axioms

MDPI

Article

Towards Optimal Robustness of Network Controllability by Nested-Edge Rectification

Zhuoran Yu, Junfeng Nie and Junli Li *

School of Computer Science, Sichuan Normal University, Chengdu 610101, China
* Correspondence: lijunli@sicnu.edu.cn

Abstract: When a network is attacked, the network controllability decreases and the network is at risk of collapse. A network with good controllability robustness can better maintain its own controllability while under attack to provide time for network recovery. In order to explore how to build a network with optimal controllability robustness, an exhaustive search with adding edges was executed on a given set of small-sized networks. By exhaustive search, we mean: (1) All possible ways of adding edges, except self-loops, were considered and calculated at the time of adding each edge. (2) All possible node removal sequences were taken into account. The nested ring structure (NRS) was obtained from the result of the exhaustive search. NRS has a backbone ring, and the remaining edges of each node point to the nearest nodes along the direction of the backbone ring's edges. The NRS satisfies an empirically necessary condition (ENC) and has great ability to resist random attacks. Therefore, nested edge rectifcation (NER) was designed to optimize the network for controllability robustness by constructing NRS in networks. NER was compared with the random edge rectification (RER) strategy and the unconstrained rewiring (UCR) strategy on synthetic networks and real-world networks by simulation. The simulation results show that NER can better improve the robustness of network's controllability, and NER can also quickly improve the initial network controllability for networks with more than one driver node. In addition, as NER is executed, NRS gains more edges in the network, so the network has better controllability robustness. NER will be helpful for network model design or network optimization in future.

Keywords: complex network; network controllability; controllability robustness; optimization; nested ring structure; edge rectification

Citation: Yu, Z.; Nie, J.; Li, J. Towards Optimal Robustness of Network Controllability by Nested-Edge Rectification. *Axioms* **2022**, *11*, 639. https://doi.org/10.3390/axioms11110639

Academic Editor: Abbe Mowshowitz

Received: 6 October 2022
Accepted: 11 November 2022
Published: 13 November 2022

1. Introduction

Complex networks have been developed greatly in the past 20 years, and they have become a new discipline involving mathematical science, social science, biological science and other fields [1–4]. Many natural and artificial systems can be abstracted into complex networks composed of nodes and edges, such as the Internet [5], transportation networks [6] and power networks [7]. The study of network formation, topology, community [8] and synchronization [9] is conducive to understanding the structure and function of a network; and the study of cycle [10,11] is a new direction. The sizes of complex networks have increased dramatically. The graph-query problem on large networks can be solved by query optimization [12]. Deep learning provides a way to evaluate the robustness of large-scale networks [13]. As controlling networks to serve people is one purpose of studying complex networks, whether the network can be controlled is critical, so network controllability has emerged as a key point for complex networks [13–18]. Controllability is the ability to guide the network from any initial state to any desired final state in a finite amount of time with appropriate input choices. The ability of complex networks to maintain controllability under attack is called controllability robustness.

For directed networks, the structural controllability of the network can be measured by finding the maximum matching of the network to determine the minimum number

of external control inputs that are driver nodes [19]. Finding maximum matching can only be applied to directed networks and is difficult to be applied to large-scale networks. Therefore, the exact controllability framework was proposed, which can be applied to all large-scale sparse networks [20].

There have been many studies on the relationship between the topology and controllability of directed networks. The underlying degree of correlation has a certain effect on network controllability. Clustering coefficient and modularity have no obvious effect on network controllability [21]. When the minimum in-degree and out-degree are both greater than two, random networks with any topology can be controlled by an infinitesimal fraction of driver nodes [14]. Based on the hierarchical structure of the directed network, a random upstream or downstream attack is designed [22]. Compared with an ordinary random attack, this attack strategy is more effective because the upstream and downstream nodes of a randomly selected node have greater chances of being the hub.

There is growing concern about random and malicious attacks on complex networks [19,23]. Random attacks refer to the uniform random selection of attack targets. Malicious attacks choose the most effective targets to attack subjectively. Malicious attacks usually achieve better results than random attacks, but random attacks take less time.

It is necessary to make networks more robust attacks, especially practical networks. For connectivity robustness, a spectral metric is taken as the objective function to optimize connectivity robustness by edge rectification, which keeps the network's degree distribution unchanged after reconnecting edges [24]. A smart rewiring strategy was used to strengthen the connections between adjacent nodes of a hub node to improve the robustness of the network against the degree attack [25]. Onion-shaped networks with better connectivity robustness were obtained through the degree-preserving edge reconnection strategy [26]. There are also studies on optimizing controllability robustness. Bridges are edges which have a significant impact on the controllability of the network after their removal, especially when the average degree of the network is low. The robustness of network controllability can be improved by backing up bridges, and adding edges to eliminate bridges can significantly improve controllability robustness [27]. An empirically necessary condition (ENC) indicates that the maximum and minimum in-degree and out-degree of the optimal network structure should be almost the same, or within a very narrow range; that is, the network should be extremely uniform [28]. Adjusting the network to meet the ENC by reconnecting edges can greatly improve the robustness of network controllability. In addition, networks with better controllability robustness can be constructed. A new complex network model, the q-snapback network, was proposed, which has gppd controllability robustness by using the feedback idea of control theory [29]. The backbone chain is beneficial to the controllability robustness of the q-snapback network, but it affects the flexibility of network construction. Thus, the superior controllability robustness of q-snapback network was improved by redirecting edges [30].

This paper explores a network structure that can enhance the robustness of network controllability against random attacks. In this paper, one edge is added to the original network, and the network with the best controllability robustness after adding the edge is used as the new original network. The nested ring structure (NRS) is obtained by exhaustive search. Then, NRS is constructed by the nested edge rectification (NER) strategy. NER constructs NRS by adjusting the edge of a node with the maximum degree to connect the node to its nearest neighboring node along the direction of the backbone ring each time. If there is no backbone, a backbone is constructed on the network first. Through NER, the heterogeneity of degree is reduced.

The main contributions of the paper are:

1. Due to the impossibility of theoretical analysis and exhaustive searching for large-sized networks, an exhaustive search was executed on feasible small-sized networks, and NRS was obtained. NRS satisfies ENC and has great controllability robustness.
2. NER is proposed to improve the robustness of the network controllability against random attacks by constructing NRS in the network. Meanwhile, NER can be applied

to networks with different scales. In addition, NER constructs a backbone ring through maximum matching, which rapidly improves the initial controllability of networks.

3. The controllability robustness can be improved on six synthetic networks and real-world networks by NER, and NER is better than other methods of edge rectification. For networks with poor controllability robustness, such as the scale-free network, NER improves controllability robustness more obviously.

