 6(a), when the average degree is 2.5, the Δn_D is the highest, indicating that the networks are the least controllability robustness against bridge removal. As the average degree increases, Δn_D decreases gradually, indicating that the controllability robustness of ER networks is gradually increasing. In fact, when the average degree is greater than 5, bridge removal has little influence on controllability. It is found that, with increasing of average degree $<k>$, the number of bridges in complex networks is gradually

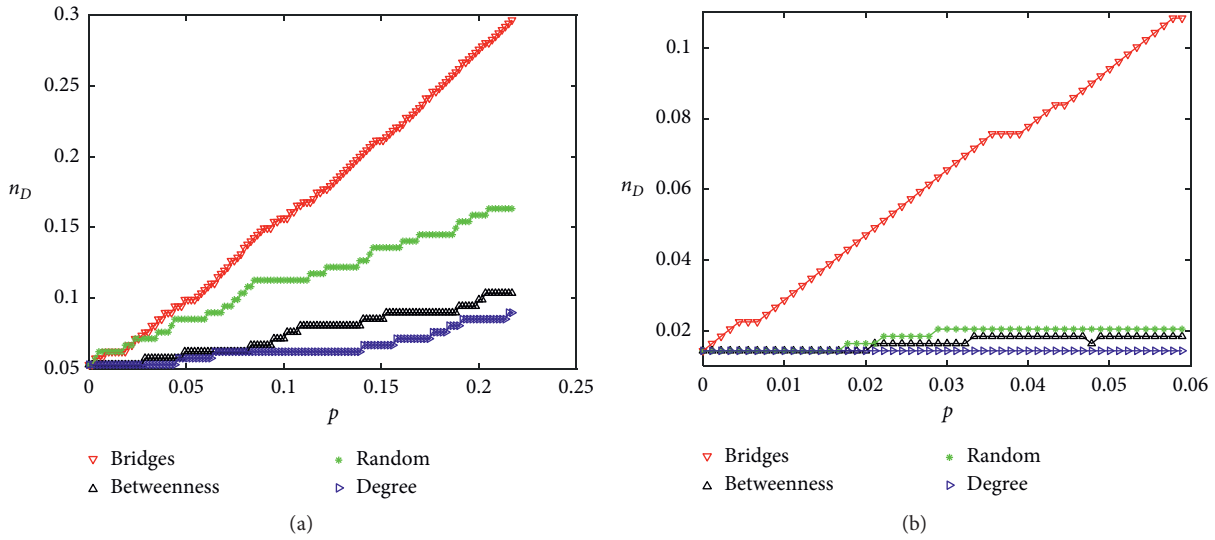

Figure 2: Controllability of ER random networks. (a) Average degree $<k> = 3$. (b) Average degree $<k> = 5$.

