

Article

Influence of Removing Leaf Node Neighbors on Network Controllability

Chengpei Wu ^{1,2}, Siyi Xu ^{1,2}, Zhuoran Yu ^{1,2} and Junli Li ^{1,2,*}

¹ School of Computer Science, Sichuan Normal University, Chengdu 610068, China; chengpei.wu@hotmail.com (C.W.); xusiyi1999@163.com (S.X.); yuzhuor@foxmail.com (Z.Y.)

² Visual Computing and Virtual Reality Key Laboratory of Sichuan, Sichuan Normal University, Chengdu 610068, China

* Correspondence: lijunli@sicnu.edu.cn

Abstract: From the perspective of network attackers, finding attack sequences that can cause significant damage to network controllability is an important task, which also helps defenders improve robustness during network constructions. Therefore, developing effective attack strategies is a key aspect of research on network controllability and its robustness. In this paper, we propose a Leaf Node Neighbor-based Attack (LNNA) strategy that can effectively disrupt the controllability of undirected networks. The LNNA strategy targets the neighbors of leaf nodes, and when there are no leaf nodes in the network, the strategy attacks the neighbors of nodes with a higher degree to produce the leaf nodes. Results from simulations on synthetic and real-world networks demonstrate the effectiveness of the proposed method. In particular, our findings suggest that removing neighbors of low-degree nodes (i.e., nodes with degree 1 or 2) can significantly reduce the controllability robustness of networks. Thus, protecting such low-degree nodes and their neighbors during network construction can lead to networks with improved controllability robustness.

Keywords: controllability; controllability robustness; undirected networks; attack strategy



Citation: Wu, C.; Xu, S.; Yu, Z.; Li, J. Influence of Removing Leaf Node Neighbors on Network Controllability. *Entropy* **2023**, *25*, 945. <https://doi.org/10.3390/e25060945>

Academic Editor: Alessandro Pluchino

Received: 8 May 2023

Revised: 13 June 2023

Accepted: 13 June 2023

Published: 15 June 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Complex networks have developed rapidly over the past two decades [1]. There are many real-world systems that can be modeled as complex networks, with a large number of nodes and edges. The study of networks can help us understand corresponding complex systems. For example, social networks can help us understand the ways in which humans interact and how information spreads in society; transportation networks can help us study the flow and congestion of traffic in cities. The controllability of a network is a crucial factor, as control networks are designed to serve people [2,3]. In this context, controllability refers to the ability of a dynamical network to be guided by external inputs from any initial state to any desired target state within a finite duration of time under an admissible control input.

Recently, failures and attacks on complex networks have become more frequent and severe [4–8]. When failures and attacks occur, they are removed in the form of node or edge removals. On node removals, the target node and the edges previously connected to the node will be removed, while on edge removals, only the target edges will be disconnected. Network attacks are typically categorized into two types: random and malicious. Random attacks refer to the uniform random selection of attack targets, while malicious attacks choose the most effective targets to attack. Malicious attacks typically have a better effect than random attacks, but they also consume more computation time. During malicious attacks, the most destructive target is selected for attacking; such target choices are usually based on the centrality of nodes. For example, the node with the highest degree is attacked firstly or the edge with the highest betweenness is preferentially removed. Besides degree and betweenness, commonly used measures of node importance include

closeness [9], Katz centrality [10], neighborhood similarity [11], branch weighting [12], structural holes [13], and so on. Many malicious attack models have been proposed; the hierarchical structure of a directed network enables a random upstream (or downstream) attack on the network controllability, which results in a more destructive attack strategy than random attacks [14]. In addition, the module-based attack strategy [15,16] aims at attacking the nodes with inter-community edges that are crucial to maintain connectivity among communities.

In addition, nodes can be categorized as critical or non-critical based on their impact on network controllability when removed. Removing critical nodes can significantly reduce network controllability [6], so they should be protected during network construction to enhance controllability robustness. Bridges, a type of edge in networks, can also be targeted for removal to decrease network controllability [17]. Many deep learning and optimization methods can be used to find such hidden patterns and key roles of networks; the proposed Finder framework, which employs reinforcement learning, offers a unified approach for identifying a group of nodes that can destroy network function to the greatest extent after removals [18]. Deep learning models are used to predict network robustness [19–22]; evolutionary algorithms are utilized for network attacks [23,24].

The research on network attacks aims to enhance the robustness of networks from the perspective of attackers, enabling them to better withstand attacks when constructing networks. One effective approach to improving the controllability robustness of networks is to protect bridges, as they play a critical role in network connectivity. Protecting critical nodes and edges during network construction is also a viable strategy for enhancing controllability robustness [6]. Studies have shown that three-ring and four-ring structures in networks are beneficial for controllability robustness [25], which suggests that networks with random triangle and random quadrilateral structures tend to exhibit good controllability robustness.

The structural controllability of the network can be evaluated by identifying the maximum matching of the network to determine the minimum number of external control inputs required as driver nodes [4]. However, this approach is only suitable for directed networks and is challenging to apply to large-scale networks. To address this issue, the exact controllability framework was proposed, which can be utilized for all large-scale sparse networks [26].