The remainder of the paper is structured as follows: Section 2 reviews network controllability and the controllability robustness of complex network. Section 3 introduces the exhaustive search. Section 4 discusses the experimental results. Section 5 presents the conclusions.

2. Network Controllability and Its Robustness

The robustness of network controllability is mainly concerned with the change in controllability when the network is attacked. Controllability robustness can evaluate the attack effect of the attack mode on the network and the ability of the network to resist the attack. Network controllability is measured by the density of driver nodes n_D.

$$n_D = \frac{N_D}{N}, \tag{1}$$

where N_D represents the number of driver nodes required to maintain network controllability and N represents the number of network nodes. The minimum value of n_D is $1/N$, and the maximum value is 1. A smaller value of n_D indicates better network controllability, whereas a larger value of n_D indicates worse network controllability.

A matching is a set of edges that do not share common start nodes or common end nodes. A maximum matching is a matching that contains as many edges as possible and cannot be extended further in the network. The end node of an edge in matching is a matched node; otherwise, it is an unmatched node. According to the minimum-inputs theorem [19], N_D can be obtained by the number of unmatched nodes for a directed network:

$$N_D = max\{1, N - |E^*|\}, \tag{2}$$

where $|E^*|$ is the size of maximum matching. For node attacks, the controllability robustness of the network can be measured by the controllability curve, which is calculated as follows:

$$n_D(i) = \frac{N_D(i)}{N - i}, i = 1, 2, 3, ..., N - 1 \tag{3}$$

where $N_D(i)$ is the number of driver nodes needed to maintain network controllability after removing i nodes. N is the size of the original network. R_N records the change in network controllability after each node is removed. The overall measure of controllability robustness can be obtained by averaging controllability curves, which is calculated as follows:

$$R_N = \frac{1}{N-1} \sum_{i=1}^{N-1} n_D(i), \tag{4}$$

where $n_D(i)$ is the structural controllability of the remaining network after i nodes are removed. In addition to the controllability curve, the robustness of network controllability can also be compared by R_N. A smaller R_N indicates better controllability robustness, whereas a larger R_N indicates worse controllability robustness.

3. Nested Ring Structure and Optimization Strategy

The relationship between network topology and network controllability robustness was explored by observing the adding-edge simulation and attack simulations on a series of small-sized networks. The topology with the best controllability robustness after adding edges can be obtained by exhaustive search. Then, NRS can be obtained by observing

the results of the exhaustive search. The NRS has a great ability to resist random attacks and satisfies the ENC. NRS is constructed in the network to improve the controllability robustness of the network under random attacks. Therefore, NER is proposed to construct a NRS in networks.

3.1. Nested Ring Structure

An exhaustive search is where all the cases of adding one edge are searched and all the node-removal sequences are considered when calculating the controllability robustness.

(a) Exhaustive adding edge. The ring structure is the network structure that may be built by N nodes and N edges that have the best controllability robustness for directed graphs, as shown in Figure 1a. With the ring structure as the initial network for adding an edge, one edge at a time, then for a network with N nodes and M edges, there are a total of $N(N-1)-M$ ways to add an edge, without considering the self-loop. Compared to all networks after adding edges, the network with the best controllability robustness is chosen as the next place to add the edge.

(b) Exhaustive attack. For each network, the controllability changes under all conceivable node-removal sequences are taken into account while determining the network controllability robustness. That is, for a network with N nodes, the number of all the node-removal sequences is $N!$. Each sequence has $N-1$ nodes, so there are $N!$ permutations of the controllability curves. The $k-th(k \in [1, N!])$ removal-node sequence is $n_D^k = \{n_D^k(1), n_D^k(2), \ldots, n_D^k(N-1)\}$, and its robustness is calculated as

$$R_N^k = \frac{1}{N-1} \sum_{i=1}^{N-1} n_D^k(i). \tag{5}$$

The overall controllability robustness is obtained by averaging the $N!$ robustness values:

$$\langle R_N \rangle = \frac{1}{N!} \sum_{k=1}^{N!} R_N^k. \tag{6}$$

An exhaustive search looks at all node-removal sequences equally. Therefore, when the random attack is repeated enough times, the average result of the exhaustive attacks is equal to the result of the random attacks. The exhaustive method is impossibly applied on the large-sized classical synthetic networks and the real-world networks, so random attacks should be used instead.

In this study, an exhaustive search was performed for networks with N = 5, 6, 7, 8, 9. When N = 8, there are $N(N-1)-N = 48$ ways to add one edge based on the ring structure in Figure 1a, without considering the self-loop. Only one equivalent structure was kept, and the final network structure is shown in Figure 1b–g. Among all the network structures, the network structure in Figure 1c has the optimal controllability robustness, and then the next adding edge is based on this network structure.

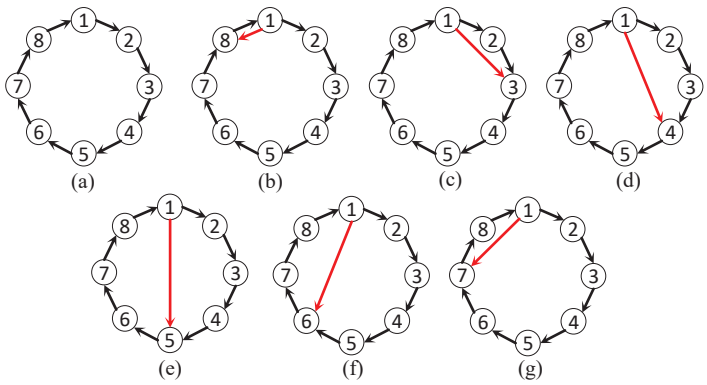

Figure 1. All cases of adding an edge for original network. (**a**) original network structure; (**b**–**g**) all cases after adding one edge to the original network. The red edge is the added edge.

The optimal way to add edges from the exhaustive search is shown in Figure 2. According to the ring structure, for all nodes $i = 1, 2, 3, \ldots, N$, an edge is added from node i to node j, $j = (i + r) \mod N$, where $r \in [2, N - 1)$. However, this rule only exists when the average degree of the network is low, so the value of r is far less than $N - 1$. The finally obtained network structure is named the nested ring structure (NRS). In addition, the structure has strong controllability robustness, since it satisfies ENC. The network structure satisfying ENC is extremely uniform, which states that the maximum and minimum out-degree (in-degree) should be equal or have a difference of 1.