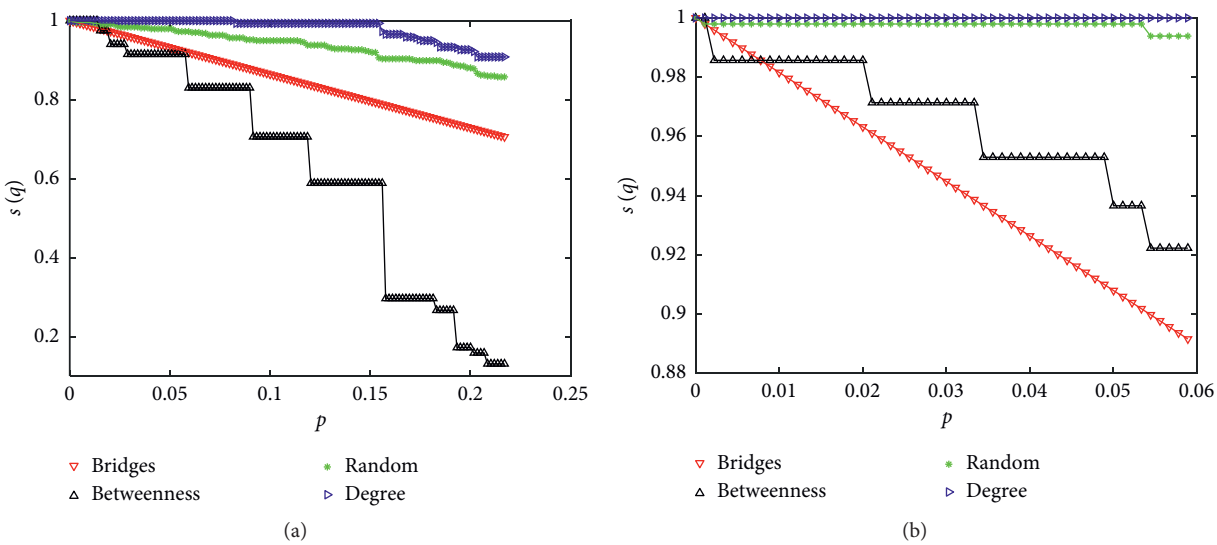

Figure 3: Connectivity of ER random networks. (a) Average degree $<k> = 3$. (b) Average degree $<k> = 5$.

reduced, which is also an important reason that networks are more robust against bridge removal.

After conducting the process of bridge removal in scale-free networks, Δn_D is shown in Figure 6(b). Similar to ER networks, the controllability robustness Δn_D of scale-free networks increases with increasing of average degree $<k>$. When the average degree $<k>$ is more than 16, the influence of bridge removal on controllability robustness becomes very limited. However, unlike ER networks, scale-free networks are dense networks. Even scale-free networks have more bridges than ER networks with the same average degree. Thus, scale-free networks have weaker controllability robustness than ER networks against bridge removal.

4. Optimization of Complex Networks Based on Bridges

4.1. Optimization Strategies. Through the analysis of the previous section, we know that bridges are important edges for maintaining controllability of networks when a network is attacked and has some link failures. Therefore, we propose two network optimization methods based on bridges to

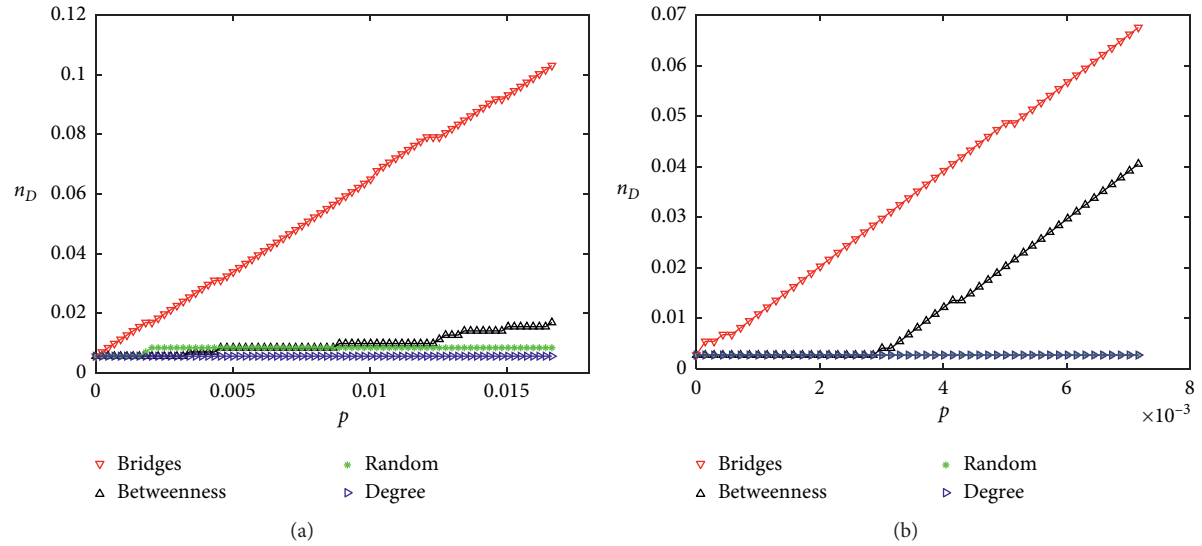

Figure 4: Controllability of BA scale-free networks. (a) Average degree$<k>=5$. (b) Average degree $<k>=13$.

