Robustness of Network Controllability with Respect to Node Removals Based on In-Degree and Out-Degree

Wang, Fenghua; Kooij, Robert E.

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

MDPI

Article

Robustness of Network Controllability with Respect to Node Removals Based on In-Degree and Out-Degree

Fenghua Wang [1,*,†] and Robert E. Kooij [1,2,†]

[1] Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, 2628 CD Delft, The Netherlands

[2] Unit ICT, Strategy and Policy, Netherlands Organisation for Applied Scientific Research (TNO), 2595 DA Den Haag, The Netherlands

* Correspondence: f.wang-8@tudelft.nl

† These authors contributed equally to this work.

Abstract: Network controllability and its robustness have been widely studied. However, analytical methods to calculate network controllability with respect to node in- and out-degree targeted removals are currently lacking. This paper develops methods, based on generating functions for the in- and out-degree distributions, to approximate the minimum number of driver nodes needed to control directed networks, during node in- and out-degree targeted removals. By validating the proposed methods on synthetic and real-world networks, we show that our methods work reasonably well. Moreover, when the fraction of the removed nodes is below 10% the analytical results of random removals can also be used to predict the results of targeted node removals.

Keywords: controllability; complex networks; node removals

1. Introduction

Network controllability is a crucial area of research that has been explored in various types of networks, including biological networks [1], transportation networks [2], and corruption networks [3]. The controllability of a network refers to the ability to steer the states of its nodes to any desired state in a finite time by manipulating the input to a subset of its nodes. Nodes whose inputs are imposed are named driver nodes. In linear time-invariant systems, Kalman's controllability rank condition [4] is the classic method of assessing controllability. However, the method has limitations such as computation complexity and the lack of information about the system's interaction matrix and input matrix. To overcome these limitations, the concept of structural controllability was proposed [5]. Structural controllability is a property of structural linear time-invariant systems with independently free parameters or fixed zero elements in their interaction and input matrices that satisfy the controllability rank condition. Directed networks are structural systems. Liu et al. [6] developed the algorithm and analytical methods to obtain the minimum number of driver nodes in directed networks with the assumption that the directed network has no self-links and a node's internal state can only be modified upon interaction with neighboring nodes [7]. Throughout this paper, we will adhere to this assumption. Besides structural controllability, Yuan et al. introduced an exact controllability paradigm to determine the minimum number of driver nodes for undirected networks with arbitrary weights by using the maximum multiplicity [8].

In recent years, network structural controllability has gained increasing attention as a tool to measure and enhance network robustness. Robustness is commonly assessed by measuring network performance under various perturbations [9]. One approach is to randomly remove nodes or links and observe the resulting changes in network performance, while another approach involves targeted attack strategies exploiting specific

features of network topology such as betweenness, degree, and closeness. Several studies have investigated the effectiveness of different targeted attack strategies on network controllability. For example, degree-based attacks have been found to be more harmful to network controllability than random attacks [10], while betweenness-based attacks are more damaging in most real-world networks [11]. Additionally, attacking bridge links, which results in a disconnected network, has been shown to be an effective way to destroy network controllability [12]. Another approach to targeted attack strategies involves identifying critical nodes and links whose removal increases the number of driver nodes [6]. Protecting critical links can make random link attacks less efficient [13]. Some studies have found that hierarchical attack strategies targeting critical nodes and links first are more efficient than metric-based attack strategies, such as betweenness- or degree-based strategies in interdependent networks [14]. In addition to assessing the robustness of network controllability under perturbations, some studies have focused on enhancing it. For example, increasing the density of nodes with an in-degree and out-degree equal to one or two has been shown to improve network controllability [15]. Adding links to low-degree nodes and creating multi-loop structures have also been found to increase the robustness of network controllability [16]. Furthermore, different redundant design strategies of interdependent networks, such as betweenness-based and degree-based strategies for node backup and high degree first strategy for edge backup, have been investigated to optimize the robustness of network controllability [17].

In addition to qualitative research, quantitative studies have been carried out to explore the robustness of network controllability under different types of perturbations. Lu et al. [11] developed numerical approximations of random and targeted node attacks based on the degree on Erdös-Rényi (ER) networks, which fit well when the fraction of nodes is below 20%. Sun et al. [13] derived closed-form approximations of the minimum number of driver nodes under various types of attacks, including random link attacks, targeted attacks, and random attacks with protection. Chen et al. [18] developed analytical approximations for the minimum number of driver nodes during random link removal using generating functions. Wang et al. [19] later conducted analytical methods based on generating functions to approximate the network controllability during random and targeted node removal based on the total degree of different kinds of networks. In addition to analytical methods, machine learning has been employed to predict network controllability robustness. Dhiman et al. [20] used machine-learning-based approximations to quantify the minimum fraction of driver nodes under random and targeted link attacks, which performed better than the closed-form approximation proposed by Sun et al. [13]. Meanwhile, by utilizing deep learning techniques, Lou et al. have developed a series of works that employ different convolutional neural network (CNN) frameworks, treating the adjacency matrix as a visual representation, to predict network controllability under random node or link attacks, degree-based targeted node or link attacks, and betweenness-based targeted node and link attacks [21–23]. Through the use of these models, they have achieved increasingly precise controllability predictions and demonstrated improved scalability. The quantitative studies provide valuable insights into the robustness of network controllability.

As the analytical approximations for targeted node removals based on node in-degree and out-degree are still lacking, in this paper, we aim to utilize the structural controllability framework for directed networks proposed by Liu et al. [6] to make the analytical approximation for those two kinds of targeted node removals. We validate our proposed methods by applying them to three types of synthetic networks and four real-world communication networks.

The remainder of the paper is structured as follows. In Section 2, we introduce the networks used in our study. Section 3 presents the analytical results of network controllability under the two classes of targeted attacks. Finally, we conclude and discuss the implications of our findings in Section 4.

2. Network Data

To validate the theoretical results presented in the following sections, we will utilize three categories of synthetic networks as well as several real-world networks. In this section, we provide specific information regarding the utilized networks.

2.1. Directed Synthetic Networks

We choose three types of synthetic networks: Erdös-Rényi (ER) networks, Swarm Signaling networks (SSNs) and Scale-free networks (SFs).

We generate a directed ER network with N nodes, whereby a directed link is placed between every pair of nodes with a given probability of p_{ER}. The average number of links is governed by the equation, $L = N(N-1)p_{ER}$. This study has employed two kinds of ER networks with $N = 50$ and $N = 100$, and $p_{ER} = 0.07$ and $p_{ER} = 0.04$, respectively.

The topology of Swarm Signaling Networks (SSNs), proposed in [24], is characterized by a regular out-degree and an in-degree distribution that follows a Poisson distribution. Two parameters must be specified to generate SSNs: the number of nodes, N, and the out-degree value, k. Each node in the network randomly creates k outgoing links to other nodes. Two kinds of SSNs are chosen, with $N = 10^4$ and average out-degree values of $k = 2$ and $k = 5$, respectively.

Scale-free networks (SFs) are a class of complex networks whose both in-degree and out-degree distributions exhibit a power-law distribution. In this paper, we generate two SFs using the Barabási–Albert model, which is a preferential attachment mechanism that generates networks with a power-law degree distribution with an exponent $\gamma = 3$ [25]. Specifically, we generate SFs in two stages. In the first stage, we generate a Barabási–Albert graph with N nodes, where the initial state is a star with $m + 1$ nodes. At each step, a node with m edges is preferentially attached to existing nodes with high degrees until the total number of nodes reaches N. In the second stage, we randomly assign directions to each link in the generated graph. The resulting SFs have in-degree and out-degree distributions that follow a power-law distribution with an exponent $\gamma = 3$. We set $m = 5$ and $m = 10$ for both SFs with $N = 10^5$ nodes, resulting in minimum in-degree and out-degree values a of 5 and 10, respectively, which are approximated by the integers that make the ceiling of the average value of the power-law distribution equal to m.

2.2. Real-World Networks

In this study, we employed real-world communication networks obtained from the Topology Zoo dataset [26]. To convert these networks from undirected to directed, we utilized the source and targeted node attributes [13]. Table 1 demonstrates the basic properties of the networks used in this study, including the number of nodes N, the number of links L, and the average total degree $< k >$. The total degree of a node is the sum of its in-degree and out-degree. Since the average in-degree equals the average out-degree, the average total degree is twice the average in-degree (and out-degree).

Table 1. Properties of four real-world communication networks.

Name	N	L	$< k >$
HinerniaGlobal	55	81	2.95
Syringa	74	74	2.00
Interoute	110	146	2.65
Cogentco	197	243	2.47

3. Network Controllability

Consider a linear, time-invariant networked system of N nodes, where each node's state is governed by $\dot{x}(t) = Ax(t) + Bu(t)$, with $x(t) = (x_1(t), x_2(t), \ldots, x_n(t))^T$ being the $N \times 1$ state vector. The $N \times N$ matrix A represents the interactions among the network

components, and the $N \times M$ matrix B specifies which nodes are under the direct control of the $M \times 1$ control input vector $u(t) = (u_1(t), u_2(t), \ldots, u_m(t))^T$.