Controllability robustness can be measured using two approaches: *A priori* measure and *A posteriori* measure. The *A priori* measure calculates network features in a single calculation, while the *A posteriori* measure simulates the change in network controllability curve under attack. Although the *A posteriori* measure is more accurate, it can be computationally expensive, especially for large-scale networks. Recently, deep learning has emerged as a promising approach to measure network robustness accurately and efficiently, providing a less time-consuming alternative to simulation-based methods [19,21,22,27,28].

The selection of literature reviewed in this paper was based on the following criteria: (1) Relevance to the research objective: we screened literature that directly related to our research topic. (2) Credibility and authority: we evaluated the credibility and authority of the literature. We specifically focused on articles published in reputable journals, conference proceedings, and reports from authoritative research organizations. (3) Time range: we limited the articles to recent publications as much as possible to ensure they represented the latest advancements in the field. By employing these criteria, we aimed to ensure the selection of the most relevant, credible, and recent literature to support the research objectives.

Overall, this paper presents an attack strategy for undirected network controllability. The main contributions are:

- (1) A novel attack strategy is proposed, which can effectively disrupt the controllability of undirected networks.
- (2) The impact of removing nodes with degree 1 and 2 on network controllability is analyzed, revealing that nodes with low degree are not beneficial to the robustness of network controllability.

- (3) The findings provide valuable insights for identifying key nodes and designing networks with improved controllability robustness in future research.

The rest of this paper is organized as follows: Section 2 introduces the preliminary concepts of controllability and controllability robustness; Section 3 illustrates in detail the proposed attack model LNNA; Section 4 demonstrates the experimental results on synthetic and real-world networks; and Section 5 concludes this paper.

2. Network Controllability and Controllability Robustness

The robustness of network controllability is mainly concerned with the change in controllability when the network is attacked [29]. Controllability robustness reflects the ability of the network to resist attacks, from the perspective of attackers, which can also be the evaluation index of attack performance, namely, the worse the robustness, the better the attack model. Network controllability is measured by the density of driver nodes n_D ,

$$n_D = \frac{N_D}{N} \quad (1)$$

where N_D represents the number of driver nodes required to maintain network controllability and N represents the total number of network nodes. The minimum value of n_D is $\frac{1}{N}$, and the maximum value is 1. A smaller value of n_D indicates better network controllability, while a larger value of n_D indicates worse network controllability. According to the minimum-inputs theorem [4], for directed networks, N_D can be obtained by the number of unmatched nodes for a directed network:

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

where $|E^*|$ is the size of maximum matching. As for exact controllability [26], N_D is calculated by:

$$N_D = \max\{1, N - \text{rank}(A)\} \quad (3)$$

where $\text{rank}(A)$ is the rank of the adjacency matrix A . For node-removal attacks, the controllability robustness of the network can be measured by the controllability curve, which is calculated as follows:

$$n_D(i) = \frac{N_D(i)}{N - i}, i = 0, 1, \dots, N - 1, \quad (4)$$

where $N_D(i)$ the number of driver nodes needed to maintain network controllability after removing a total of i nodes, N is the size of the original network, N_D is calculated by using the exact controllability framework as Equation (3), which applies to large and sparse undirected networks, n_D records the changes in network controllability after each node is removed. The overall measure of controllability robustness can be obtained by averaging controllability curves as follows:

$$R_N = \frac{1}{N - 1} \sum_{i=1}^{N-1} n_D(i), \quad (5)$$

where $n_D(i)$ is the structural controllability of the remaining network after i nodes are removed. The network controllability robustness can be evaluated by R_N , a smaller R_N indicates better controllability robustness, while a larger R_N indicates worse controllability robustness. For an attack model, a better controllability robustness indicates a worse attack performance.

3. Leaf Node Neighbor-Based Attack Strategy

The removal of different nodes in networks has different impacts on the controllability of networks. Leaf nodes, which are the nodes with a degree of 1, are most likely driver

nodes in the network. If the only neighbor of a leaf node is removed, the leaf node will become an isolated node and the number of connected components of the network will increase. Furthermore, after the neighbor of a leaf node is attacked, which is connected to many leaf nodes, all the leaf nodes connected to it will become drive nodes. Therefore, the neighbors of a leaf node are important for controllability attacks, and the number of leaf nodes connected by that neighbor node is also an important reference. The above ideas are applied to the following attack strategy design; the following subsections analyze in detail the impacts of removing leaf node neighbors on network controllability.

3.1. Leaf Node Neighbor-Based Attack Strategy

As neighbors of leaf nodes can be removed to reduce the controllability of a network, a leaf node neighbor-based attack (LNNA) strategy is proposed. Before proposing the algorithm, there are two necessary concepts, k -neighbor node and k -neighbor degree, which are pre-defined, where k -neighbor node is a neighbor of a node with degree k , and k -neighbor degree for a node is the number of neighbors with degree k . The proposed LNNA is based on the above concepts and is described in detail in Algorithm 1.