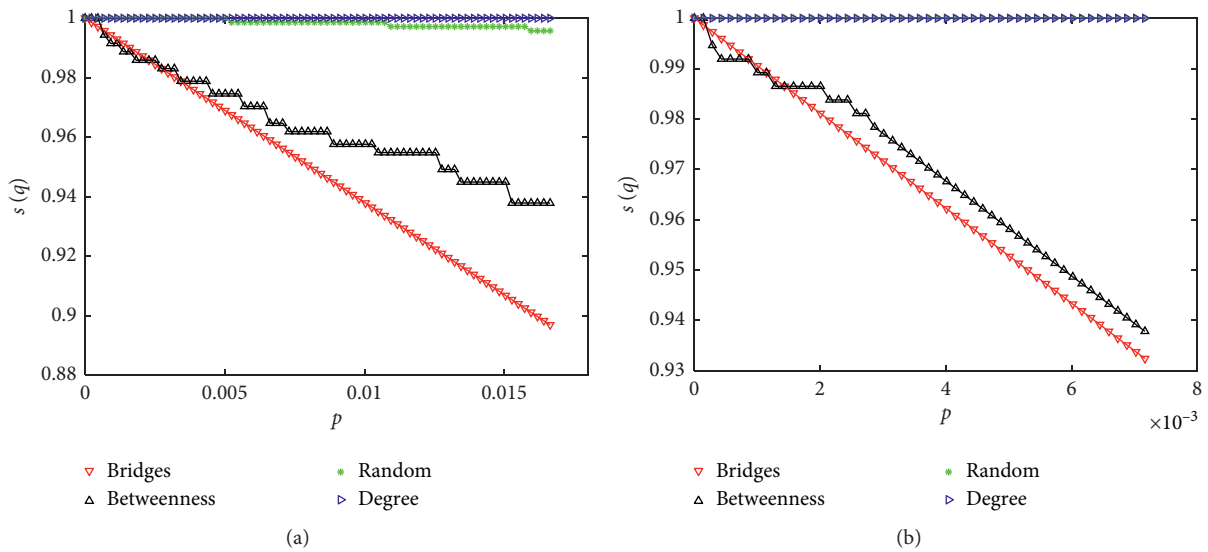

Figure 5: Connectivity of BA scale-free networks. (a) Average degree $<k>=5$. (b) Average degree $<k>=13$.

improve the ability to cope with various accidents and emergencies.

4.1.1. Bridge Backup. Bridge removal has a great impact on networks, so it is necessary against this situation. If bridges are backed up, the backup edges will be activated after a certain bridge failed so that the network will be restored to connections, thereby ensuring the network's security.

Figure 7 shows the model of bridge backup, and e_{12} (e_{ij} represents the edge from node i to node j) is a bridge of the network. Figure 7(a) shows the case of no backups, and we assume that backup edges will not be activated when the network is running; normally, they will not affect the topology of networks. Network after bridge backup is shown in Figure 7(b). When the bridge e_{12} is attacked, activate its backup edge to ensure that the network will not fail, as shown in Figure 7(c).

4.1.2. Bridge Elimination. The strategy eliminates bridges by adding edges on the periphery of bridges on the basis of the original network. Bridge elimination can not only ensure that there are no bridges in networks but also improve the performance. The specific operation process is as follows:

(i) Step 1: find all bridges in networks

(ii) Step 2: if the bridge is in the periphery position, starting from the peripheral node connected with bridge, the node that is found after expanding one edge in the direction of the other is the end point. Add an edge between the two nodes as an

