Robustness of Network Controllability with Respect to Node Removals

Fenghua Wang and Robert Kooij

Abstract Network controllability and its robustness has been widely studied. However, analytical methods to calculate network controllability with respect to node removals are currently lacking. This paper develops methods, based upon generating functions for the in- and out-degree distributions, to approximate the minimum number of driver nodes needed to control directed networks, during random and targeted node removals. By validating the proposed methods on synthetic and real-world networks, we show that our methods work very well in the case of random node removals and reasonably well in the case of targeted node removals, in particular for moderate fractions of attacked nodes.

Keywords Controllability · Complex networks · Node failures · Node attacks

1 Introduction

Network controllability has been investigated for different kinds of networks, like biological networks [1], transportation networks [2] and corruption networks [3]. A network is controllable if the states of nodes can be steered to any expected states in a finite time by imposing external inputs to some of the nodes. Kalman's controllability rank condition is used to judge whether a linear system is controllable or not [4]. However, sometimes we do not know the weighted interactions within the network, which describe the strength with which a node affects other nodes. To overcome the issue, the concept of structural controllability has been proposed [5].

F. Wang (✉)
Delft University of Technology, 2628 CD, Delft, The Netherlands
e-mail: F.Wang-8@tudelft.nl
URL: https://nas.ewi.tudelft.nl/index.php/fenghua-wang

R. Kooij
TNO, Unit ICT, 2595 DA, Den Haag, The Netherlands
e-mail: R.E.Kooij@tudelft.nl
URL: https://nas.ewi.tudelft.nl/index.php/rob-kooij

H. Cherifi et al. (eds.), *Complex Networks and Their Applications XI*,
Studies in Computational Intelligence 1078,
https://doi.org/10.1007/978-3-031-21131-7_30

The interaction matrix and input matrix of the linear time-invariant system are structural if their elements are independently free parameters or some are fixed zeros. The system is called structurally controllable if it is possible to find values of structural interaction and input matrices to make the system satisfy the usual controllability condition. Besides investigating the necessary and sufficient conditions to make the specific system strong structural controllable [6], another research direction is to find the minimum set of inputs to make the system fully controllable [7]. Liu et al. [8] reduce the structural controllability problem into the optimization problem of finding a set of unmatched nodes in a maximum matching of the network. The nodes where the external input signals are imposed are named driver nodes. The number of unmatched nodes equals the minimum number of driver nodes needed to fully control the network. Note that the results reported in Liu et al. [8] critically depend on the assumption that the direct network has no self-links, i.e. a node's internal state can only be changed upon interaction with neighboring nodes [9]. We will follow this assumption throughout the paper.

Network structural controllability as a generic system property is applied to measure and enhance network robustness. Measuring network robustness is usually done by measuring network performance changes during perturbations imposed upon the network [10]. The widely adopted perturbations in the research of the robustness of network controllability are random node or link removal, which are used as a benchmark compared with other perturbations. Another kind of perturbation deals with targeted attack strategies. For example, attack strategies can relate to network topology features, such as betweenness, degree and closeness. Pu et al. [11] demonstrate that degree-based attacks are more harmful to network controllability compared to random attacks. Lu et al. [12] find that a betweenness-based attack strategy is more harmful than a degree-based attack strategy in most real-world networks. However, Wang et al. [13] find that attacking bridge links, whose removal results in a disconnected network, is an effective way to destroy network controllability. Another kind of targeted attack strategy is based on critical nodes and links. Critical nodes and links are defined through the property that their removal will increase the number of driver nodes [8]. Sun et al. [14] report random attack under the protection of critical links is less efficient than a random link attack, and a targeted attack aiming at critical links is more harmful than a random attack. Lou et al. [15] propose a hierarchical attack removal framework where nodes or links are classified into critical, sub-critical and normal categories. They find that hierarchical attack strategies are more efficient than some metric-based attack strategies such as betweenness- or degree-based strategies in interdependent networks. There is also some research focusing on how to enhance the robustness of network controllability. Giulia et al. [16] show that network controllability is determined by the density of nodes with in-degree and out-degree equal to one or two. Adding links to low degree nodes is beneficial to network controllability. Lou et al. [17] find that multi-loop structures can improve the robustness of network controllability. Zhang et al. [18] investigate different redundant design strategies of interdependent networks. They present that betweenness-based strategy and degree-based strategy for node backup and high degree first strategy for edge backup can optimize robustness of network controllability.

Besides the aforementioned qualitative research on the robustness of network controllability, quantitative research has been conducted. Lu et al. [12] develop the numerical approximations of random node attacks and target node attacks based on degree on Erdös-Rényi (ER) networks. The results fit well when the fraction of nodes is below 20%. Sun et al. [14] explore the closed-form approximation of the number of controllable nodes under random link attacks, targeted attacks and random attacks with protection. Dhiman et al. [19] use machine learning to quantify the minimum fraction of driver nodes under random link attacks and target link attacks, which performs better than the closed-form approximation proposed by Sun et al. [14]. Later, Chen et al. [20] develop analytical approximations for the minimum number of driver nodes during random link removal by using methods based on generating functions.

However, to our knowledge, analytical methods to approximate the network controllability during random and targeted node removal on different kinds of networks are lacking. The framework to calculate the structural controllability of linear systems for directed networks has been proposed by Liu et al. [8]. This paper uses their framework to develop analytical approximations based on degree distributions to calculate the minimum fraction of driver nodes during node removal. We choose two cases for the removal of nodes: random node removal and targeted node removal, based upon the node degrees. In order to validate our methods, we use two types of synthetic networks and four real-world communication networks.