A linear, time-invariant networked system is controllable if it can reach any desired state within a finite time by applying external inputs. The Kalman rank criterion requires that the rank of the controllability matrix $[B, AB, A^2B, \ldots, A^{n-1}B]$ equals N for the system to be fully controllable. Liu et al. introduced the maximum matching method and the minimum inputs theorem to determine the minimum number of driver nodes required to ensure network structural controllability [6]. The number of driver nodes, N_D, can be obtained by mapping a directed network into a bipartite network [13], obtaining a maximum matching edge set using the maximum matching algorithm [27], and then calculating $N_D = \min\{1, N - N_m\}$, where N_m is the number of directed edges in the maximum matching set without sharing the same source or end nodes.

4. In-Degree and Out-Degree Node Attacks

Centrality analysis is an essential research area in studying network robustness [28]. Nodes with a high degree are known to have a substantial impact on network functioning and are more susceptible to targeted attacks. In this study, our objective is to investigate an analytical approximation of network controllability during targeted node removal based on two types of degrees: in-degree and out-degree.

Assuming that the probability of node attack is proportional to some power of its in-degree and out-degree, we can express the probability of removing node i based on its in-degree k_{in_i} as p_{in_i} and based on its out-degree k_{out_i} as p_{out_i}. The formula for calculating these probabilities is given as follows:

$$
\begin{aligned}
p_{in\_i} &= \frac{k_{in\_i}^{\alpha}}{\sum_{j \in \mathcal{N}} k_{in\_j}^{\alpha}}, \\
p_{out\_i} &= \frac{k_{out\_i}^{\alpha}}{\sum_{j \in \mathcal{N}} k_{out\_j}^{\alpha}}.
\end{aligned}
\tag{1}
$$

In the node removal process, after some nodes are removed, we recalculate the removal probabilities for the remaining nodes using Equation (1). We then select nodes to remove based on the recalculated probabilities until all nodes are removed.

When $\alpha = 0$, the aforementioned equations become

$$
\begin{aligned}
p_{in\_i} &= \frac{1}{N}, \\
p_{out\_i} &= \frac{1}{N},
\end{aligned}
\tag{2}
$$

which indicates that each node has an equal probability of being removed, resulting in a random removal strategy. On the other hand, for $\alpha > 0$, nodes with higher degrees have a greater likelihood of being removed, while for $\alpha < 0$, nodes with lower degrees are more likely to be removed.

In this study, we investigate the impact of degree-based node removal strategies on network robustness. To this end, we focus on $\alpha > 0$, as higher-degree nodes are commonly targeted for attack in real-world scenarios. Specifically, we consider two values of α, namely $\alpha = 1$ and $\alpha = 10$, to evaluate the impact of removing nodes proportional to their degree and removing high-degree nodes more aggressively, respectively. By using Equation (1), we obtain the probabilities of the node being removed based on in-degree and out-degree when $\alpha = 1$ as follows:

$$
\begin{aligned}
p_{in\_i} &= \frac{k_{in\_i}}{\sum_{j \in \mathcal{N}} k_{in\_j}}, \\
p_{out\_i} &= \frac{k_{out\_i}}{\sum_{j \in \mathcal{N}} k_{out\_j}}.
\end{aligned}
\tag{3}
$$

Analogously, the node removal probabilities based on in-degree or out-degree with $\alpha = 10$ can be calculated by

$$p_{in\_i} = \frac{k_{in\_i}^{10}}{\sum_{j \in \mathcal{N}} k_{in\_j}^{10}},$$

$$p_{out\_i} = \frac{k_{out\_i}^{10}}{\sum_{j \in \mathcal{N}} k_{out\_j}^{10}}. \tag{4}$$

Our results show that, for $\alpha = 10$, the removal of high-degree nodes does not lead to a significant reduction in network robustness in the beginning stage. For several networks, there are no significant differences between the results with $\alpha = 1$ and $\alpha = 100$. Interestingly, we observe that increasing the value of α to 100 does not result in further performance gains, as the performance of attacks with $\alpha = 100$ is similar to that of attacks with $\alpha = 10$. Additional details on these findings can be found in Appendix A. Furthermore, we find that when $\alpha = 1$, the removal strategies based on in-degree or out-degree can be more detrimental to certain networks than node removal based on the total degree. However, for some other networks, the harmful effects of these strategies are comparable. The results are presented in Appendix B.

5. Minimum Fraction of the Number of Driver Nodes under Targeted Node Attacks

5.1. Analytical Approximation

The analytical approximation for targeted node removal based on in- and out-degrees with different α is derived from the analytical approximation of random node removal. As such, we begin by introducing the methodology for approximating the minimum fraction of driver nodes under random removal, and then introduce the analytical methods of the cases: $\alpha = 1$ and $\alpha = 10$.

5.1.1. Case: $\alpha = 0$

To predict the minimum fraction of driver nodes under random removal, $\alpha = 0$, by using the analytical method based on generating function of degrees, we first employ the framework proposed by Liu et al. [6]. Given a directed network $\mathcal{G}(N, L)$ with N nodes and L links, we can determine the minimum fraction of driver nodes using the generating function of the in- and out-degree distributions, denoted by $G_{in}(x)$ and $G_{out}(x)$, respectively, as well as the excess in- and out-degree distributions, denoted by $H_{in}(x)$ and $H_{out}(x)$, respectively. These generating functions can be defined as follows:

$$G_{in}(x) = \sum_{k=0}^{\infty} P_{in}(k_{in}) x^{k_{in}},$$

$$G_{out}(x) = \sum_{k=0}^{\infty} P_{out}(k_{out}) x^{k_{out}},$$

$$H_{in}(x) = \frac{\sum_{k=1}^{\infty} k_{in} P_{in}(k_{in}) x^{k_{in}-1}}{<k_{in}>} = \frac{G'_{in}(x)}{G'_{in}(1)}, \tag{5}$$

$$H_{out}(x) = \frac{\sum_{k=1}^{\infty} k_{out} P_{out}(k_{out}) x^{k_{out}-1}}{<k_{out}>} = \frac{G'_{out}(x)}{G'_{out}(1)},$$

where k_{in} and k_{out} represent in-degree and out-degree, respectively, while $P_{in}(.)$ and $P_{out}(.)$ are in- and out-degree probability distributions, respectively. Then, the minimum fraction of driver nodes can be obtained by

$$n_d = \frac{1}{2} \{ G_{in}(\omega_2) + G_{in}(1 - \omega_1) - 2 + G_{out}(\hat{\omega}_2) + G_{out}(1 - \hat{\omega}_1) + k[\hat{\omega}_1(1 - \omega_2) + \omega_1(1 - \hat{\omega}_2)] \}, \tag{6}$$

where ω_1, ω_2, $\hat{\omega}_1$ and $\hat{\omega}_2$ satisfy

$$
\begin{aligned}
\omega_1 &= H_{out}(\hat{\omega}_2), \\
\omega_2 &= 1 - H_{out}(1 - \hat{\omega}_1), \\
\hat{\omega}_1 &= H_{in}(\omega_2), \\
\hat{\omega}_2 &= 1 - H_{in}(1 - \omega_1),
\end{aligned}
\tag{7}
$$

and k denotes half of the average degree equal to the average in-degree and the average out-degree, $k = \frac{1}{2} < k > = < k_{in} > = < k_{out} >$. We aim to determine the minimum fraction of driver nodes n_D needed to control the remaining part of the network after removing a fraction p of nodes. To this end, we partition the network into two sets: a set containing N_D driver nodes that can control the rest of the network and a set of N_r removed nodes. We assume that each removed node requires the control of an individual driver node. Then, we define the fraction of driver nodes n_D as $n_D = \frac{N_D + N_r}{N}$. After removing a fraction p of nodes from the network, we can obtain the following expression for the minimum fraction of driver nodes n_D,

$$
n_D = \frac{n_d(1 - p)N + pN}{N} = n_d(1 - p) + p.
\tag{8}
$$

We adopt the method proposed by Shao et al. [29] to adjust the generating functions of in- and out-degree and the excess in- and out-degree after randomly removing a fraction p of nodes from the network. According to this method, the generating function after random removal can be obtained by applying an adjusted augmentation $\bar{x} = p + (1 - p)x$ to the original generating functions. Hence, the generating functions of the in- and out-degree and the excess the in- and out-degree after removing a fraction p of nodes can be expressed as follows:

$$
\begin{aligned}
\bar{G}_{in}(x) &= G_{in}(p + (1 - p)x), \\
\bar{G}_{out}(x) &= G_{out}(p + (1 - p)x), \\
\bar{H}_{in}(x) &= \frac{\bar{G}'_{in}(x)}{\bar{G}'_{in}(1)}, \\
\bar{H}_{out}(x) &= \frac{\bar{G}'_{out}(x)}{\bar{G}'_{out}(1)}.
\end{aligned}
\tag{9}
$$

Next, we use Equations (6) and (8) to obtain the fraction of the minimum number of nodes n_D after removing a fraction p of nodes,

$$
\begin{aligned}
n_D = \frac{1}{2}(1 - p)\{ &\bar{G}_{in}(\omega_2) + \bar{G}_{in}(1 - \omega_1) - 2 + \bar{G}_{out}(\hat{\omega}_2) + \bar{G}_{out}(1 - \hat{\omega}_1) \\
&+ k(1 - p)[\hat{\omega}_1(1 - \omega_2) + \omega_1(1 - \hat{\omega}_2)]\} + p,
\end{aligned}
\tag{10}
$$

where ω_1, ω_2, $\hat{\omega}_1$ and $\hat{\omega}_2$ satisfy

$$
\begin{aligned}
\omega_1 &= \bar{H}_{out}(\hat{\omega}_2), \\
\omega_2 &= 1 - \bar{H}_{out}(1 - \hat{\omega}_1), \\
\hat{\omega}_1 &= \bar{H}_{in}(\omega_2), \\
\hat{\omega}_2 &= 1 - \bar{H}_{in}(1 - \omega_1).
\end{aligned}
\tag{11}
$$

5.1.2. Case: $\alpha = 1$

In-degree: In undirected networks, after a fraction p of nodes have been removed based on their degree; specifically, the probability of a node removal is proportional to some power of its degree, see Equation (1); the generating function of the degree distribution, $G(x)$, transforms into function $\bar{G}(x)$, which is as follows [28]:

$$\bar{G}(x) = \frac{1}{1-p} \sum_{k=0}^{\infty} p_k f^{k^{\alpha}} (1 + \frac{fG'_{\alpha}(f)}{<k>}(x-1))^k, \tag{12}$$

where $f \equiv G_{\alpha}^{-1}(1-p)$, $G_{\alpha}(x) \equiv \sum_k p_k x^{k^{\alpha}}$ and $<k>$ is the average degree of the initial network.