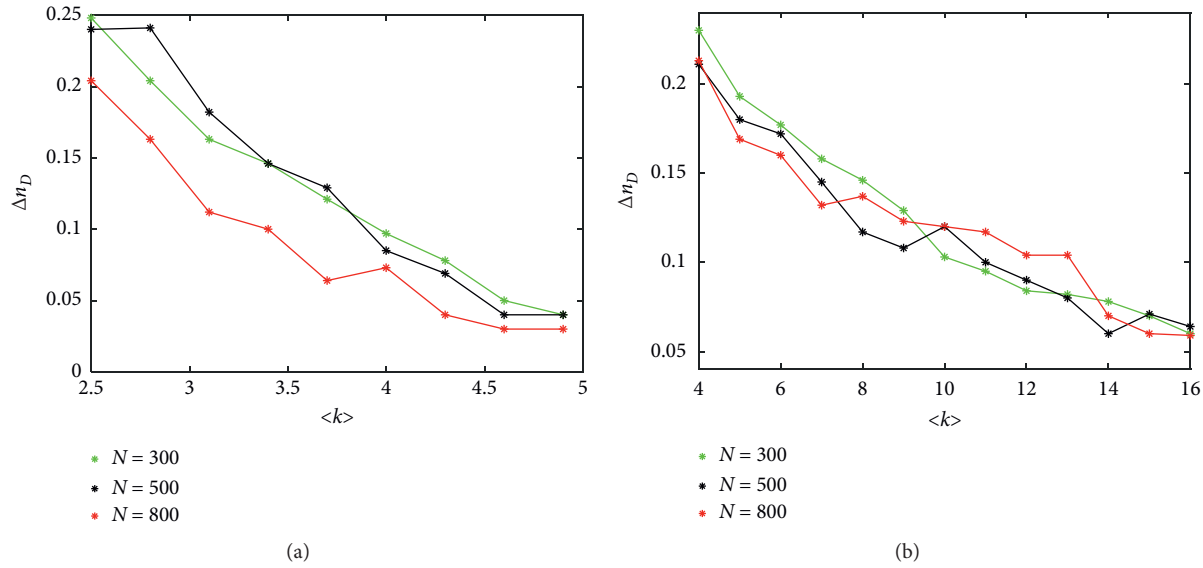

Figure 6: Change of controllability after bridge removal. (a) ER network and (b) BA scale-free network.

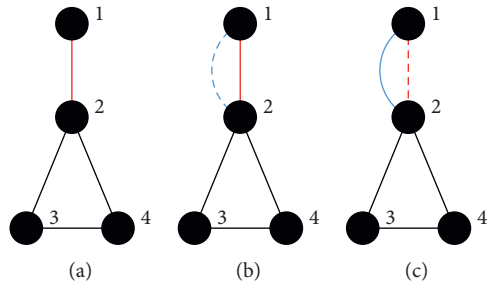

Figure 7: Model of bridge backup. (a) Initial network, (b) bridge backup, and (c) backup edge activation.

optimization edge. If the bridge is in the position of center, starting from the node on the side with more nodes connected with bridge, the node that is found after expanding one edge in the direction of the other is the end point. Add an edge between the two nodes to eliminate bridges and ensure networks are more uniform.

The model of bridges elimination is shown in Figure 8, where Figure 8(a) shows the situation that bridge e_{12} in the position of periphery. Node 1 is the peripheral node connected with the bridge. Expand one edge to the other side of the bridge and find node 3 and 4 (node 3 and 4 are symmetric). Randomly select one node as the end point, and add e_{13} as the optimization edge here; Figure 8(b) shows the case where the bridge is in the position of center. The number of nodes included on node 4 side is larger. Extend an edge to the other side of the bridge and find the nodes 6 and 7; the two nodes are symmetrically. Here, node 6 is taken as the end point, adding e_{46} as the optimization edge.

4.2. Optimization Effect in Model Network. As mentioned above, two optimization algorithms based on bridges are proposed. We will verify the effectiveness of the two optimization strategies in this section. In order to verify the feasibility and effectiveness of the strategies that we proposed, some classic optimization strategies [21, 22], including edge backup by degree, betweenness, random backups, and initial network without optimization, are chosen as comparison.

n_D reflects the controllability of complex networks and $s(q)$ reflects the connectivity of complex networks. And there is some relationship between the two parameters. Combining the parameters $s(q)$ and n_D, the following comprehensive performance indicator of networks is given:

$$R = \frac{s(q)}{n_D} = \frac{S}{N_D}. \tag{7}$$

The changes of R reflect the comprehensive adaptability of complex networks against attack. Optimizing this indicator can improve the topology of networks. Thus, if a network is under attack, the network can not only maintain a large connected subgraph but also retain a relatively complete control chain without being destroyed.

The procedure of bridge backup and bridge elimination is starting from two initial networks composed of $N = 800$ nodes, ER network with average degree $<k> = 3$, and BA network with average degree $<k> = 5$, respectively. In order to compare the

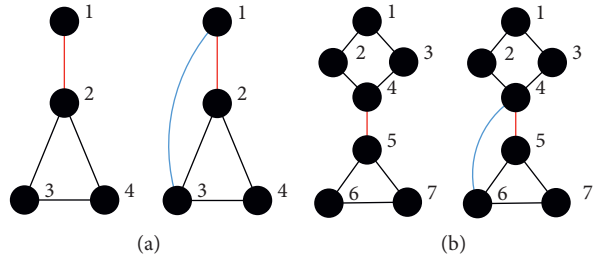

Figure 8: Model of bridge elimination. (a) Bridge in the position of periphery. (b) Bridge in the position of center.