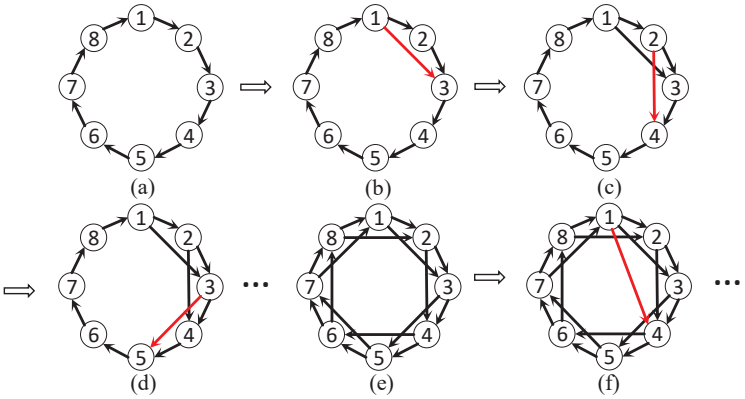

Figure 2. Adding edge results for exhaustive search. (**a**) Original network; (**b**–**f**) the result of incrementally adding edges.

As shown in Figure 3, the network has a NRS after adding a certain number of edges, which requires only one driver node to control the whole network, and the number of driver nodes does not increase immediately when the network suffers from random attacks. It can be seen that the more edges are contained in NRS, the stronger network's controllability robustness under random attacks and the more nodes need to be removed before the number of driver nodes increases from 1 to 2. In NRS, each node has an edge leading from its predecessor node to its successor node, which makes the network have a larger average distance, but at the same time, it makes the network can maintain the backbone ring structure after the node is removed. In Figure 3a, if node 2 is removed, there is still an edge A_{13} from its predecessor node 1 to its successor node 3. It implies that the NRS can increase its ability to maintain the backbone ring by having more edges.

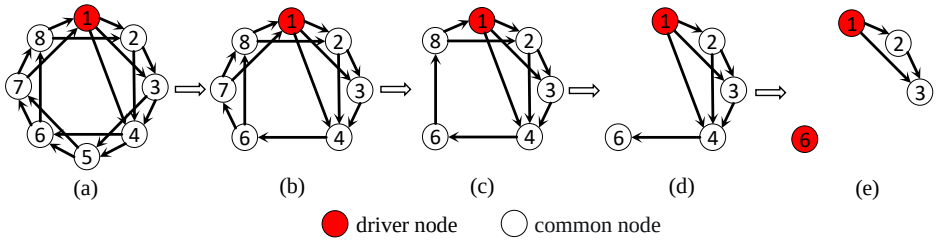

Figure 3. The process of a random attack. (**a**) Original network; (**b**–**e**) The network under random attack processes.

3.2. Nested Edge Rectification

NRS is a structure with great controllability robustness. NRS is constructed in networks by NER to optimize networks. When NRS is constructed in networks, a backbone is firstly constructed through maximum matching. The subsequent operations to build the NRS are performed on the backbone.

The NER is as follows:

Step 1: Whether a backbone ring exists should be determined in the original network G. If so, go to Step 2. If not, look for a kind of maximum matching in network. Delete the edge

A_{ij} (node i is the node with the largest out-degree in the network, node j is the node with the largest in-degree among the successors of node i and A_{ij} is not in the maximum matching). Add edge A_{kl} (node k is only the end node of the edge in the maximum matching, and node l is only the start node of the edge in the maximum matching) and run the command N_D times.

Step 2: Find the backbone ring in the network G and label the nodes as $1, 2, ..., N$.

Step 3: For node m (m belongs to $[1, N]$), check whether there is an edge $A_{(m(m+r))}$ (r belongs to $[2, M/N-1)$; if not, a backbone is constructed through maximum matching, as shown in Figure 4. Delete edge A_{ij} (node i is the node with the largest out-degree in the network, node j is the node with the largest in-degree in the successor nodes of node i and node j is not $i+1, i+2, \ldots, i+r$). Add an edge $A_{(m(m+r))}$. Record the number of adding edges and judge whether the number of added edges reaches the preset value; if so, stop, and if not, repeat step 3.

The details of NER execution process are shown in Algorithm 1:

Algorithm 1 Nested ring rectification strategy

input: The adjacency matrix of the network A; the number of network nodes N; the number of network edges M; Number of reconnected edges $TIMES$
Output: Adjacency matrix of the optimized network A
$t \leftarrow 0$;
if backbone does not exists on the network **then**
  $STARTNODE \leftarrow$ nodes that are only the started node of an edge in a maximum matching
  $ENDNODE \leftarrow$ nodes that are only the ended node of an edge in a maximum matching

  for $i \leftarrow 1$ **to** $|STARTNODE|$ **do**
    $i \leftarrow$ node with the largest out-degree
    $j \leftarrow$ node with the largest in-degree among the successors of node i
    delete edge $A_{(i,j)}$
    add edge $A_{(STARTNODE(i),STARTNODE(mod(i+1,N)))}$
    $t \leftarrow t+1$
  end for
  Number nodes as $1, 2, ...N$ through backbone;
end if
for $r \leftarrow 2$ **to** M/N **do**
  for $m \leftarrow 1$ **to** N **do**
    if do not exist edge $A_{(m,m+r)}$ **then**
      $i \leftarrow$ node with the largest out-degree
      $j \leftarrow$ The node with the largest outdegree among the successors of node i is except $i+1, i+2, ..., i+r-1$
      delete edge $A_{(i,j)}$
      add edge $A_{(j,mod(j+r,N)}$
      $t \leftarrow t+1$
      if $t == TIMES$ **then**
        return A
      end if
    end if
  end for
end for
return A

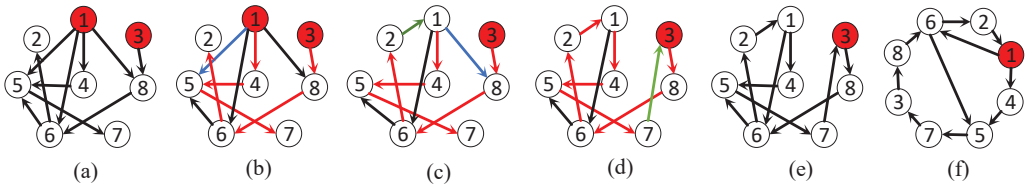

Figure 4. Construct backbone ring. (**a**) Original network; (**b**) a kind of maximum matching of the network; (**c**,**d**) the backbone ring is constructed by maximum matching; (**e**) the final network; (**f**) equivalent structure of the final network. The red line is maximum matching, the blue edge is a deleted edge and the green edge is an added edge.