Algorithm 1 Leaf Node Neighbor-based Attack Strategy

Input: a network G with N nodes

Output: index t of target node to be attacked

```

1:  $degrees \leftarrow \{\}$ 
2:  $neighbors \leftarrow \{\}$ 
3: // get node degrees and neighbors
4: for  $i = 1$  to  $N$  do
5:    $d \leftarrow get\_degree(node_i)$ 
6:   if  $d \neq 0$  then
7:      $degrees[i] \leftarrow d$ 
8:      $neighbors[i] \leftarrow get\_neighbor\_indexes(node_i)$ 
9:   end if
10: end for
11: if  $degrees.size() \neq 0$  then
12:   // get the nodes and their neighbors with smallest degree  $k$ , generally,  $k$  equals to 1
13:    $k \leftarrow degrees.minimum()$ 
14:    $k\_nodes \leftarrow \{\}$ 
15:    $k\_neighbors \leftarrow \{\}$ 
16:   for  $j = degrees.keys()$  do
17:     if  $degrees[j] == k$  then
18:        $k\_nodes.insert(j)$ 
19:        $k\_neighbors.insert(neighbors[j])$ 
20:     end if
21:   end for
22:    $k\_neighbor\_degrees \leftarrow Array(k\_neighbors.size())$ 
23:   for  $j = 1$  to  $k\_neighbors.size()$  do
24:     for  $neighbor\_id = get\_neighbor\_indexes(k\_neighbors[j])$  do
25:       if  $neighbor\_id$  in  $k\_nodes$  then
26:          $k\_neighbor\_degrees[j] \leftarrow k\_neighbor\_degrees[j] + 1$ 
27:       end if
28:     end for
29:   end for
30:    $t \leftarrow k\_neighbors[argmax(k\_neighbor\_degrees)]$ 
31: else
32:    $t \leftarrow random\_integer(1, N)$ 
33: end if
34: return  $t$ 

```

As shown in Algorithm 1, LNNA usually starts from the neighboring node of leaf nodes, i.e., 1-neighbors. When attacking the 1-neighbors, the attack target is determined based on the number of leaf nodes connected to these nodes, i.e., the 1-neighbor degree. The node with the highest 1-neighbor degree among the 1-neighbors will be attacked. When there are no leaf nodes in the network, LNNA will choose nodes to attack from the 2-neighbors. Similarly, the node with the highest 2-neighbor degree among the 2-neighbors will be selected as the target. This process continues recursively.

In terms of time complexity, for each attack, finding neighbors of each node is $O(N^2)$, N is the number of nodes; finding and getting the smallest k -neighbors is $O(N)$; getting k -neighbor degrees is $O(KN)$, K is the number of k -neighbors, $K < N$; thus, the total time complexity is $\max\{O(N^2), O(N), O(KN)\} = O(N^2)$. For typical malicious attack methods, namely, degree- (DEG), betweenness- (BET), closeness- (CLO) based attacks, the time complexity comparison is listed in Table 1. For degree-based attacks, getting the degree of each node is $O(N^2)$, similar to finding neighbors of each node; for a betweenness-based attack, getting the betweenness of each node is $O(N^3)$ when using the Floyd–Warshall algorithm; for a closeness-based attack, computing time of closeness is $O(N(M + N))$, and M is the number of edges.

Table 1. Time complexity of attack methods.

Method	LNNA	DEG	BET	CLO
Time complexity	$O(N^2)$	$O(N^2)$	$O(N^3)$	$O(N(M + N))$

3.2. Influence of Leaf Node Neighbor Failures

An algorithm that targets the neighbors of low-degree nodes (i.e., leaf nodes) with a node attack has been developed in Section 3.1. In this subsection, we also provide a mathematical proof detailing why attacking the neighbors of leaf nodes is effective and leads to an increase in the number of driver nodes.

Theorem 1. Let A_N be the adjacency matrix of a network, and A_{N-1} be the adjacency matrix after removing a node V_r . $\text{rank}(A_N) = \text{rank}(A_{N-1}) + 2$, if the following condition holds: V_r is the only neighbor of a leaf node V_l .

Proof. The adjacency matrix A_N and A_{N-1} can be represented as follows:

$$A_N = \begin{bmatrix} 0 & \vec{0}' & 1 \\ \vec{0} & D & \vec{a}' \\ 1 & \vec{a}' & 0 \end{bmatrix}, A_{N-1} = \begin{bmatrix} 0 & \vec{0}' \\ \vec{0} & D \end{bmatrix},$$

As the permutation invariance of adjacency matrix, the first row (column) of A_N represents V_l , the last row (column) of A_N represents V_r ; it is clear that

$$\text{rank}(D) = \text{rank}(A_{N-1}) = \text{rank}(A_N) - 2$$

□

Theorem 2. Let N_D be the number of driver nodes in a network, and N'_D be the number of driver nodes on the network after removing a leaf node neighbor. $N'_D = N_D + 1$, if the following condition holds: $\text{rank}(A_N) < N$.

Proof. If $\text{rank}(A_N) < N$, then, $\text{rank}(A_{N-1}) = \text{rank}(A_N) - 2 < N - 2$. Therefore, the following equation holds:

$$\begin{aligned}
N_D &= \max\{1, N - \text{rank}(A_N)\} \\
&= N - \text{rank}(A_N) \\
&= N - \text{rank}(A_{N-1}) - 2 \\
&= [(N - 1) - \text{rank}(A_{N-1})] - 1 \\
&= \max\{1, (N - 1) - \text{rank}(A_{N-1})\} - 1 \\
&= N'_D - 1
\end{aligned}$$

□

Theorem 3. Let N_D be the number of driver nodes in a network, and N'_D be the number of driver nodes on the network after removing a leaf node neighbor. $N'_D = N_D = 1$, if the following condition holds: $\text{rank}(A_N) = N$.