We investigate the extension of prior conclusions to directed networks while removing nodes based on their in-degree. We assume that a node's in-degree and out-degree are independent and uncorrelated, such that removing a fraction p of nodes based on their in-degree results in the generating function of the in-degree distribution described by Equation (12). Furthermore, the generating function of the out-degree distribution is given by $\bar{G}_{out}(x) = G_{out}(p + (1-p)x)$ following the equation of random node removals. So, if we remove nodes based on in-degree, function $\bar{G}_{in}(x)$ and function $\bar{G}_{in}(x)$ satisfy

$$\bar{G}_{in}(x) = \frac{1}{1-p} \sum_{k_{in}=0}^{\infty} p_{k_{in}} f^{k_{in}} (1 + \frac{fG'_1(f)}{<k_{in}>}(x-1))^{k_{in}},$$
$$\bar{G}_{out}(x) = G_{out}(p + (1-p)x). \tag{13}$$

Then, we can obtain the analytical approximation of the minimum fraction of driver nodes under node removals based on in-degree using Equation (10).

Out-degree: Analogously, if we remove a fraction p of nodes based on their out-degree, we maintain the assumption that the generating function of the out-degree distribution is described by Equation (12). Additionally, the generating function of the in-degree distribution can be expressed as $\bar{G}_{in}(x) = G_{in}(p + (1-p)x)$. Therefore, we have function $\bar{G}_{in}(x)$ and function $\bar{G}_{in}(x)$ as follows:

$$\bar{G}_{in}(x) = G_{in}(p + (1-p)x),$$
$$\bar{G}_{out}(x) = \frac{1}{1-p} \sum_{k_{out}=0}^{\infty} p_{k_{out}} f^{k_{out}} (1 + \frac{fG'_1(f)}{<k_{out}>}(x-1))^{k_{out}}. \tag{14}$$

Furthermore, utilizing Equation (10), we can derive an analytical approximation of the minimum fraction of driver nodes when nodes are removed based on out-degree.

5.1.3. Case: $\alpha = 10$

When $\alpha = 10$, we encounter difficulties in obtaining a numerical solution for $f \equiv G_{\alpha}^{-1}(1-p)$, where $G_{\alpha}(x) \equiv \sum_k p_k x^{k^{\alpha}}$. Consequently, it becomes challenging to determine the evolution of the generating functions for in-degree and out-degree distributions during the node removal process. To address this challenge, we propose a heuristic approach whereby we map the targeted node removal process based on in-degree or out-degree into a random node attack process.

Specifically, for node removals based on in-degree with $\alpha = 10$, where a fraction of p nodes are to be removed, we map this process to the removal of $\bar{p}$ nodes in the in-degree distribution, while maintaining the fraction of nodes in the out-degree distribution at p. Similarly, for node removals based on out-degree with $\alpha = 10$, we map the process to the random removal of a fraction of $\bar{p}$ nodes in the out-degree distribution, as well as a fraction of p nodes in the in-degree distribution.

In-degree: In order to estimate the corresponding $\bar{p}$ of a given fraction p under node removals based on in-degree with $\alpha = 10$, we adopt the assumption that nodes are removed in descending order of in-degree. Specifically, we first sort the nodes according to their in-degree and then remove nodes starting from the node with the highest in-degree until the targeted fraction p is reached.

Next, we calculate the total in-degree of all the removed nodes by utilizing the original in-degree distribution and the targeted removal fraction p. The effective fraction $\bar{p}$ is

then obtained by normalizing the total in-degree of all removed nodes with respect to the total in-degree of all nodes in the initial network. This can be calculated as follows:

$$\bar{p}_{in} = \frac{\sum_{k_{in}=k_{in_{max}}}^{k_{in}=\bar{k}_{in}} p_{k_{in}} N k_{in}}{N < k_{in} >} = \frac{\sum_{k_{in}=k_{in_{max}}}^{k_{in}=\bar{k}_{in}} p_{k_{in}} k_{in}}{< k_{in} >}, \quad (15)$$

where the largest in-degree value is denoted as $k_{in_{max}}$, the probability of removed nodes with degree k_{in} is denoted as $p_{k_{in}}$ and degree $\bar{k}_{in}$ satisfies $\sum_{k_{in}=k_{in_{max}}}^{k_{in}=\bar{k}_{in}} p_{k_{in}} = p$. It is worth mentioning that except for removed probability $p_{\bar{k}_{in}}$, other probability $p_{k_{in}}$ is equal to probability $P_{in}(k_{in})$ in the generating function. Then, we can use effective proportion $\bar{p}_{in}$ for the approximation of the minimum fraction of driver nodes as follows:

$$\begin{aligned} \bar{G}_{in}(x) &= G_{in}(\bar{p}_{in} + (1 - \bar{p}_{in})x), \\ \bar{G}_{out}(x) &= G_{out}(p + (1 - p)x), \\ n_D &= \frac{1}{2}\{\bar{G}_{in}(\omega_2) + \bar{G}_{in}(1 - \omega_1) - 2 + \bar{G}_{out}(\hat{\omega}_2) + \bar{G}_{out}(1 - \hat{\omega}_1) \\ &\quad + k(1 - \frac{p + \bar{p}_{in}}{2})[\hat{\omega}_1(1 - \omega_2) + \omega_1(1 - \hat{\omega}_2)]\}(1 - \frac{p + \bar{p}_{in}}{2}) + \frac{p + \bar{p}_{in}}{2}, \end{aligned} \quad (16)$$

where $\omega_1, \omega_2, \bar{\omega}_1$ and $\bar{\omega}_2$ satisfy Equation (11).

Out-degree: Analogously, for targeted node removal based on out-degree with $\alpha = 10$, the calculation of fraction $\bar{p}_{out}$ follows the same assumption: nodes are removed from the node with the highest out-degree to the node with the lowest out-degree until the removed fraction of nodes reaches p. The effective fraction $\bar{p}_{out}$ is the total out-degree of removed nodes normalized by the total out-degree in the original network, which can be calculated by

$$\bar{p}_{out} = \frac{\sum_{k_{out}=k_{out_{max}}}^{k_{out}=\bar{k}_{out}} p_{k_{out}} N k_{out}}{N < k_{out} >} = \frac{\sum_{k_{out}=k_{out_{max}}}^{k_{out}=\bar{k}_{out}} p_{k_{out}} k_{out}}{< k_{out} >}, \quad (17)$$

where the largest degree value is denoted as $k_{out_{max}}$, and the probability of removed nodes with out-degree k_{out} as $p_{k_{out}}$. To achieve the targeted removal fraction p, we find the minimum out-degree value $\bar{k}_{out}$ satisfying $\sum_{k_{out}=k_{out_{max}}}^{k_{out}=\bar{k}_{out}} p_{k_{out}} = p$. For all out-degree values except for $\bar{k}_{out}$, their corresponding probabilities $p_{k_{out}}$ are equal to the probabilities $P_{out}(k_{out})$ in the generating function. Then, we use $\bar{p}_{out}$, the effective proportion of removed nodes based on out-degree, to estimate the minimum number of driver nodes, which is given by the following expression:

$$\begin{aligned} \bar{G}_{in}(x) &= G_{in}(p + (1 - p)x), \\ \bar{G}_{out}(x) &= G_{out}(\bar{p}_{out} + (1 - \bar{p}_{out})x), \\ n_d &= \frac{1}{2}\{\bar{G}_{in}(\omega_2) + \bar{G}_{in}(1 - \omega_1) - 2 + \bar{G}_{out}(\hat{\omega}_2) + \bar{G}_{out}(1 - \hat{\omega}_1) \\ &\quad + k(1 - \frac{p + \bar{p}_{out}}{2})[\hat{\omega}_1(1 - \omega_2) + \omega_1(1 - \hat{\omega}_2)]\}(1 - \frac{p + \bar{p}_{out}}{2}) + \frac{p + \bar{p}_{out}}{2}, \end{aligned} \quad (18)$$

where $\omega_1, \omega_2, \bar{\omega}_1$ and $\bar{\omega}_2$ satisfy Equation (11).