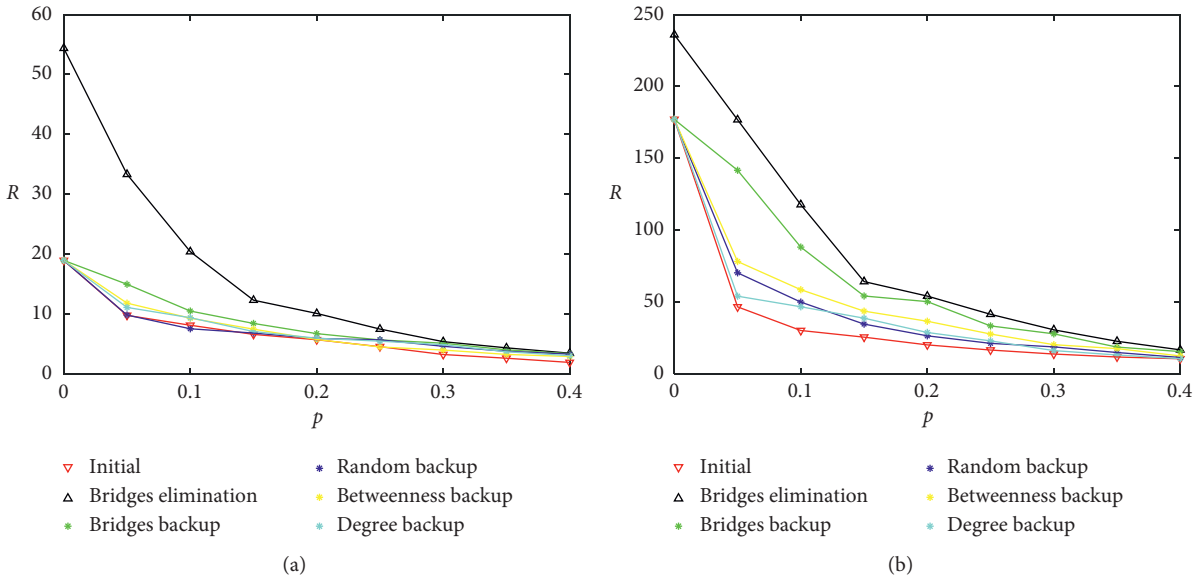

Figure 9: Comparison of optimization effect. (a) ER random network and (b) BA scale-free network.

effect of the two optimization strategies, edge backup based on degree, betweenness, random backup, and initial network without optimization are chosen as comparison.

We first remove the bridges in networks until all bridges are removed, and then continue to attack the networks with random failure strategies. A plot of R versus p under attack is shown in Figure 9. Except for the unstable random backup, all of strategies have a better performance than the initial network in the improvement on robustness of the network. The optimized network with bridge backup has the same performance on R with the initial network. This is because the strategy does not influence network structure before edges are attacked. The backup edges will be activated after certain bridges failed. However, bridge elimination can obviously improve the performance of networks before edges are attacked because the strategy influence network structure before an edge is attacked. As the proportion p of attack increases, bridge backup and bridge elimination have better effect than others.

4.3. Optimization Effect in Real Network. The transcription factor is one of the most basic elements for gene transcription regulation, which can bind DNA sites and regulate the corresponding target genes (transcription genes). *E. coli* transcription factors are abstracted into nodes in a network, and there is an edge connection if there is an interaction (regulatory effect) between the two factors, otherwise there is no edge connection. The *E. coli* transcription network is processed on the dataset [26], and the *E. coli* transcription network is constructed into an unweighted and undirected network with 688 nodes and 1078 edges.

The power grid is composed of transmission lines, power stations, and substations. This paper selects the 300-node standard test system as an example [27] to model the power network. The power plants and substations are abstracted into nodes, and the transmission lines are abstracted into edges in a complex network. The abstracted power network has 300 nodes and 409 edges.

In order to compare the effect of bridge backup, bridge elimination, and other backup methods for optimizing the real network, we take the *E. coli* transcription network and the IEEE standard power test network as examples. The optimized network and the initial network are tested for robustness by randomly deleting edges. The change of the comprehensive index R with the random failure ratio of edges is shown in Figure 10.