Proof. If $\text{rank}(A_N) = N$, then $N_D = \max\{1, N - \text{rank}(A_N)\} = 1$, the following equation holds:

$$\text{rank}(A_{N-1}) = \text{rank}(A_N) - 2 = N - 2, N'_D = \max\{1, (N - 1) - \text{rank}(A_{N-1})\} = 1$$

□

According to Theorem 1, 2, and 3, removing the neighbor of a leaf node from the network increases or maintains the total number of driver nodes. From Equations (1) and (4), we can find that the more driver nodes there are, the worse controllability the network has.

4. Experimental Studies

LNNA is applied to three kinds of synthetic networks and real networks. In order to verify its effectiveness, the performance of LNNA was compared with feature-based attacks such as degree-, betweenness-, and closeness-based attacks. The main focus of this paper is to investigate the impact of attacking nodes with the lowest degree, excluding isolated nodes, on network controllability. Specifically, the study explores the effects of removing neighbors of leaf nodes on network controllability.

The three synthetic networks are Erdős-Rényi (ER) random-graph [30], Generic scale-free (SF) network [31], and Newman-Watts small-world (SW) network [32]. The real-world networks are *econ-mahindas* and *soc-wiki-Vote*; all networks are undirected. The number of nodes are $N = 500$ and $N = 1000$; the average degree $\langle k \rangle = 3, 5$, and 10 , respectively. In order to reduce the influence of randomness, 30 random instances are generated for each network.

4.1. Results on Synthetic Networks for Different Average Degrees

Liu et al. [4] suggested that controlling sparse heterogeneous networks can be challenging and that such networks tend to have poor network controllability and robustness. Conversely, dense homogeneous networks are easier to control and have better network controllability and robustness. Moreover, networks with higher average degrees have more redundant edges, which help maintain the core structure of the network and make it less susceptible to destruction, resulting in better network controllability and robustness.

As shown in Figure 1, for ER and SW networks with an average degree of 3, LNNA can effectively disrupt network controllability from the beginning of attacks. When the average degree is 5, for the degree- (DEG), betweenness- (BET), closeness- (CLO) based attacks on ER networks, the controllability of ER networks begins to decrease significantly after about 20% of nodes are removed, and for the SW networks, the threshold proportion is 40%. However, LNNA can significantly reduce the controllability of networks from the beginning of the attacks. For SF networks, there is no significant difference between different attacks, since the topology of SF networks makes the network robust on controllability, and nodes that can disrupt the network controllability are easy to find. When $\langle k \rangle = 10$, for ER

networks, the three feature-based attacks rapidly reduce the controllability of the network when more than 40% of the nodes are removed. For SW networks, the ratio is around 50%. For SF networks, LNNA is slightly better than other attacks, because with the increase in average degree, the network controllability robustness is improved. Overall, as shown in Table 2, LNNA has the best attack effect on the three synthetic networks with different average degrees;

4.2. Results on Synthetic Networks for Different Network Sizes

The size of a network is typically defined as the number of nodes in the network. Large-scale networks tend to be more complex and may exhibit a variety of structures, and the controllability robustness of networks can vary across different scales. Moreover, in terms of attack strategies, networks with more nodes require higher computational costs relative to smaller networks. As shown in Figure 2, the effect of different attacks on the three synthetic networks is similar when the average degree is 5, regardless of network size (i.e., 500, 1000, or 1500 nodes). However, LNNA shows better attack performance on ER and SW networks compared to other attack methods, while no significant difference is observed in SF networks. Table 3 also shows that when the average degree is 5, LNNA performs the best on the three networks with 500, 1000, and 1500 nodes.