5.2. Results for Targeted Node Attacks

5.2.1. Case: $\alpha = 1$

We ran simulations on various networks, as described in Section 2. We carried out 10,000 realizations for all networks to ensure sufficient statistical power. For ER and real-world networks, which have a relatively small number of nodes, one node was removed at each step until all nodes had been removed during each realization. Then, a recalculation of the minimum fraction of driver nodes was conducted by using the algorithm. On the other hand, due to the large number of nodes in SSNs and SFs, 1% of nodes were removed

at each step until all nodes had been removed during each realization. Subsequently, the minimum fraction of driver nodes was recalculated based on the modified network structure. The average value of results obtained from the 10,000 realizations was taken as the final simulation output.

We present the results of targeted node removal based on in-degree and out-degree with $\alpha = 1$, as depicted in Figures 1 and 2. The simulation results are shown in green lines, whereas the analytical results are in red. The results of random node removal are also presented in gray lines for comparison. We observe that the analytical results serve as a closed-form approximation of the minimum fraction of driver nodes (n_D), as a discrepancy exists between the predicted and simulation values during the targeted node removal process based on in-degree or out-degree. In the case of ER networks and SFs, the in-degree and out-degree distributions are identical. Consequently, the predicted values of targeted removal based on in-degree and out-degree are also the same. For SSNs, the out-degree of nodes is fixed. Therefore, the lines of analytical results of targeted node removal based on out-degree with $\alpha = 1$ in SSNs overlap with the lines of random node removal. We find that for SFs and SSNs, the simulation results of targeted removal based on in-degree and out-degree are slightly different from the simulation results of random removals. Thus, even though the analytical results of SFs differ slightly from the simulation results of random removals and the analytical results of SSNs are the same as the random removal results, they closely approach the simulation results of targeted removals.
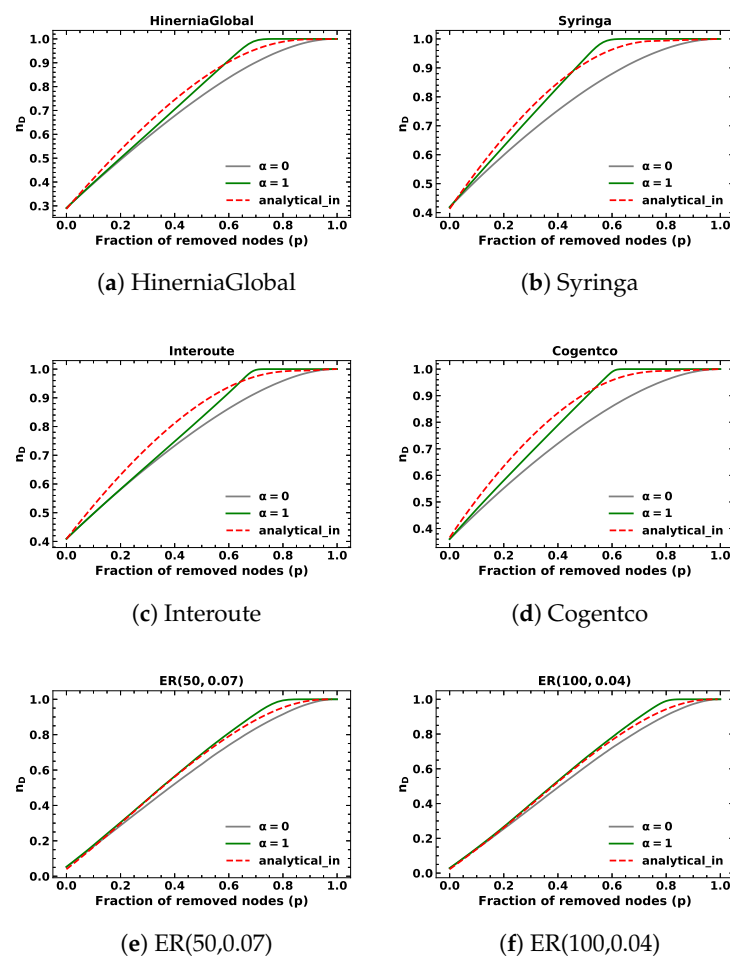

(**a**) HinerniaGlobal

(**b**) Syringa

(**c**) Interoute

(**d**) Cogentco

(**e**) ER(50,0.07)

(**f**) ER(100,0.04)

Figure 1. *Cont.*

Figure 1. The minimum fraction of driver nodes n_D during targeted node removal based on in-degree with $\alpha = 1$ for different kinds of networks.

Figure 2. *Cont.*

(g) SSN($10^4, 2$)

(h) SSN($10^4, 5$)

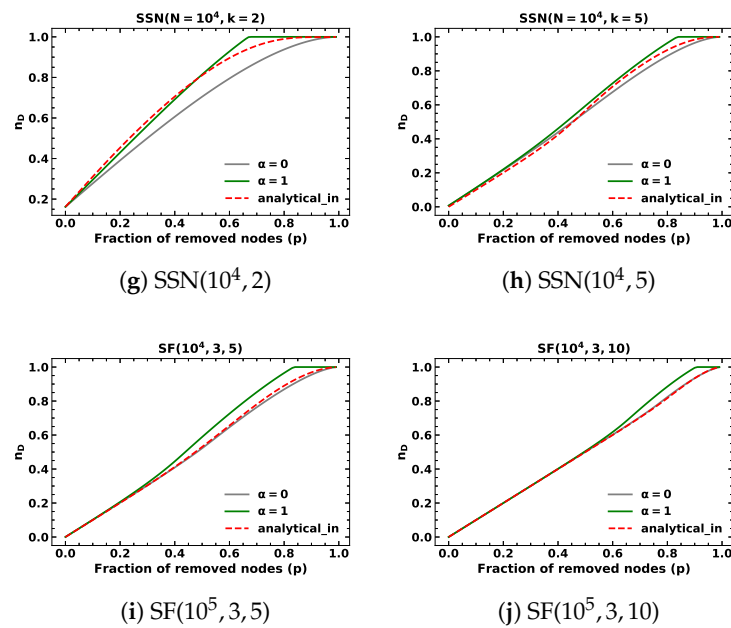**(i)** SF($10^5, 3, 5$)

(j) SF($10^5, 3, 10$)

Figure 2. The minimum fraction of driver nodes n_D during targeted node removal based on out-degree with $\alpha = 1$ for different kinds of networks.
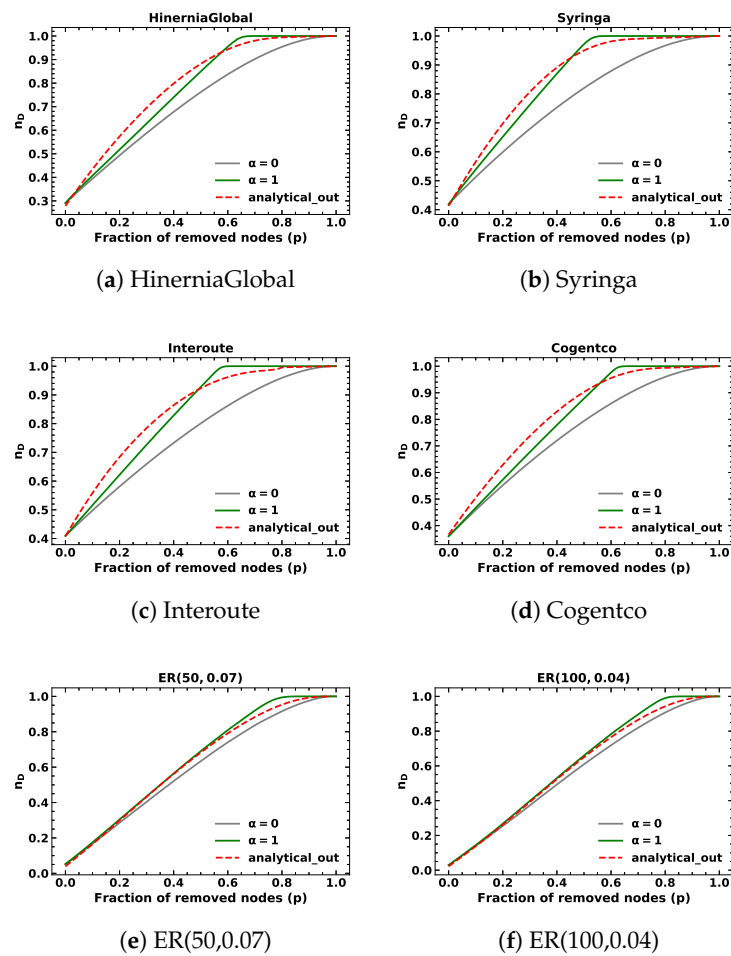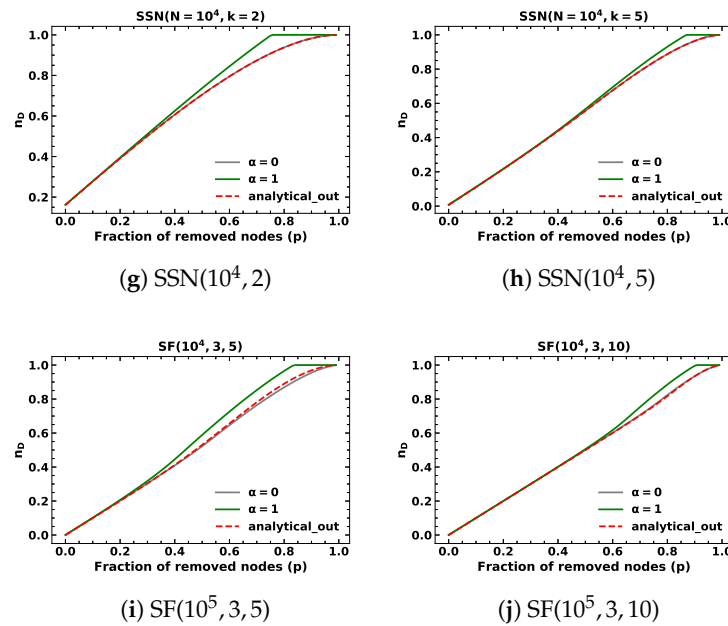
When the removed fraction p is small, the simulation results of targeted removals based on in-degree and out-degree are close to those of random removals. We verified this by calculating the Root Mean Square Error (RMSE) between the simulation results of targeted removals based on in-degree and out-degree and analytical results of randomly removing nodes below 10%, as shown in Table 2. Moreover, we calculated the RMSE between the simulation and analytical results of targeted node removals based on in-degree and out-degree below 10%, as shown in Table 3. The results indicated that both methods provide a good approximation of the simulation results, as the values in both tables for targeted node removals based on in-degree and out-degree with $\alpha = 1$ are reasonably small.