3.3. Computational Complexity

It is mainly through the Hopcroft—Karp algorithm that the maximum matching is found to determine the starting nodes and ending nodes that are only used as the maximum matching edges. The computational complexity is $O(M \cdot \sqrt{N})$, where N is the number of nodes and M is the number of edges. The computational complexity of constructing a backbone is $O(N)$. The computational complexity of constructing a NRS is $O(N \cdot M^2 - 2 \cdot N^2)$ by rectifying edges after constructing backbone.

4. Simulation Results

NER was applied to six synthetic networks and two real-world networks to optimize the controllability robustness of these networks. In order to verify the effectiveness of NER, it is compared with the random edge rectification (RER) strategy and the unconstrained-rewiring (UCR) strategy. This paper mainly explores the influence of NER on the controllability robustness and the changes in network features.

The six synthetic networks were the Erdös–Rényi random-graph (ER) network [31], Generic scale-free (SF) network [32], random triangle (RT) network [33], random rectangle (RR) network [33], Newman–Watts small-world (SW) network [34] and q-snapback (QS) network [32]. The real-world networks were Roget network and ia-email-univ network [35]. All of these are directed networks.

4.1. Results on Synthetic Networks

For directed networks, the network size was set to 500, 1000 or 1500. This paper mainly discusses the networks with 1000 nodes. The average degree of the network was set $<k> = 4$. In order to reduce the influence of randomness, 30 instances were generated for each network, and the values of the controllability robustness of 30 random attacks for each instance were averaged.

As shown in Figure 5, six synthetic networks were used as the initial networks for optimization. For each network, the network optimized by building a NRS in the network through NER had the best controllability robustness compared with UCR- and RER-treated networks. The controllability robustness is shown in Table 1 after performing different types of edge rectification. RER and NER can improve the robustness of the network's controllability more than UCR, and the effect of NER is better than that of RER, especially on SF and QS. Figures A1 and A2 and Tables A1 and A2 in Appendix A show similar effects for networks with 500 and 1500 nodes. Networks had the best controllability robustness after optimization by NER on the six synthetic networks with 500 and 1500 nodes. NER can be applied to networks of different scales, which shows that NER has good scalability.

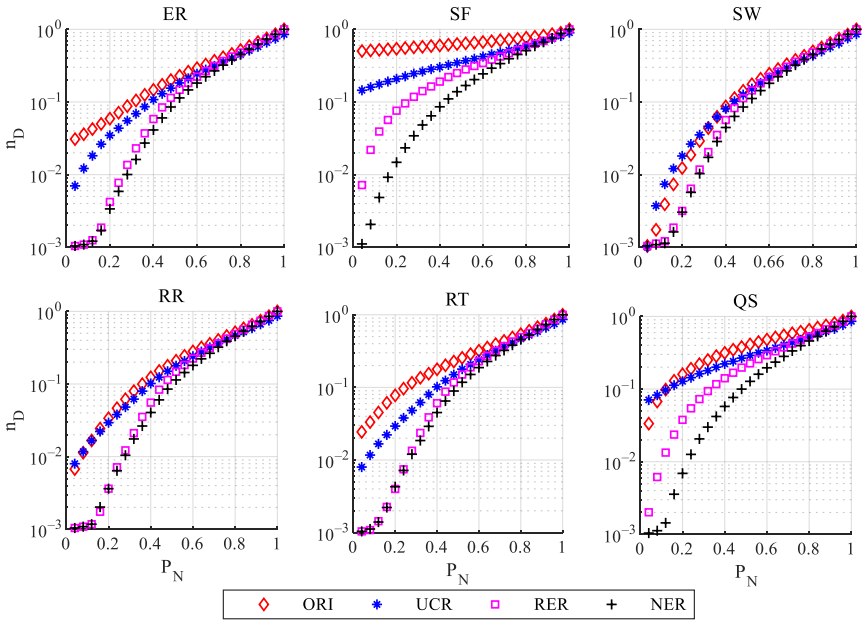

Figure 5. Robustness of the structural controllability of the six original networks with $N = 1000$ by rewiring 2000 times. P_N represents the proportion of nodes to be removed. ORI represents the original network without edge rectification. UCR, RER and NER represent the ways of edge rectification.

Table 1. Robustness of network controllability with different numbers of edge rectification operations.

Number of Edge Rectification	Strategy	ER	SF	RT	RR	SW	QS
0		0.2963	0.6557	0.3124	0.2798	0.2605	0.4168
1000	UCR	0.2884	0.5147	0.2995	0.2796	0.2634	0.4012
	RER	0.2510	0.4414	0.2564	0.2478	0.2437	0.3451
	NER	0.2437	0.3527	0.2482	0.2419	0.2362	0.2900
1500	UCR	0.2852	0.4696	0.2962	0.2787	0.2657	0.3852
	RER	0.2446	0.3745	0.2472	0.2433	0.2420	0.3121
	NER	0.2353	0.2891	0.2368	0.2338	0.2301	0.2591
2000	UCR	0.2820	0.4348	0.2927	0.2786	0.2641	0.3682
	RER	0.2419	0.3221	0.2435	0.2412	0.2402	0.2856
	NER	0.2242	0.2603	0.2253	0.2233	0.2228	0.2322

In Figure 6, each boxplot shows the proportion of nodes that needed to be removed to make the number of driver nodes changed from 1 to 2 when a network obtained by NER or RER on six synthetic networks was subjected to random attacks. For SF and QS, networks obtained by NER obviously needed to remove more nodes than networks obtained by RER to increase the number of driver nodes. After performing the same number of operations, the fewest nodes needed to be removed in SF, and the most nodes needed to be removed in SW, which is also related to the robustness of the original network controllability. The SF needs a considerable number of edge rectification operations to construct the backbone ring. Therefore, when the same number of edge rectification operations is performed, the number of edges of the NRS in the network is much less than those of other networks. QS has a backbone structure, so NRS produced more edges in QS with the same number of operations, which makes QS have a strong ability to resist random attacks.

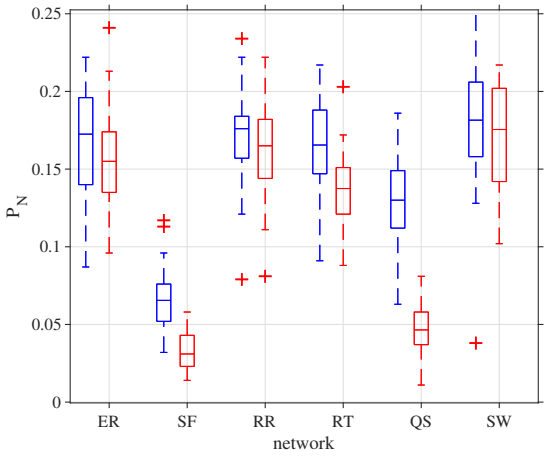

Figure 6. Ratio of nodes to be removed when the number of driver nodes changes from 1 to 2 on six synthetic networks after 2N NER operations. The blue represents networks after NER, and the red represents networks after RER. "network" represents the types of original networks. P_N represents the ratio of nodes to be removed.