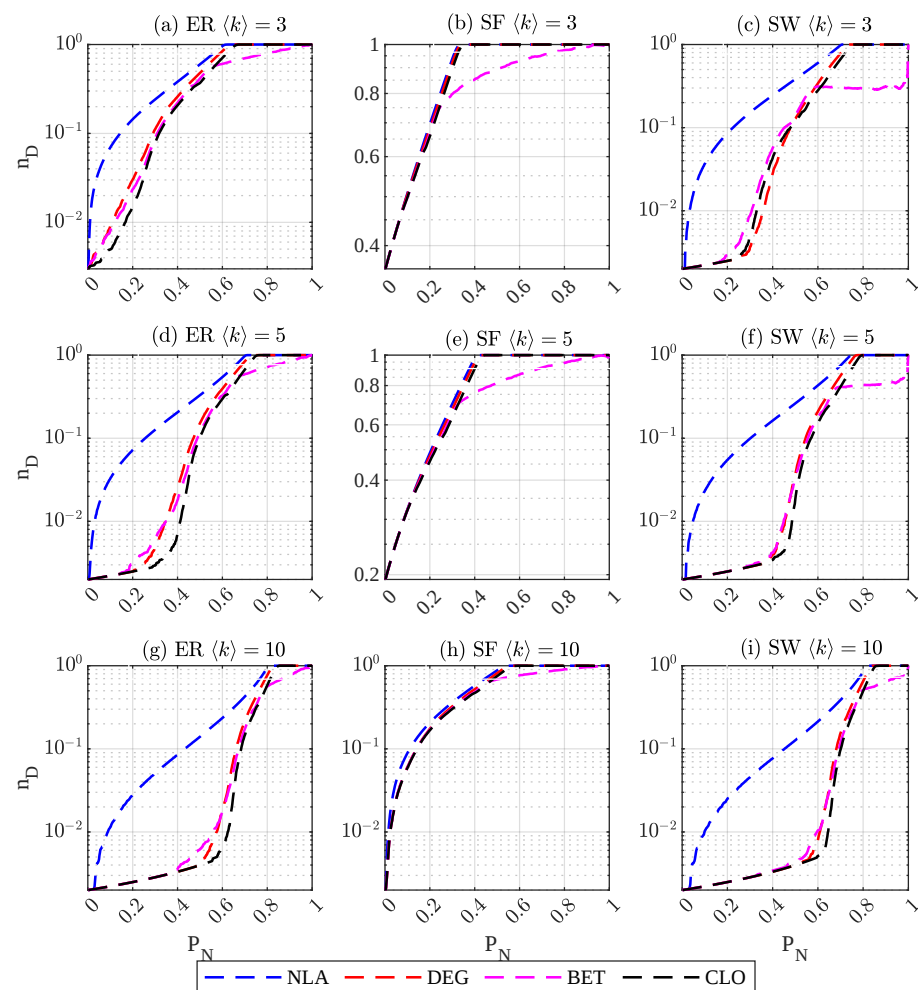


Figure 1. Controllability robustness of networks with $N = 1000$.

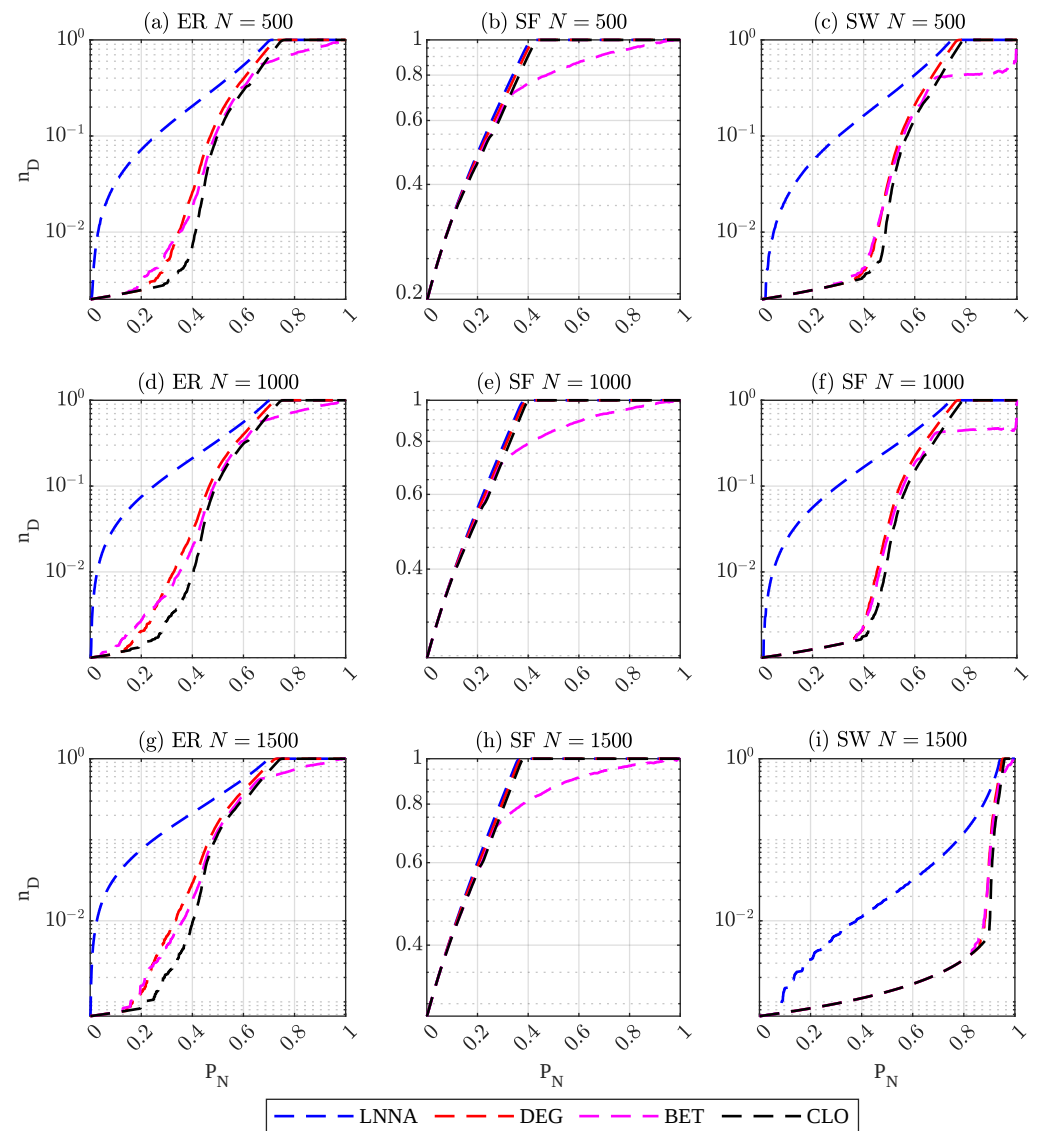


Figure 2. Controllability robustness of networks with $\langle k \rangle = 5$.

Table 2. Robustness of network controllability with different average degrees; the values are calculated by Equation (5).