Table 2. The RMSE between the analytical results of random removals and the simulation results under random removals, target removals with $\alpha = 1$ and $\alpha = 10$, respectively, while removing 10% of the nodes. The column labeled "Random" indicates the RMSE under random removals. The columns labeled "$\alpha = 1$" and "$\alpha = 10$" represent the RMSE under targeted node removals with $\alpha = 1$ and $\alpha = 10$, respectively. The columns labeled "Indegree", "Outdegree", and "Degree" represent the RMSE under targeted node removals based on in-degree, out-degree, and total degree, respectively. The analytical method for random removals is from the reference [19].

Network	Random	$\alpha = 1$			$\alpha = 10$		
		Indegree	Outdegree	Degree	Indegree	Outdegree	Degree
SF($10^5, 3, 5$)	0.0005	0.0010	0.0010	0.0010	0.0032	0.0032	0.0032
SF($10^5, 3, 10$)	0.0001	0.0001	0.0001	0.0001	0.0001	0.0001	0.0001
ER(50, 0.07)	0.0137	0.0164	0.0156	0.0155	0.0190	0.0195	0.0223
ER(100, 0.04)	0.0079	0.0086	0.0095	0.0094	0.0126	0.0121	0.0156
HinerniaGlobal	0.0039	0.0052	0.0110	0.0084	0.0025	0.0152	0.0152
Syringa	0.0071	0.0136	0.0217	0.0179	0.0237	0.0263	0.0443
Interoute	0.0011	0.0008	0.0106	0.0056	0.0064	0.0072	0.0175
Cogentco	0.0011	0.0090	0.0053	0.0071	0.0156	0.0091	0.0248
SSN($10^4, 2$)	0.0000	0.0103	0.0003	0.0052	0.0143	0.0007	0.0155
SSN($10^4, 5$)	0.0000	0.0006	0.0000	0.0003	0.0008	0.0001	0.0008

Table 3. The RMSE between the analytical results of the proposed analytical methods and the simulation results under different kinds of removals while removing 10% of the nodes. The column labeled "Random" indicates the RMSE under random removals. The columns labeled "$\alpha = 1$" and "$\alpha = 10$" represent the RMSE under targeted node removals with $\alpha = 1$ and $\alpha = 10$, respectively. The columns labeled "Indegree", "Outdegree", and "Degree" represent the RMSE under targeted node removals based on in-degree, out-degree, and total degree, respectively. The analytical methods for random removals and targeted node removals based on the total degree are from the reference [19].

Network	Random	$\alpha = 1$			$\alpha = 10$		
		Indegree	Outdegree	Degree	Indegree	Outdegree	Degree
SF(10^5, 3, 5)	0.0005	0.0010	0.0010	0.0546	0.0764	0.0764	0.1573
SF(10^5, 3, 10)	0.0001	0.0001	0.0001	0.0555	0.0799	0.0799	0.1600
ER(50, 0.07)	0.0137	0.0122	0.0113	0.0095	0.0588	0.0595	0.0543
ER(100, 0.04)	0.0079	0.0058	0.0067	0.0039	0.0189	0.0193	0.0284
HinerniaGlobal	0.0039	0.0089	0.0136	0.0025	0.0281	0.0349	0.0354
Syringa	0.0071	0.0096	0.0143	0.0061	0.0157	0.0235	0.0142
Interoute	0.0011	0.0151	0.0242	0.0009	0.0265	0.0454	0.0229
Cogentco	0.0011	0.0233	0.0244	0.0050	0.0314	0.0330	0.0322
SSN(10^4, 2)	0.0000	0.0085	0.0002	0.0027	0.0331	0.0006	0.0343
SSN(10^4, 5)	0.0000	0.0094	0.0000	0.0024	0.0167	0.0001	0.0264

5.2.2. Case: $\alpha = 10$

We ran the simulations of 10,000 realizations with $\alpha = 10$ under in-degree and out-degree node removals in mentioned networks. Each realization of every network is the same as described in case $\alpha = 1$. The simulation results of network controllability are shown in the green lines in Figures 3 and 4. As before, the analytical results are depicted in red lines, while the simulation results of network controllability under random node attacks are shown in gray lines.

In addition to targeted node removals based on out-degree in SSNs with fixed out-degree, the analytical results are consistent with random node removals. Notably, the analytical results exhibit a similar pattern for $\alpha = 10$, where they initially surpass the simulation results before eventually intersecting and becoming inferior to the targeted node attack lines but superior to the random node attack lines as the fraction of removed nodes approaches one. We find the proposed methods can closely approximate network controllability using a closed-form approach, but do not precisely align with simulation results.

Upon examining Tables 2 and 3, we observe that both the proposed analytical methods and the analytical results of random node removal demonstrate satisfactory performance for targeted node removal based on in-degree and out-degree with $\alpha = 10$ when the fraction of removed nodes p is below 10%. However, the values obtained for $\alpha = 10$ are comparatively inferior to those obtained for $\alpha = 1$ and random node removal. These outcomes highlight the limitations of our proposed approach. Specifically, our method assumes that nodes are removed from the node with the highest degree to the node with the lowest degree, which is true when α is large enough, such as infinity. In this context, we choose $\alpha = 10$ and the node with the highest degree is much more likely to be removed, but still cannot be guaranteed to be removed at each step.
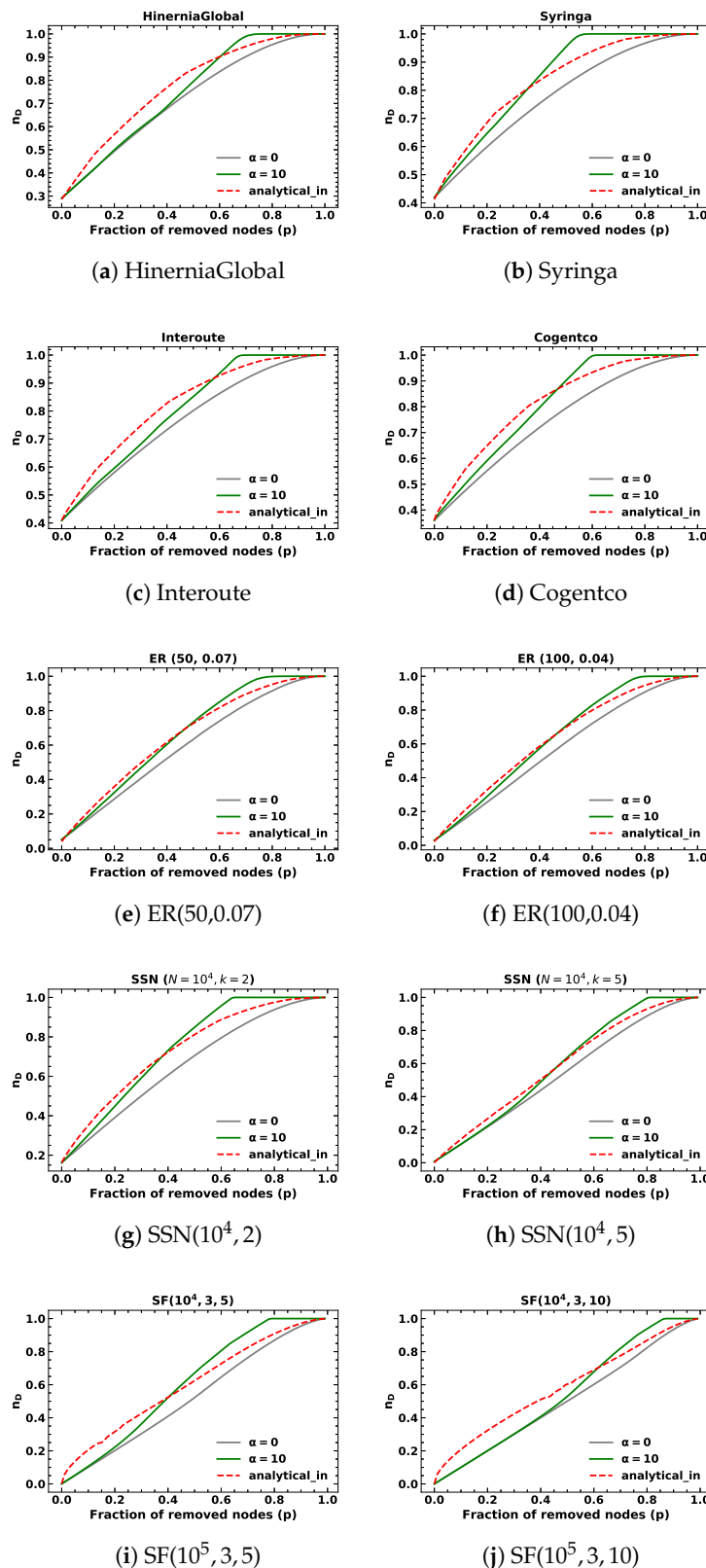
(**a**) HinerniaGlobal