In Figure 7, the variation in heterogeneity of out-degree (HO) and that in the heterogeneity of in-degree (HI) during the attack are shown. It can be seen that the heterogeneity of degree gradually increases as the attack goes on. SF has the largest HO and HI of the original networks, and SW has the smallest HO and HI. As the number of NER operations increased, the differences in HI and HO of different networks became smaller. This suggests that networks with lower HO and HI have better controllability robustness. More features of networks are shown in Table 2. In addition to QS, the network obtained by NER had the largest average, the shortest path and the largest medium number. It had the largest clustering coefficient of all networks. RER and NER both reduced the heterogeneity of degree.

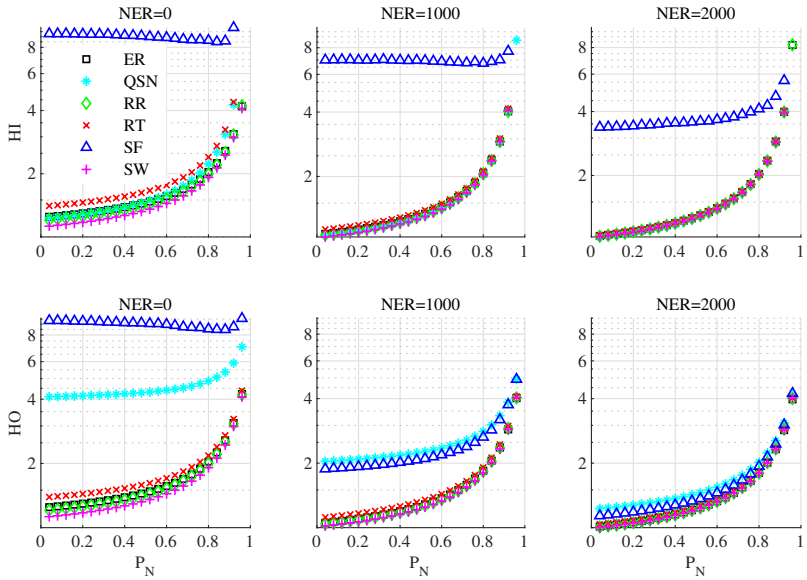

Figure 7. Changes in HO and HI of six networks after NER for different lengths of time under random attacks.

Table 2. Changes in the basic features of the original network and the network for which the edge rectification operation was performed 2000 times. Average path length (APL), average (node), betweenness centrality (ABC), clustering coefficient (CC), heterogeneity of out-degree (HO), and heterogeneity of in-degree (HI).

	Strategy	ER	SF	RT	RR	SW	QS
APL	ORI	INF	INF	4.8536	4.7131	5.1819	206.6615
	UCR	INF	INF	INF	INF	INF	INF
	RER	4.8772	4.3943	4.9356	4.8762	4.9145	5.0733
	NER	6.0785	5.8503	6.3936	6.0961	7.0076	65.9633
ABC	ORI	3875	1351.8	4185.7	3709.4	3849.8	205460
	UCR	4002.3	2543.7	3867.0	3881.2	3912.7	4304.2
	RER	3873.4	3390.9	3931.7	3972.3	3910.6	4069.0
	NER	5073.4	4845.4	5388.2	5091.0	6001.6	64898
CC	ORI	0.0024	0.0526	0.0014	0.0027	0.0020	0.0002
	UCR	0.0033	0.0185	0.003	0.0032	0.0019	0.0021
	RER	0.0019	0.0072	0.0020	0.0020	0.0019	0.0016
	NER	0.1540	0.1572	0.1616	0.1307	0.3329	0.4094
HO	ORI	1.2521	9.3584	1.3645	1.1989	1.1215	4.0503
	UCR	1.1291	4.0055	1.1868	1.1929	1.1211	2.2373
	RER	1.0166	2.0102	1.0217	1.0144	1.0009	1.5408
	NER	1.0115	1.1357	1.0366	1.0070	1.0001	1.2281
HI	ORI	1.2486	9.2805	1.4021	1.2171	1.1311	1.2288
	UCR	1.2401	4.2642	1.3044	1.2238	1.1298	1.2392
	RER	1.0163	2.0038	1.0203	1.0137	1.0106	1.0132
	NER	1.0280	3.3571	1.0371	1.0248	1.0233	1.0173

4.2. Results of Real-World Networks

The real-world networks used by NER were Roget network and ia-email-univ network, and their information is shown in Table 3:

Table 3. Parameters of the two real-world networks.

Network	*N*	*M*
Roget	1022	5075
ia-email-univ	1133	5451

As shown in Figure 8, similarly to the synthetic networks, the controllability robustness of the two networks was improved after NER. Compared with RER and UCR, NER had the best effect on the robustness of network controllability. At the same time, the number of driver nodes of Roget network and ia-email-univ network is not 1. Both NER and RER greatly improved the initial controllability of the networks after 2*N* operations.

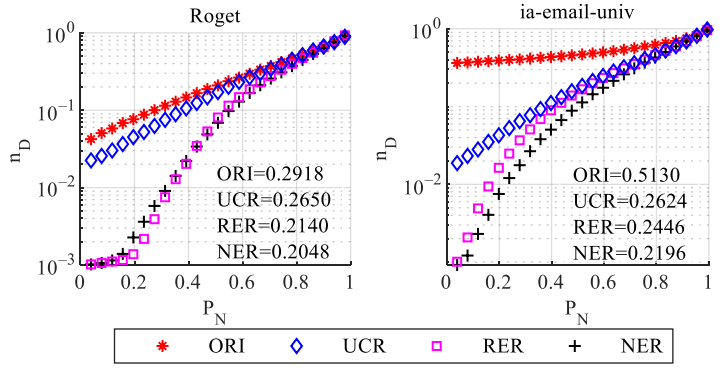

Figure 8. Robustness of structural controllability after edge rectification 2*N* times on real-world networks.

4.3. Discussion

RER can adjust the networks to satisfy ENC, so that the networks gradually approach the optimal controllability robustness. NER can build a NRS in networks, and NRS also satisfies the ENC. Take ER with $N = 1000$ and $M = 4000$ as an example. As shown in Figure 9, NER is similar to RER: the out-degree distribution is concentrated around M/N with the increase in the number of operations. Unlimited NER and RER operations will make the ER extremely homogeneous.