Networks	$\langle k \rangle$	LNNA	DEG	BET	CLO
ER	3	0.5893	0.5258	0.4274	0.4921
	5	0.4759	0.3942	0.3139	0.3619
	7	0.3382	0.2537	0.2012	0.2299
SF	3	0.8836	0.8808	0.8259	0.8759
	5	0.8085	0.8027	0.7322	0.7938
	7	0.6636	0.6421	0.5683	0.6273
SW	3	0.4961	0.382	0.1612	0.3656
	5	0.4324	0.3354	0.1802	0.3073
	7	0.3236	0.2375	0.166	0.2173

Table 3. Robustness of network controllability with different network sizes; the values are calculated by Equation (5).

Network	N	LNNA	DEG	BET	CLO
ER	500	0.4759	0.3942	0.3139	0.3619
	1000	0.4803	0.3963	0.318	0.3654
	1500	0.4815	0.3966	0.3211	0.3676
SF	500	0.8085	0.8027	0.7322	0.7938
	1000	0.8357	0.8312	0.765	0.8242
	1500	0.8519	0.848	0.787	0.8422
SW	500	0.4324	0.3354	0.1802	0.3073
	1000	0.4347	0.3368	0.1788	0.3066
	1500	0.1238	0.072	0.0582	0.061

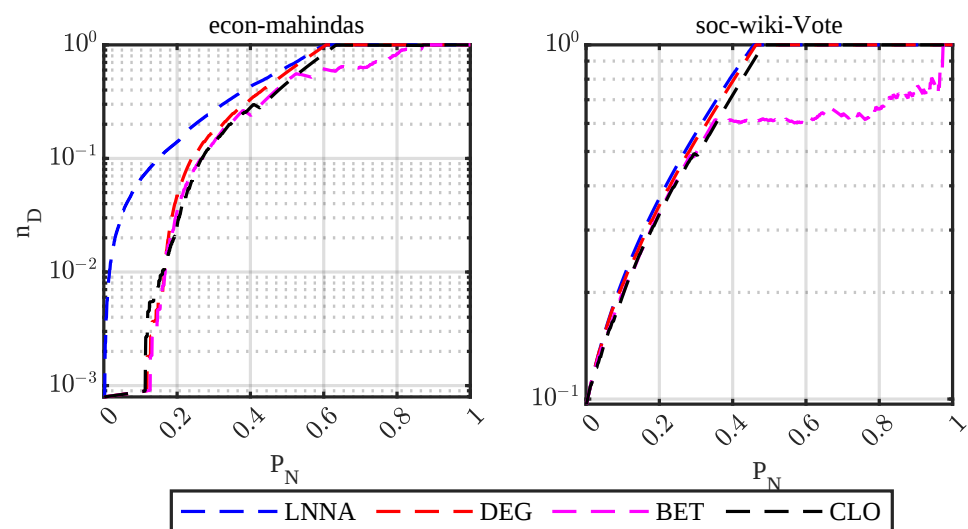
4.3. Results on Real-World Networks

LNNA is applied to two real-world networks, called *econ-mahindas* and *soc-wiki-Vote* [33]. The information of networks is shown in Table 4.

Table 4. Information of real-world networks.

Network	N	M
econ-mahindas	1258	7682
soc-wiki-Vote	889	2914

As shown in Figure 3, for the *econ-mahindas* network, the attack effect of LNNA is obviously better than that of other attack strategies. For the *soc-wiki-Vote* network, the attack effect of LNNA is slightly better than other strategies, but there is no significant difference. These results are consistent with those obtained on synthetic networks. Furthermore, for networks with good controllability robustness, LNNA is more destructive to the network controllability.

**Figure 3.** Controllability robustness of real-world networks.

4.4. Attack Process Discussion

Figure 4 illustrates types of the selected nodes during the LNNA. When approximately 70% of the nodes are removed, only isolated nodes remain in the network.

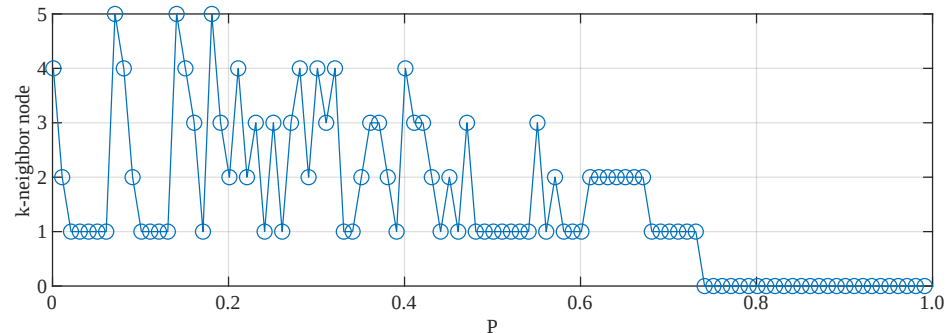


Figure 4. Visualization of targeted nodes in the attack process of LNNA.

Figure 5 illustrates the proportion of different nodes removed by different networks under LNNA. It can be observed that the proportion of nodes decreases as the k of k -neighbor increases. Apart from isolated nodes, the largest proportion represents 1-neighbor nodes, which refers to the neighbor of a leaf node. When a k -neighbor node is attacked, a $(k - 1)$ -neighbor node is generated. In the case of ER and SW networks, 1-neighbor nodes account for approximately 30% and 25%, respectively, and the damage to network controllability is significant. For the SF network, it can be seen that the attacked nodes are 1-neighbor nodes, accounting for about 40%. Subsequently, only isolated nodes remain in the network, indicating that the SF network is vulnerable to attack.