(**b**) Syringa

(**c**) Interoute

(**d**) Cogentco

(**e**) ER(50,0.07)

(**f**) ER(100,0.04)

(**g**) SSN(10^4, 2)

(**h**) SSN(10^4, 5)

(**i**) SF(10^5, 3, 5)

(**j**) SF(10^5, 3, 10)

Figure 3. The minimum fraction of driver nodes n_D during targeted node removal based on in-degree with $\alpha = 10$ for different kinds of networks.
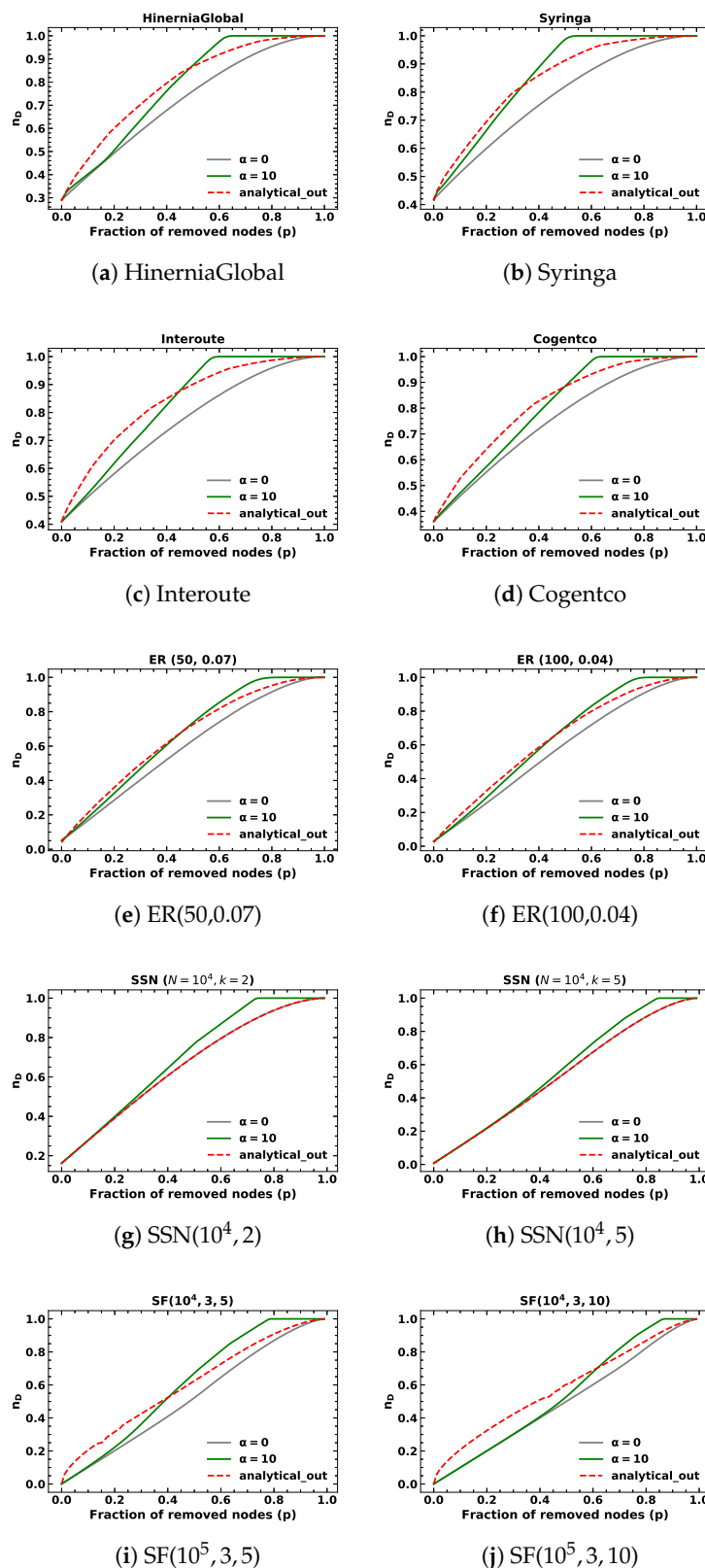
(**a**) HinerniaGlobal

(**b**) Syringa

(**c**) Interoute

(**d**) Cogentco

(**e**) ER(50,0.07)

(**f**) ER(100,0.04)

(**g**) SSN(10^4, 2)

(**h**) SSN(10^4, 5)

(**i**) SF(10^5, 3, 5)

(**j**) SF(10^5, 3, 10)

Figure 4. The minimum fraction of driver nodes n_D during targeted node removal based on out-degree with $\alpha = 10$ for different kinds of networks.

6. Conclusions and Discussion

This study introduces analytical methods based on generating functions to determine the minimum fraction of driver nodes required to maintain network controllability in directed networks under node failures based on in-degree and out-degree. We develop separate analytical techniques for two scenarios, namely $\alpha = 1$ and $\alpha = 10$. Our proposed analytical methods demonstrate reasonable results to predict the minimum fraction of driver nodes under targeted attacks. Furthermore, our investigation indicates that random node removal may also serve as a reliable predictor of the results of various targeted node removals, particularly when the fraction of removed nodes is minimal (below 10%).

In addition to the findings presented in this paper, we have endeavored to apply our simulations to various other real-world networks. Our analysis reveals that the minimum fraction of driver nodes calculated by the proposed analytical method utilizing generating functions does not coincide with the results obtained using the maximum matching algorithm before node removal. As such, our proposed methods are inadequate for predicting the minimum fraction of driver nodes under node removal for these networks. When targeted node removal is based on in-degree and out-degree with $\alpha = 10$, our approximation method assumes that nodes are removed in descending order of in-degree and out-degree. However, the assumption does not reflect the actual removal process, as we recalculated the removal probabilities to choose nodes at each step. This discrepancy is one of the reasons for the inaccurate results obtained. Moreover, we acknowledge that further improvements are required to enhance the method's efficacy. Notably, the numerical solution of the predicted outcomes can be challenging to obtain, particularly when attempting to acquire the results for SFs with some other parameters.

The approximation of node removals based on in- or out-degree involves an assumption that the in-degree distribution and out-degree distribution evolve independently. However, the assumption requires further investigation to ensure its validity. To address this issue, an avenue of promising research involves examining the relationship between in-degree and out-degree distributions through the randomization of networks. Such analyses may provide upper and lower bounds for analytical methods, contributing to the improvement of predictions about network controllability under targeted attacks based on in-degree and out-degree.

In the future, we aim to broaden the scope of our findings by including other types of node attacks, specifically localized node attacks, as documented in [28]. Furthermore, we intend to verify our conclusions on a more comprehensive collection of real-world networks and various types of networks, such as interdependent networks. We also plan to apply additional prediction techniques, such as machine learning methods, to assess network controllability under node removals concerning in-degree and out-degree.