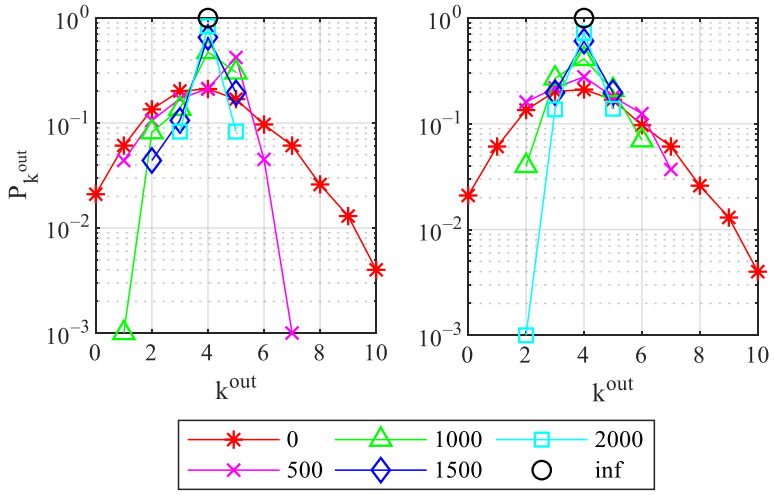

Figure 9. The changes in out-degree distribution under different numbers of iterations for NER and RER. k^{out} represents the out-degree of nodes. $P_{k^{out}}$ represents the proportion of nodes with k^{out} out-degree of all nodes.

NRS is a fixed structure that satisfies ENC. The NRS is shown in Figure 10a, where the edges point to the nearest nodes along the backbone ring direction for each node. The structure satisfying ENC obtained by RER is shown in Figure 10c. Compared with NRS, the edges of each node do not point to a specific node. It can be seen that the NRS constructed by NER is fixed, and the network satisfying ENC by RER may be different. That is because RER randomly selects nodes that make the network not meet ENC and executes edge rectification, and NER selects certain targets.

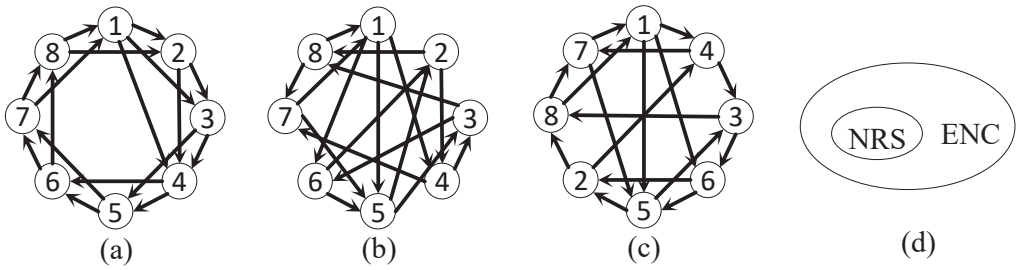

Figure 10. Relationship between NRS and the structure satisfying ENC. (**a**) NRS. (**b**) General structure satisfying ENC. (**c**) Equivalent structure of (**b**). (**d**) Relationship between NRS and ENC.

NRS has a backbone ring. For a network which does not have a backbone ring, NER first builds a backbone ring in the network during the execution process. Therefore, NER can make the number of driver nodes of the network become one quickly. For when NER and RER were executed for ER, SF, RT, RR, Roget network and ia-email-univ network, the numbers of executions required to make the number of driver nodes become one are shown in Figure 11. NER requires a much smaller number of executions than RER. NER builds the backbone ring through maximum matching. It only needs to execute N_D times to build the backbone ring. The original controllability of networks determines the speed of constructing the backbone in networks through NER during execution. A network with

good initial controllability, such as RR, only needs a few operations for the building of a backbone. SF needs more operations for the building of a backbone. Thus, the scale of NRS built by NER in the network is affected. Other effects of network topology on NER need to be further studied.

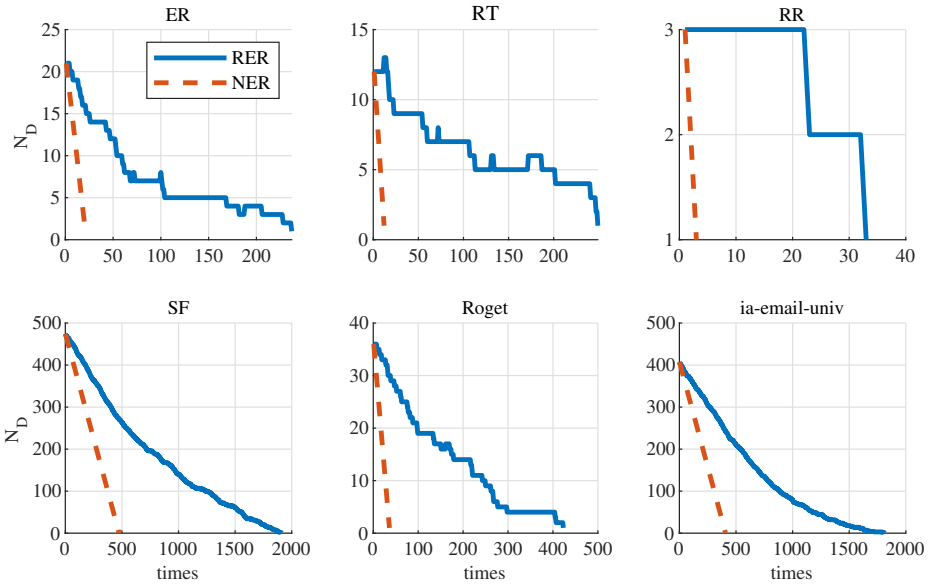

Figure 11. The number of operations required for NER and RER to make the number of driver nodes one. The times axis represents the number of NER and RER.

5. Conclusions

This paper explores how to obtain networks with optimal controllability robustness. Based on the exhaustive search results on small-sized networks, the nested ring structure (NRS) was obtained. The NRS satisfies ENC, which means the degree distribution is extremely uniform. NRS has great ability to resist random attacks, and it is easy to be built in networks. Then, the NER was proposed to construct NRS in networks to improve the robustness of network controllability under random attacks. At the same time, the initial controllability of networks is rapidly improved because of the construction of a backbone. However, the topology of networks is changed greatly after NER optimization, and the number of NER operations can be limited in order to make the network have a NRS completely. In addition, the NRS in networks enhances the local connections and increases the clustering coefficient of the network, and reduces the heterogeneity of degree. NRS can provide a reference for the future designing of network models such as power grids, where the unexpected failure of a substation will not affect the transmission of other circuits.