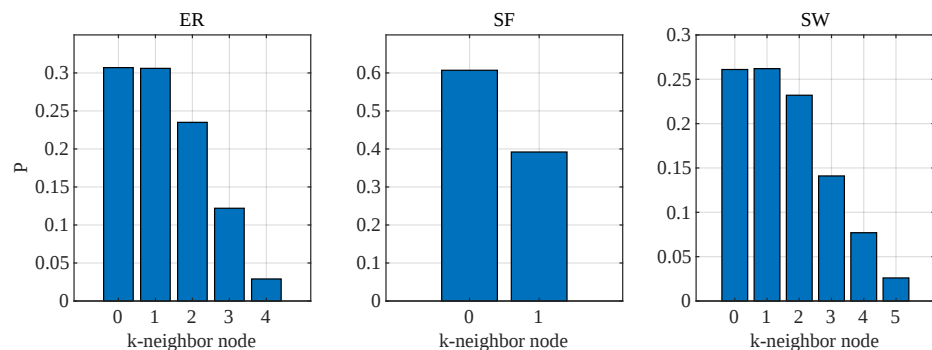


Figure 5. The proportion of attacked node types in the three networks under LNNA, $N = 1000$ and $\langle k \rangle = 5$.

5. Conclusions

In order to investigate the controllability robustness of networks from the perspective of attacks, this paper mainly examines the destructive impact of the neighbor nodes of a node with low degree on network controllability. We proposed an attack strategy targeted on leaf node neighbors, named LNNA, and introduced the defined concepts of k -neighbor nodes and k -neighbor degrees. First, we investigated the role of neighboring nodes of leaf nodes in network controllability and the changes that occur in network controllability when these nodes are removed. Then, we defined the concepts of k -neighbor nodes and k -neighbor degrees, which denote the neighboring nodes of a node with degree k , and the degree of k -neighbor node itself. Based on the exploration, we proposed an attack strategy targeting these nodes to achieve maximum disruption of network controllability; the attack strategy prioritizes attacking the neighbor node of a node with the lowest degree, except for isolated nodes. In a network, if the k -neighbor nodes are attacked, the $(k - 1)$ -neighbor nodes will be generated, and this process continues until 1-neighbor nodes appear,

which will then be attacked. Simulated experiments on synthetic and real-world networks demonstrate that the proposed LNNA performs better than degree-, betweenness-, and closeness-based attacks. This suggests that the presence of low-degree nodes in networks is not conducive to network controllability robustness. In the future, when designing networks with good controllability robustness, it is advisable to make the network more homogeneous to avoid the presence of a large number of low-degree neighbor nodes, such as 1-neighbor nodes and 2-neighbor nodes.

Author Contributions: Conceptualization, software, investigation, methodology, writing—original draft preparation, C.W. and Z.Y.; formal analysis, visualization, S.X.; investigation, project administration and supervision, J.L. 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.

Institutional Review Board Statement: Not applicable.

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.

References

- Chen, G.; Wang, X.; Li, X. *Fundamentals of Complex Networks: Models, Structures and Dynamics*, 2nd ed.; John Wiley & Sons: Hoboken, NJ, USA, 2014.
- 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. [[CrossRef](#)] [[PubMed](#)]
- Zhang, Y.; Zhou, T. Controllability Analysis for a Networked Dynamic System with Autonomous Subsystems. *IEEE Trans. Autom. Control* **2017**, *62*, 3408–3415. [[CrossRef](#)]
- Liu, Y.Y.; Slotine, J.J.; Barabási, A.L. Controllability of Complex Networks. *Nature* **2011**, *473*, 167–173.
- Xiao, Y.D.; Lao, S.Y.; Hou, L.L.; Bai, L. Optimization of robustness of network controllability against malicious attacks. *Chin. Phys. B* **2014**, *23*, 118902. [[CrossRef](#)]
- Lou, Y.; Wang, L.; Chen, G. A Framework of Hierarchical Attacks to Network Controllability. *Commun. Nonlinear Sci. Numer. Simul.* **2021**, *98*, 105780. [[CrossRef](#)]
- Wandelt, S.; Lin, W.; Sun, X.; Zanin, M. From random failures to targeted attacks in network dismantling. *Reliab. Eng. Syst. Saf.* **2022**, *218*, 108146. [[CrossRef](#)]
- Li, S.; Liu, W.; Wu, R.; Li, J. An adaptive attack model to network controllability. *Reliab. Eng. Syst. Saf.* **2023**, *235*, 109252. [[CrossRef](#)]
- Borgatti, S.P. Centrality and network flow. *Soc. Netw.* **2005**, *27*, 55–71. [[CrossRef](#)]
- Katz, L. A new status index derived from sociometric analysis. *Psychometrika* **1953**, *18*, 39–43. [[CrossRef](#)]
- Ruan, Y.-R.; Yang, L.S.; Wang, J.-D.; Bai, L.; Chen, L.D. Node importance measurement based on neighborhood similarity in complex network. *Acta Phys. Sin.* **2017**, *66*, 038902. [[CrossRef](#)]
- Šimon, M.; Luptáková, I.D.; Huraj, L.; Host'ovecký, M.; Pospíchal, J. Combined Heuristic Attack Strategy on Complex Networks. *Math. Probl. Eng.* **2017**, *2017*, 6108563. [[CrossRef](#)]
- Yang, H.; An, S. Critical Nodes Identification in Complex Networks. *Symmetry* **2020**, *12*, 123. [[CrossRef](#)]
- Liu, Y.Y.; Slotine, J.J.; Barabási, A.L. Control Centrality and Hierarchical Structure in Complex Networks. *PLoS ONE* **2012**, *7*, e44459. [[CrossRef](#)]
- da Cunha, B.R.; González-Avella, J.C.; Gonçalves, S. Fast Fragmentation of Networks Using Module-Based Attacks. *PLoS ONE* **2015**, *10*, e0142824. [[CrossRef](#)]
- Shai, S.; Kenett, D.Y.; Kenett, Y.N.; Faust, M.; Dobson, S.; Havlin, S. Critical tipping point distinguishing two types of transitions in modular network structures. *Phys. Rev. E* **2015**, *92*, 062805. [[CrossRef](#)]
- Wang, L.; Zhao, G.; Kong, Z.; Zhao, Y. Controllability and Optimization of Complex Networks Based on Bridges. *Complexity* **2020**, *2020*, 6695026. [[CrossRef](#)]
- Fan, C.; Zeng, L.; Sun, Y.; Liu, Y.Y. Finding key players in complex networks through deep reinforcement learning. *Nat. Mach. Intell.* **2020**, *2*, 317–324. [[CrossRef](#)]