Abbreviations

The following abbreviations are used in this manuscript:

ER	Erdös-Rényi networks
SSNs	Swarm Signal networks
SFs	Scale-free networks
RMSE	Root Mean Square Error

Appendix A. The Simulation Results Based on Different α Values

The following figures demonstrate for $\alpha = 0$, $\alpha = 1$, $\alpha = 10$ and $\alpha = 100$ how the minimum fraction of driver nodes changes under targeted attacks based on degree, in-degree and out-degree for ER networks and SSNs. We find that the results of $\alpha = 10$ and $\alpha = 100$ overlap.
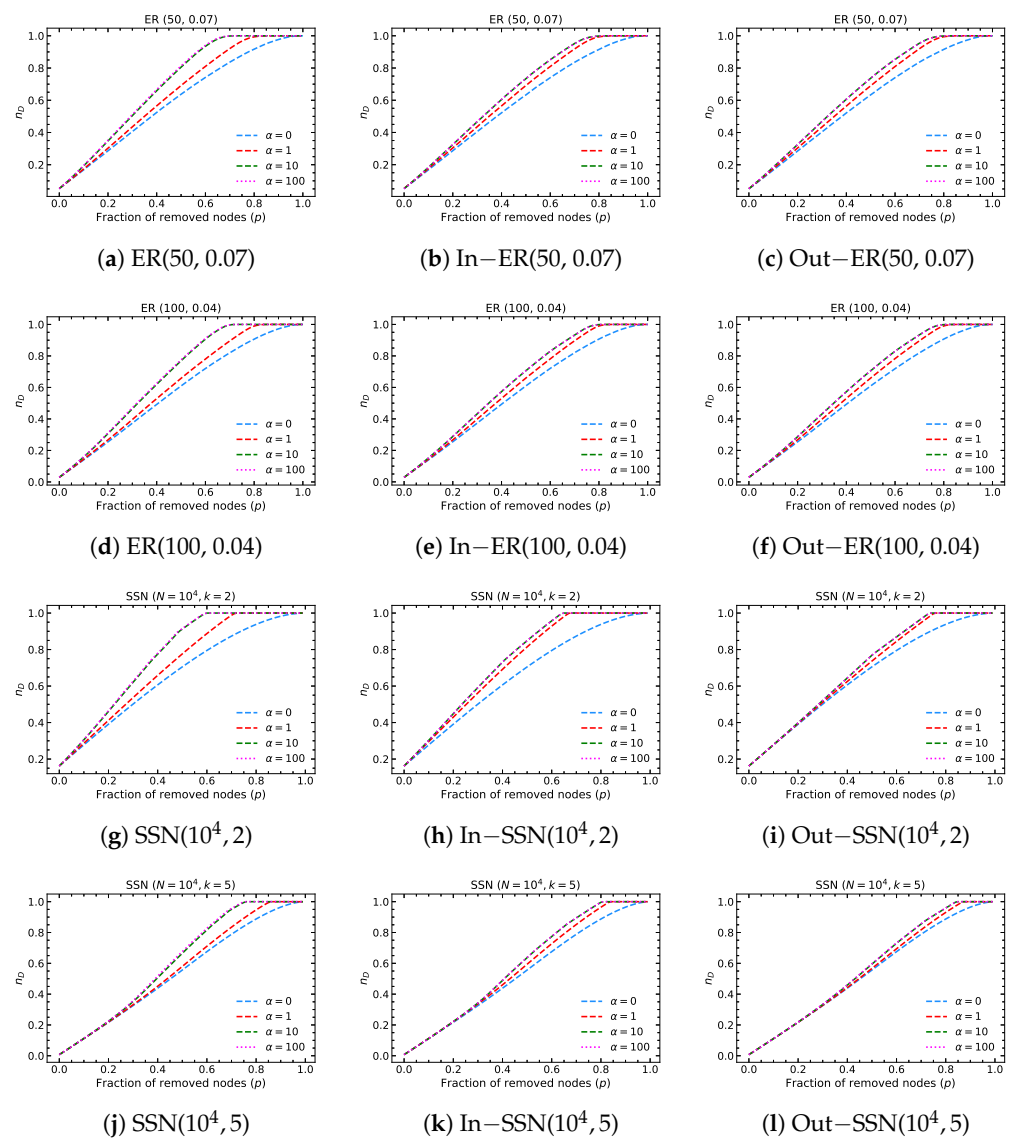

(a) ER(50, 0.07) **(b)** In−ER(50, 0.07) **(c)** Out−ER(50, 0.07)

(d) ER(100, 0.04) **(e)** In−ER(100, 0.04) **(f)** Out−ER(100, 0.04)

(g) SSN(10^4, 2) **(h)** In−SSN(10^4, 2) **(i)** Out−SSN(10^4, 2)

(j) SSN(10^4, 5) **(k)** In−SSN(10^4, 5) **(l)** Out−SSN(10^4, 5)

Figure A1. The minimum fraction of driver nodes n_D during targeted node removal based on in-degree and out-degree with $\alpha = 0$, $\alpha = 1$, $\alpha = 10$ and $\alpha = 100$ for different kinds of networks. The results are the average n_D calculated by the maximum matching algorithm over 10,000 realizations of real-world networks and 1000 realizations of model networks. The blue, orange, and green dashed lines are the results of simulations with $\alpha = 0$, $\alpha = 1$ and $\alpha = 10$ separately. The pink dotted lines are obtained by the simulation results with $\alpha = 100$.

Appendix B. Comparison with Node Removal Based on Degree with $\alpha = 1$

We present the results of four types of node removal strategies: random removal, targeted node removal based on the total degree with $\alpha = 1$, targeted node removal based on in-degree with $\alpha = 1$, and targeted node removal based on out-degree with $\alpha = 1$ for three networks in Figure A2. We find that the three targeted node removal strategies are more disruptive than random removal. However, the effectiveness of the targeted node removal strategies varies depending on the network structure. For instance, in ER(100,0.04), all three targeted node removal strategies show similar performance. In SSN($10^4, 2$), the targeted node removal based on in-degree is the most disruptive; whereas, in HinerniaGlobal, the targeted node removal based on out-degree is the most disruptive.
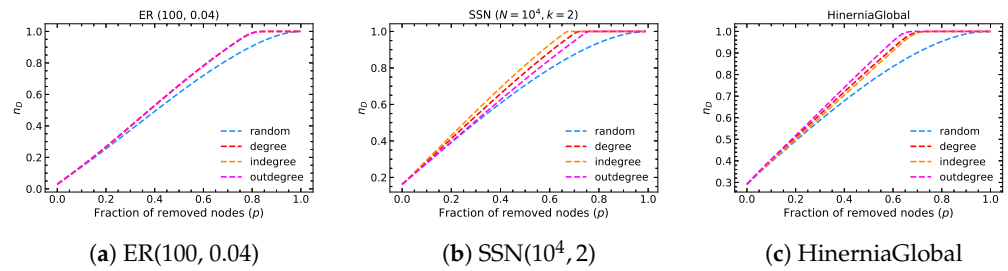

(a) ER(100, 0.04)	**(b)** SSN(10^4, 2)	**(c)** HinerniaGlobal

Figure A2. The minimum fraction of driver nodes n_D during random removal and targeted node removal based on degree, in-degree and out-degree with $\alpha = 1$ for three networks. The results are the average n_D calculated by the maximum matching algorithm over 10,000 realizations of HinerniaGlobal and 1000 realizations of ER(100, 0.04) and SSN($10^4, 2$). The blue, red, orange and pink dashed lines are the results of simulations with random removal, target removal based on the total degree with $\alpha = 1$, target removal based on in-degree with $\alpha = 1$ and target removal based on out-degree with $\alpha = 1$ separately.

Appendix C. Another Real-World Network Results

In this study, the real-world graphs utilized have an average degree ranging from 2 to 3. To further evaluate the efficacy of the proposed techniques, we selected a network from the Topology Zoo dataset, namely BtNorthAmerica, which possesses an average total degree of 4.22. The network under consideration comprises 36 nodes and 76 links. We analyzed the controllability of the network under node removals concerning node in-degree and out-degree with different α. The results are presented in Figure A3 and Tables A1 and A2. Our findings suggest that the predicted values of the proposed methods are valid. It is worth mentioning that, when $\alpha = 10$, attacks based on out-degree at the onset are not as deleterious as random removals. Removing the node with the highest out-degree in the initial steps results in a lower average number of driver nodes than removing other nodes, on average.

Table A1. The RMSE between the analytical results of random removals and the simulation results under random removals, target removals with $\alpha = 1$ and $\alpha = 10$, respectively, while removing 10% of the nodes. The analytical method for random removals is from the reference [19].

Network	Random	$\alpha = 1$			$\alpha = 10$		
		Indegree	Outdegree	Degree	Indegree	Outdegree	Degree
BtNorthAmerica	0.0097	0.0140	0.0104	0.0121	0.0117	0.0096	0.0101

Table A2. The RMSE between the analytical results of the proposed analytical methods and the simulation results under different kinds of removals while removing 10% of the nodes. The analytical methods for random removals and targeted node removals based on the total degree are from the reference [19].

Network	Random	$\alpha = 1$			$\alpha = 10$		
		Indegree	Outdegree	Degree	Indegree	Outdegree	Degree
BtNorthAmerica	0.0097	0.0126	0.0175	0.0091	0.0538	0.0612	0.0527

(**a**) In-degree with $\alpha = 1$

(**b**) Out-degree with $\alpha = 1$

(**c**) In-degree with $\alpha = 10$

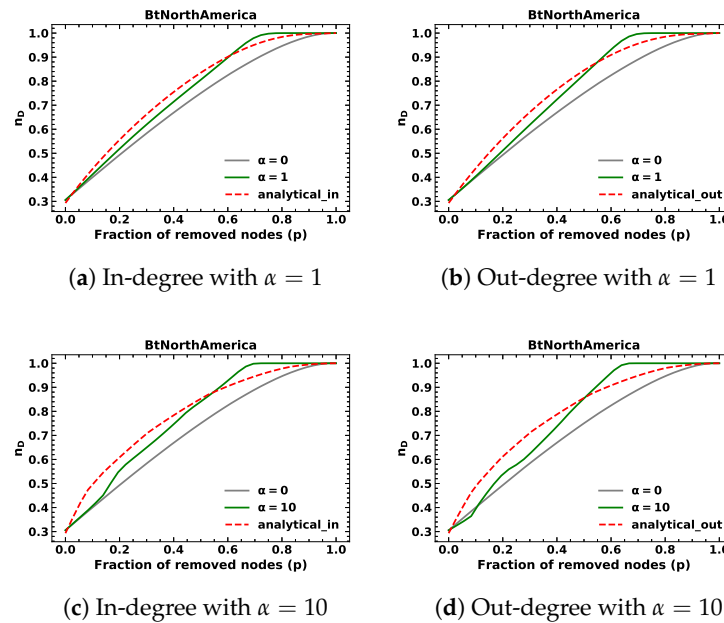(**d**) Out-degree with $\alpha = 10$

Figure A3. The minimum fraction of driver nodes n_D during targeted node removal based on in-degree and out-degree with $\alpha = 1$ and $\alpha = 10$, respectively, for the network BtNorthAmerica.