It can be seen that the bridge elimination method can effectively improve the network's ability to deal with

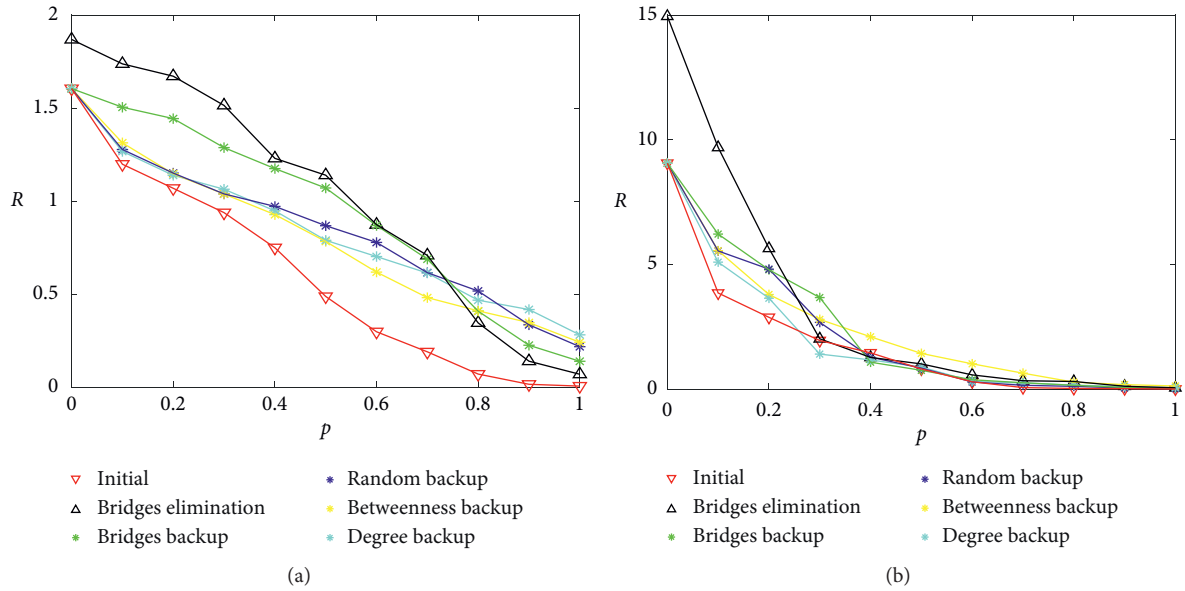

Figure 10: Optimization of real networks. (a) *E. coli* transcription network and (b) IEEE standard power network.

external attacks and can improve the controllability and connectivity of the initial network. The bridge backup does not change the network structure and only works when the bridges fail. Therefore, the performance of the network with zero failure ratio is the same as that of the initial network. However, as the proportion of edge failures increases, under the same cost (the number of backup edges is the same), it has a greater advantage over other methods.

5. Conclusions

We investigate the controllability of complex networks when bridges are iteratively deleted by attacks. And edge attacks based on degree, betweenness, and random failure are chosen as comparison. It is found that bridge removal has larger effect on the network controllability than that of other attacks. In addition, the results show that the effect on controllability of bridge removal is related to the degree of networks. When the average degree of network is low, bridge removal has more influence on controllability. While the average degree grows, the controllable robustness of networks against bridge removal is improved. On this basis, we propose two strategies for optimization of complex networks. Both bridge backup and bridge elimination can indeed improve the robustness of networks. Therefore, when we design a network, we should try to avoid the situation that the network includes a large number of bridges.

The source code of the work is available in [28].

Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author upon reasonable request. And the simulation data used to support the findings of this study and MATLAB programs can be obtained from [28].

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by National Natural Science Foundation of China (Grant nos. 61573077 and U1808205) and Fundamental Research Funds for the Central Universities (Grant no. N2023022).

References

[1] P. G. Sun, "Controllability and modularity of complex networks," *Information Sciences*, vol. 325, pp. 20–32, 2015.

[2] H. Cherifi, G. Palla, B. K. Szymanski, and X. Lu, "On community structure in complex networks: challenges and opportunities," *Applied Network Science*, vol. 4, no. 1, p. 117, 2019.

[3] Z. Shen, W. X. Wang, Y. Fan, Z. Di, and Y. C. Lai, "Reconstructing propagation networks with natural diversity and identifying hidden sources," *Nature Communications*, vol. 5, p. 4323, 2014.

[4] X. Liu and T. Chen, "Synchronization of complex networks via aperiodically intermittent pinning control," *IEEE Transactions on Automatic Control*, vol. 60, no. 12, pp. 3316–3321, 2015.

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

[6] Q. Xuan and T. J. Wu, "Node matching between complex networks," *Physical Review E*, vol. 80, no. 2, Article ID 026103, 2009.