Author Contributions: Z.Y., conceptualization, formal analysis, investigation, methodology, writing—original draft preparation; J.N., formal analysis, visualization; J.L., investigation, project administration, supervision. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported in part by the National Natural Science Foundation of China (number 62002249) and in part by the Open Project Program of the State Key Lab of CADCG (A2112), Zhejiang University.

Data Availability Statement: Not applicable.

Acknowledgments: This research was supported in part by the National Natural Science Foundation of China (number 62002249) and in part by the Open Project Program of the State Key Lab of CADCG (A2112), Zhejiang University. The author would like to acknowledge the tutor and students for their valuable feedback on the draft to improve the flow and quality of the work.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

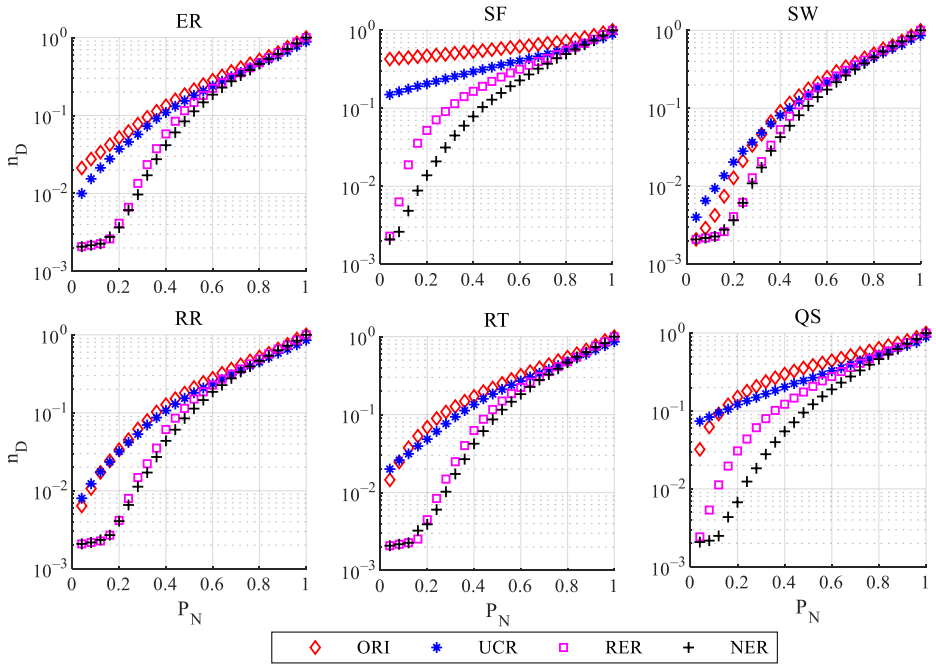

Figure A1. Robustness of the structural controllability of the six original networks with $N = 500$ by rewiring 1000 times. P_N represents the proportion of nodes to be removed. ORI represents the original network without edge rectification. UCR, RER and NER represent the ways of edge rectification.

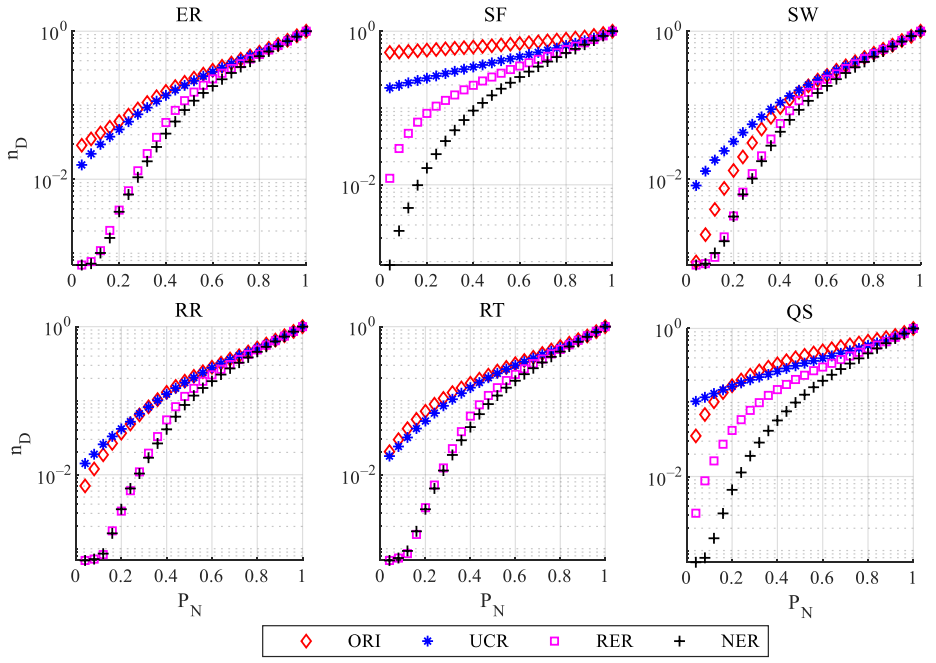

Figure A2. Robustness of structural controllability of the six original networks with $N = 1500$ by rewiring 3000 times. P_N represents the proportion of nodes to be removed. ORI represents original network without edge rectification. UCR, RER and NER represent the ways of edge rectification.

Table A1. Robustness of network controllability with different numbers of edge rectification operations for networks with $N = 500$.

Number of Edge Rectification	Strategy	ER	SF	RT	RR	SW	QS
0		0.2957	0.6186	0.3135	0.2792	0.2593	0.3927
500	UCR	0.2890	0.4891	0.3022	0.2801	0.2643	0.3783
	RER	0.2512	0.4162	0.2560	0.2477	0.2445	0.3190
	NER	0.2442	0.3366	0.2478	0.2418	0.2368	0.2811
750	UCR	0.2837	0.4490	0.2998	0.2799	0.2669	0.3621
	RER	0.2448	0.3542	0.2473	0.2435	0.2422	0.2913
	NER	0.2352	0.2815	0.2368	0.2346	0.2295	0.2538
1000	UCR	0.2831	0.4176	0.2977	0.2798	0.2672	0.3487
	RER	0.2417	0.3050	0.2436	0.2416	0.2406	0.2710
	NER	0.2241	0.2549	0.2256	0.2243	0.2236	0.2303

Table A2. Robustness of network controllability with different numbers of edge rectification operations for networks with $N = 1500$.