Appendix D. Analytical Approximation of Random Node Removals about SFs

This section shows the analytical solution for random node removal in SFs. In SFs, the in-degree distribution and out-degree distribution both follow the pure power-law distribution with minimum degree a and exponent γ, which can be denoted as follows:

$$P_{in}(k_{in}) = C_{in}k_{in}^{-\gamma}, \quad P_{out}(k_{out}) = C_{out}k_{out}^{-\gamma}, \tag{A1}$$

where $C_{in} = \frac{1}{\sum_{k_{in}=a}^{\infty} k_{in}^{-\gamma}} = \frac{1}{\zeta(\gamma,a)}$ and $C_{out} = \frac{1}{\sum_{k_{out}=a}^{\infty} k_{out}^{-\gamma}} = \frac{1}{\zeta(\gamma,a)}$, where $\zeta(\gamma,a)$ is the Hurwitz Zeta function, and the average degree $k = \frac{\zeta(\gamma-1,a)}{\zeta(\gamma,a)}$. Correspondingly, the generating functions can be obtained by

$$G_{in}(x) = \frac{x^a \Phi(x,\gamma,a)}{\zeta(\gamma,a)}, \quad G_{out}(x) = \frac{x^a \Phi(x,\gamma,a)}{\zeta(\gamma,a)}, \tag{A2}$$

where $\Phi(z,s,\alpha)$ denotes the Lerch transcendent function.

Together with Equations (9) and (10), the fraction of the minimum number of driver nodes n_D after randomly removing a fraction p nodes can be calculated by

$$
\begin{aligned}
n_D = {} & \frac{(1-p)(-p\omega_2 + p + \omega_2)^a \Phi(-p\omega_2 + p + \omega_2, \gamma, a)}{\zeta(\gamma, a)} + \\[2mm]
& \frac{(1-p)\Phi\left(\frac{(p-1)\Phi(-p\omega_2 + p + \omega_2, \gamma-1, a)(-p\omega_2 + p + \omega_2)^{a-1}}{\zeta(\gamma-1, a)} + 1, \gamma, a\right)}{\zeta(\gamma, a)} \\[2mm]
& \times \left(\frac{(p-1)(-p\omega_2 + p + \omega_2)^{a-1}\Phi(-p\omega_2 + p + \omega_2, \gamma-1, a)}{\zeta(\gamma-1, a)} + 1\right)^a \\[2mm]
& + \frac{k(2p-1-p^2)(\omega_2 - 1)(-p\omega_2 + p + \omega_2)^{a-1}\Phi(-p\omega_2 + p + \omega_2, \gamma-1, a)}{\zeta(\gamma-1, a)} + 2p - 1
\end{aligned}
\tag{A3}
$$

where $1 - \omega_2 - \bar{H}_{out}(1 - \bar{H}_{in}(\omega_2)) = 0$.

References

1. Wu, L.; Li, M.; Wang, J.X.; Wu, F.X. Controllability and its applications to biological networks. *J. Comput. Sci. Technol.* **2019**, *34*, 16–34. [CrossRef]
2. Rinaldi, M. Controllability of transportation networks. *Transp. Res. Part B Methodol.* **2018**, *118*, 381–406. [CrossRef]
3. Solimine, P.C. Network Controllability Metrics for Corruption Research. In *Corruption Networks*; Granados, O.M., Nicolás-Carlock, J.R., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 29–50. [CrossRef]
4. Kalman, R.E. Mathematical Description of Linear Dynamical Systems. *J. Soc. Ind. Appl. Math. Ser. A Control* **1963**, *1*, 152–192.
5. Lin, C.T. Structural controllability. *IEEE Trans. Autom. Control* **1974**, *19*, 201–208. [CrossRef]
6. Liu, Y.Y.; Slotine, J.J.; Barabási, A.L. Controllability of complex networks. *Nature* **2011**, *473*, 167–173. [CrossRef]
7. Cowan, N.J.; Chastain, E.J.; Vilhena, D.A.; Freudenberg, J.S.; Bergstrom, C.T. Nodal Dynamics, Not Degree Distributions, Determine the Structural Controllability of Complex Networks. *PLoS ONE* **2012**, *7*, e38398. [CrossRef]
8. Yuan, Z.; Zhao, C.; Di, Z.; Wang, W.X.; Lai, Y.C. Exact controllability of complex networks. *Nat. Commun.* **2013**, *4*, 2447. [CrossRef]
9. Van Mieghem, P.; Doerr, C.; Wang, H.; Hernandez, J.M.; Hutchison, D.; Karaliopoulos, M.; Kooij, R. *A Framework for Computing Topological Network Robustness*; Report20101218; Delft University of Technology: Delft, The Netherlands, 2010; pp. 1–15. [CrossRef]
10. Pu, C.L.; Pei, W.J.; Michaelson, A. Robustness analysis of network controllability. *Phys. A Stat. Mech. Its Appl.* **2012**, *391*, 4420–4425. [CrossRef]
11. Lu, Z.M.; Li, X.F. Attack Vulnerability of Network Controllability. *PLoS ONE* **2016**, *11*, e0162289. [CrossRef]
12. Wang, L.; Zhao, G.; Kong, Z.; Zhao, Y. Controllability and Optimization of Complex Networks Based on Bridges. *Complexity* **2020**, *2020*, 6695026. [CrossRef]
13. Sun, P.; Kooij, R.E.; Van Mieghem, P. Reachability-Based Robustness of Controllability in Sparse Communication Networks. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 2764–2775. [CrossRef]
14. Lou, Y.; Wang, L.; Chen, G. A Framework of Hierarchical Attacks to Network Controllability. *Commun. Nonlinear Sci. Numer. Simul.* **2021**, *98*, 105780. [CrossRef]
15. 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]
16. Lou, Y.; Yang, D.; Wang, L.; Tang, C.B.; Chen, G. Controllability Robustness of Henneberg-Growth Complex Networks. *IEEE Access* **2022**, *10*, 5103–5114. [CrossRef]
17. Zhang, Z.; Yin, Y.; Zhang, X.; Liu, L. Optimization of robustness of interdependent network controllability by redundant design. *PLOS ONE* **2018**, *13*, e0192874. [CrossRef]
18. Chen, A.; Sun, P.; Kooi, R.E. The Recoverability of Network Controllability. In Proceedings of the 2021 5th International Conference on System Reliability and Safety (ICSRS), Palermo, Italy, 24–26 November 2021; pp. 198–208. [CrossRef]
19. Wang, F.; Kooij, R. Robustness of Network Controllability with Respect to Node Removals. In *Proceedings of the Complex Networks and Their Applications XI*; Cherifi, H., Mantegna, R.N., Rocha, L.M., Cherifi, C., Micciche, S., Eds.; Springer International Publishing: Cham, Switzerland, 2023; pp. 383–394. [CrossRef]
20. Dhiman, A.; Sun, P.; Kooij, R. Using Machine Learning to Quantify the Robustness of Network Controllability. In *Machine Learning for Networking*; Springer International Publishing: Cham, Switzerland, 2021; pp. 19–39. [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.; He, Y.; Wang, L.; Tsang, K.F.; Chen, G. Knowledge-Based Prediction of Network Controllability Robustness. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**, *33*, 5739–5750. [CrossRef]
23. 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. [CrossRef]
24. Komareji, M.; Bouffanais, R. Resilience and Controllability of Dynamic Collective Behaviors. *PLoS ONE* **2013**, *8*, e82578. [CrossRef]
25. Barabási, A.L.; Albert, R. Emergence of Scaling in Random Networks. *Science* **1999**, *286*, 509–512. [CrossRef]
26. Knight, S.; Nguyen, H.X.; Falkner, N.; Bowden, R.; Roughan, M. The Internet Topology Zoo. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 1765–1775. [CrossRef]

27. Hopcroft, J.E.; Karp, R.M. An n^5/2 algorithm for maximum matchings in bipartite graphs. *SIAM J. Comput.* **1973**, *2*, 225–231. [CrossRef]

28. Kenett, D.Y.; Gao, J.; Huang, X.; Shao, S.; Vodenska, I.; Buldyrev, S.V.; Paul, G.; Stanley, H.E.; Havlin, S., Network of Interdependent Networks: Overview of Theory and Applications. In *Networks of Networks: The Last Frontier of Complexity*; Springer International Publishing: Cham, Switzerland, 2014; pp. 3–36. [CrossRef]

29. Shao, J.; Buldyrev, S.V.; Braunstein, L.A.; Havlin, S.; Stanley, H.E. Structure of shells in complex networks. *Phys. Rev. E* **2009**, *80*, 036105. [CrossRef] [PubMed]