19. Lou, Y.; He, Y.; Wang, L.; Tsang, K.F.; Chen, G. Knowledge-Based Prediction of Network Controllability Robustness. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *33*, 5739–5750. [\[CrossRef\]](#)
20. Wu, C.; Lou, Y.; Wu, R.; Liu, W.; Li, J. CNN-based Prediction of Network Robustness With Missing Edges. In Proceedings of the 2022 International Joint Conference on Neural Networks (IJCNN), Padua, Italy, 18–23 July 2022; IEEE: Piscataway, NJ, USA, 2022. [\[CrossRef\]](#)
21. Lou, Y.; He, Y.; Wang, L.; Chen, G. Predicting Network Controllability Robustness: A Convolutional Neural Network Approach. *IEEE Trans. Cybern.* **2022**, *52*, 4052–4063. [\[CrossRef\]](#)
22. Lou, Y.; Wu, R.; Li, J.; Wang, L.; Li, X.; Chen, G. A Learning Convolutional Neural Network Approach for Network Robustness Prediction. *IEEE Trans. Cybern.* **2022**, 1–14.
23. Deng, Y.; Wu, J.; Qi, M.; Tan, Y. Optimal disintegration strategy in spatial networks with disintegration circle model. *Chaos Interdiscip. J. Nonlinear Sci.* **2019**, *29*, 061102. [\[CrossRef\]](#) [\[PubMed\]](#)
24. Ventresca, M. Global search algorithms using a combinatorial unranking-based problem representation for the critical node detection problem. *Comput. Oper. Res.* **2012**, *39*, 2763–2775. [\[CrossRef\]](#)
25. Lou, Y.; Wang, L.; Chen, G. Toward Stronger Robustness of Network Controllability: A Snapback Network Model. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2018**, *65*, 2983–2991. [\[CrossRef\]](#)
26. Yuan, Z.Z.; Zhao, C.; Di, Z.R.; Wang, W.X.; Lai, Y.C. Exact Controllability of Complex Networks. *Nat. Commun.* **2013**, *4*, 2447. [\[CrossRef\]](#) [\[PubMed\]](#)
27. Lou, Y.; Wu, R.; Li, J.; Wang, L.; Chen, G. A Convolutional Neural Network Approach to Predicting Network Connectedness Robustness. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 3209–3219. [\[CrossRef\]](#)
28. Lou, Y.; Wu, R.; Li, J.; Wang, L.; Tang, C.B.; Chen, G. Classification-based prediction of network connectivity robustness. *Neural Netw.* **2023**, *157*, 136–146. [\[CrossRef\]](#)
29. Freitas, S.; Yang, D.; Kumar, S.; Tong, H.; Chau, D.H. Graph Vulnerability and Robustness: A Survey. *IEEE Trans. Knowl. Data Eng.* **2023**, *35*, 5915–5934. [\[CrossRef\]](#)
30. Erdős, P.; Rényi, A. On the Strength of Connectedness of a Random Graph. *Acta Math. Hung.* **1964**, *12*, 261–267. [\[CrossRef\]](#)
31. Goh, K.I.; Kahng, B.; Kim, D. Universal Behavior of Load Distribution in Scale-free Networks. *Phys. Rev. Lett.* **2001**, *87*, 278701. [\[CrossRef\]](#)
32. Newman, M.E.; Watts, D.J. Renormalization Group Analysis of the Small-world Network Model. *Phys. Lett. A* **1999**, *263*, 341–346. [\[CrossRef\]](#)
33. Rossi, R.; Ahmed, N. The Network Data Repository with Interactive Graph Analytics and Visualization. *Proc. AAAI Conf. Artif. Intell.* **2015**, *29*, 9277. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.