[7] Z. Yuan, C. Zhao, Z. Di, W.-X. Wang, and Y. C. Lai, "Exact controllability of complex networks," *Nature Communications*, vol. 4, p. 2447, 2013.

[8] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang, "Attack robustness and centrality of complex networks," *PloS One*, vol. 8, no. 4, Article ID e59613, 2013.

[9] J. Wang, "Robustness of complex networks with the local protection strategy against cascading failures," *Safety Science*, vol. 53, pp. 219–225, 2013.
[10] Z. Chen, J. Wu, Y. Xia, and X. Zhang, "Robustness of interdependent power grids and communication networks: a complex network perspective," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 1, pp. 115–119, 2018.
[11] G. Kashyap and G. Ambika, "Link deletion in directed complex networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 514, pp. 631–643, 2019.
[12] C.-L. Pu and W. Cui, "Vulnerability of complex networks under path-based attacks," *Physica A: Statistical Mechanics and Its Applications*, vol. 419, pp. 622–629, 2015.
[13] Z. M. Lu and X. F. Li, "Attack vulnerability of network controllability," *PloS One*, vol. 11, no. 9, Article ID e0162289, 2016.
[14] J. Thomas, S. Ghosh, D. Parek, D. Ruths, and J. Ruths, "Robustness of network controllability to degree-based edge attacks," in *Proceedings of the International Workshop on Complex Networks and Their Applications*, pp. 525–537, Springer, Milan, Italy, November 2016.
[15] S.-M. Chen, Y.-F. Xu, and S. Nie, "Robustness of network controllability in cascading failure," *Physica A: Statistical Mechanics and Its Applications*, vol. 471, pp. 536–539, 2017.
[16] M. M. Danziger, L. M. Shekhtman, A. Bashan et al., "Vulnerability of interdependent networks and networks of networks," in *Interconnected Networks*, pp. 79–99, Springer, Cham, Switzerland, 2016.
[17] L. Hou, S. Lao, M. Small, and Y. Xiao, "Enhancing complex network controllability by minimum link direction reversal," *Physics Letters A*, vol. 379, no. 20-21, pp. 1321–1325, 2015.
[18] Y.-D. Xiao, S.-Y. Lao, L.-L. Hou, and L. Bai, "Optimization of robustness of network controllability against malicious attacks," *Chinese Physics B*, vol. 23, no. 11, Article ID 118902, 2014.
[19] X.-F. Li and Z.-M. Lu, "Optimizing the controllability of arbitrary networks with genetic algorithm," *Physica A: Statistical Mechanics and Its Applications*, vol. 447, pp. 422–433, 2016.
[20] F. L. Iudice, F. Garofalo, and F. Sorrentino, "Structural permeability of complex networks to control signals," *Nature Communications*, vol. 6, p. 8349, 2015.
[21] Z. Zhang, Y. Yin, X. Zhang, L. Liu et al., "Optimization of robustness of interdependent network controllability by redundant design," *PloS One*, vol. 13, no. 2, Article ID e0192874, 2018.
[22] L. Liu, Y. Yin, Z. Zhang, and Y. K. Malaiya, "Redundant design in interdependent networks," *PloS One*, vol. 11, no. 10, Article ID e0164777, 2016.
[23] X. Y. Yan, W. X. Wang, G. R. Chen, and D. H. Shi, "Multiplex congruence network of natural numbers," *Scientific Reports*, vol. 6, p. 23714, 2016.
[24] Y. Lou, L. Wang, and G. Chen, "Toward stronger robustness of network controllability: a snapback network model," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 9, pp. 2983–2991, 2018.
[25] A. K. Wu, L. Tian, and Y. Y. Liu, "Bridges in complex networks," *Physical Review E*, vol. 97, no. 1, Article ID 012307, 2018.
[26] R. A. Rossi and N. K. Ahmed, "The network data repository with interactive graph analytics and visualization," in *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence*, Austin, TX, USA, January 2015.
[27] X. Dong, H. Sun, C. Wang et al., "Power flow analysis considering automatic generation control for multi-area interconnection power networks," *IEEE Transactions on Industry Applications*, vol. 53, no. 6, pp. 5200–5208, 2017.
[28] Complexity paper codes. Accessed: 2020. [Online]. Available: https://github.com/RCRC-123/Complexity_Paper-Codes.