Number of Edge Rectification	Strategy	ER	SF	RT	RR	SW	QS
0		0.2955	0.6709	0.3130	0.2796	0.2591	0.4284
1500	UCR	0.2895	0.5242	0.3028	0.2809	0.2640	0.4166
	RER	0.2512	0.4524	0.2562	0.2476	0.2439	0.3566
	NER	0.2437	0.3606	0.2482	0.2417	0.2354	0.2941
2250	UCR	0.2885	0.4798	0.3004	0.2796	0.2669	0.3989
	RER	0.2439	0.3856	0.2465	0.2433	0.2419	0.3235
	NER	0.2355	0.2926	0.2368	0.2339	0.2291	0.2618
3000	UCR	0.2871	0.4428	0.2971	0.2800	0.2687	0.3811
	RER	0.2423	0.3301	0.2425	0.2412	0.2403	0.2951
	NER	0.2238	0.2632	0.2249	0.2238	0.2231	0.2332

References

1. Barabási, A.L. *Network Science*; Cambridge University Press: Cambridge, UK, 2016.
2. Newman, M.E. *Networks: An Introduction*; Oxford University Press: London, UK, 2010.
3. Chen, G.R.; Wang, X.F.; Li, X. *Fundamentals of Complex Networks: Models, Structures and Dynamics*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
4. Chen, G.R.; Lou Y. *Naming Game:Models, Simulation and Analysis*; Springer International Publishing: Cham, Switzerland, 2019.
5. Yang, L.X.; Yang, X.F.; Liu, J.M. Epidemics of computer viruses: A complex-network approach. *Appl. Math. Comput.* **2013**, *219*, 8705–8717.
6. Xu, Z.W.; Harriss, R. Exploring the structure of the US intercity passenger air transportation network: A weighted complex network approach. *GeoJournal* **2008**, *73*, 87–102.
7. Buldyrev, S.V.; Parshani, R.; Paul, G. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028.
8. Cherifi, H.;Palla, G.;Szymanski, B.K.; Lu, X. On community structure in complex networks: Challenges and opportunities. *Appl. Netw. Sci.* **2019**, *4*, 117.
9. Liu, X.;Chen, T. Synchronization of complex networks via aperiodically intermittent pinning control. *IEEE Trans. Autom. Control* **2015**, *60*, 3316–3321.
10. Shi, D.H.; Lü, L. Chen G.R. Totally homogeneous networks. *Natl. Sci. Rev.* **2019**, *6*, 962–969.
11. Fan, T.; Lü, L.; Shi, D.H. Towards the cycle structures in complex network: A new perspective. *arXiv* **2019**, arXiv:1903.01397.
12. Zhao, P.; Han, J. On graph query optimization in large networks. *Proc. VLDB Endow.* **2010**, *3*, 340–351.
13. Lou, Y.; He, Y.D.; Wang L. Knowledge-Based Prediction of Network Controllability Robustness. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**, *33*, 5739–5750.
14. Menichetti, G.; Dall'Asta, L.; Bianconi, G. Network controllability is determined by the density of low in-degree and out-degree nodes. *Phys. Rev. Lett.* **2014**, *113*, 078701.
15. Zhang, Y.; Zhou, T. Controllability analysis for a networked dynamic system with autonomous subsystems. *IEEE Trans. Autom. Control* **2016**, *62*, 3408–3415.
16. Xiang, L.Y.; Chen, F.; Ren W. Advances in network controllability. *IEEE Circuits Syst. Mag.* **2019**, *19*, 8–32.

17. Guang-Ren, D. High-order system approaches: II. Controllability and full-actuation. *Acta Autom. Sin.* **2020**, *46*, 1571–1581.
18. Lou, Y.; He, Y.D.; Wang L. Predicting Network Controllability Robustness: A Convolutional Neural Network Approach. *IEEE Trans. Cybern.* **2022**, *52*, 4052–4063.
19. Liu, Y.Y.; Slotine, J.J.;Barabási, A.L. Controllability of complex networks. *Nature* **2011**, *473*, 167–173.
20. Yuan, Z.;Zhao, C.; Di, Z.;Wang, W.X. ;Lai, Y.C. Exact controllability of complex networks. *Nat. Commun.* **2013**, *4*, 2447.
21. Pósfai, M.; Liu, Y.Y.; Slotine J.J. Effect of correlations on network controllability. *Sci. Rep.* **2013**, *3*, 1067.
22. Liu, Y.Y.; Slotine, J.J.; Barabási, A.L. Control centrality and hierarchical structure in complex networks. *PLoS ONE* **2012**, *7*, e44459.
23. Xiao, Y.D.; Lao, S.Y.; Hou, L.L. Optimization of robustness of network controllability against malicious attacks. *Chin. Phys. B* **2014**, *23*, 118902.
24. Chan, H.; Akoglu, L. Optimizing network robustness by edge rewiring: A general framework. *Data Min. Knowl. Discov.* **2016**, *30*, 1395–1425.
25. Louzada, V.H.; Daolio, F.; Herrmann, H.J. Smart rewiring for network robustness. *J. Complex Netw.* **2013**, *1*, 150–159.
26. Herrmann, H.J.; Schneider, C.M.; Moreira, A.A.; Onion-like network topology enhances robustness against malicious attacks. *J. Stat. Mech. Theory Exp.* **2011**, *2011*, P01027.
27. Wang, L.F.; Zhao, G.T.; Kong, Z. Controllability and Optimization of Complex Networks Based on Bridges. *Complexity* **2020**, *2020*, 6695026.
28. Lou, Y.; Wang, L.; Tsang, K.F. Towards optimal robustness of network controllability: An empirical necessary condition. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2020**, *67*, 3163–3174.
29. Lou, Y.; Wang, L.; Chen, G.R. Toward Stronger Robustness of Network Controllability: A Snapback Network Model. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2018**, *65*, 2983–2991.
30. Lou, Y.; Wang, L.; Chen, G.R. Enhancing Controllability Robustness of q-Snapback Networks through Redirecting Edges. *Research* **2019**, *2019*, 7857534.
31. Erdős, P.; Rényi, A. On the strength of connectedness of a random graph. *Acta Math. Hung.* **1961**, *12*, 261–267.
32. Pu, C.L.; Pei, W.J.; Michaelson, A. Robustness analysis of network controllability. *Phys. A Stat. Mech. Its Appl.* **2012**, *391*, 4420–4425.
33. Chen, G.R.; Lou, Y.; Wang, L. A comparative study on controllability robustness of complex networks. *IEEE Trans. Circuits Syst. II Express Briefs* **2019**, *66*, 828–832.
34. Newman, M.E.J.; Watts, D.J. Renormalization group analysis of the small-world network model. *Phys. Lett. A* **1999**, *263*, 341–346.
35. Rossi, R.; Ahmed, N. The network data repository with interactive graph analytics and visualization. In Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence, Austin, TX, USA, 25–30 January 2015.