This paper is organized as follows. The second section introduces the networks used in the study for validation. The analytical results for the robustness of network controllability during random node removal are presented in the third section. The fourth section shows the results for the robustness of network controllability for targeted node removal. The final section reports the conclusion and discussion.

2 Network Data

We will validate our theoretical results, which will be derived in the subsequent sections, on two classes of synthetic networks and on a number of real-world networks. In this section, we give details on the used networks.

2.1 Directed Synthetic Networks

We choose two kinds of synthetic networks: Erdös-Rényi (ER) networks and Swarm Signalling networks (SSNs).

We generate a directed ER network on N nodes, by placing a directed link between any pair of nodes, with a given probability p_{ER}. The average number of links for such ER networks satisfies $L = N(N-1)p_{ER}$. In this paper we have used two ER networks, with $N = 50$, $p_{ER} = 0.07$ and $N = 100$, $p_{ER} = 0.04$.

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

The topology for Swarm Signalling Networks (SSNs) that we use was suggested in [21]. The SSN has a regular out-degree, while the in-degree distribution follows a Poisson distribution. To generate SSNs, we need two parameters. One is the number of nodes N, and the other is the out-degree value k. For each node, the node randomly creates k outgoing links to other nodes. In this paper we have used two SSNs, both with $N = 10^4$ and with $k = 2$ and $k = 5$.

2.2 Real-World Networks

The real-world networks used in this study are taken from the Internet Topology Zoo [22], a collection of real-world communication networks. We change those undirected networks into directed networks by using two attributes: source node and target node [14]. The properties of the networks are shown in Table 1, which shows the number of nodes N, the number of links L, and the average total degree $< k >$. The total degree is the sum of the in-degree and the out-degree. Obviously, the average in-degree equals the average out-degree and therefore the average total degree is twice the average in-degree (and hence the average out-degree).

3 Minimum Fraction of Driver Nodes Under Random Node Removals

This section presents how to analytically approximate network controllability in the case of random node removals.

3.1 Analytical Approximation

3.1.1 General Networks

From [8], for directed network $\mathcal{G}(N, L)$ with N nodes and L links, we can determine the minimum number of driver nodes by using generating functions of the in- and

out-degree distributions ($G_{in}(x)$ and $G_{out}(x)$, respectively) and of the excess in- and out-degree distributions ($H_{in}(x)$ and $H_{out}(x)$, respectively). These generating functions are defined as follows:

$$\begin{aligned} G_{in}(x) &= \sum_{k=0}^{\infty} P_{in}(k_{in}) x^{k_{in}}, \; G_{out}(x) = \sum_{k=0}^{\infty} P_{out}(k_{out}) x^{k_{out}}, \\ H_{in}(x) &= \frac{\sum_{k=1}^{\infty} k_{in} P_{in}(k_{in}) x^{k_{in}-1}}{< k_{in} >} = \frac{G'_{in}(x)}{G'_{in}(1)}, \\ H_{out}(x) &= \frac{\sum_{k=1}^{\infty} k_{out} P_{out}(k_{out}) x^{k_{out}-1}}{< k_{out} >} = \frac{G'_{out}(x)}{G'_{out}(1)}, \end{aligned} \tag{1}$$

where k_{in} and k_{out} denote in- and out-degree, respectively, while $P_{in}(\cdot)$ and $P_{out}(\cdot)$ are in- and out-degree probability distribution, respectively. Then the minimum fraction of driver nodes is given by:

$$\begin{aligned} n_d = \frac{1}{2}\{&G_{in}(\omega_2) + G_{in}(1-\omega_1) - 2 + G_{out}(\hat{\omega_2}) + G_{out}(1-\hat{\omega_1}) \\ &+ k[\hat{\omega_1}(1-\omega_2) + \omega_1(1-\hat{\omega_2})]\}, \end{aligned} \tag{2}$$

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

$$\omega_1 = H_{out}(\hat{\omega_2}), \omega_2 = 1 - H_{out}(1-\hat{\omega_1}), \hat{\omega_1} = H_{in}(\omega_2), \hat{\omega_2} = 1 - H_{in}(1-\omega_1), \tag{3}$$

and k denotes half of the average degree equal to the average in-degree and the average out-degree, $k = \frac{1}{2} < k > = < k_{in} > = < k_{out} >$.

During the node removal process, the set of driver nodes includes two parts. One is the set containing N_D driver nodes that control the remaining part of the network, and the other set is formed by N_r removed nodes. We assume that each removed node needs to be controlled by an individual driver node. We define the fraction of driver nodes n_D as $n_D = \frac{N_D + N_r}{N}$. After randomly removing a fraction p of nodes in the network, the fraction of driver nodes n_D satisfies

$$n_D = \frac{n_d(1-p)N + pN}{N} = n_d(1-p) + p. \tag{4}$$

Based on the research of Shao et al. [23], the generating function after randomly removing a fraction p nodes corresponds to the original generating function, with the adjusted argument $\bar{x} = p + (1-p)x$. Then the generating functions of in- and out-degree, and the excess in- and out-degree, after randomly removing a fraction p of nodes, are adjusted as follows:

$$\bar{G}_{in}(x) = G_{in}(p + (1-p)x), \quad \bar{G}_{out}(x) = G_{out}(p + (1-p)x),$$
$$\bar{H}_{in}(x) = \frac{\bar{G}'_{in}(x)}{\bar{G}'_{in}(1)}, \quad \bar{H}_{out}(x) = \frac{\bar{G}'_{out}(x)}{\bar{G}'_{out}(1)}. \tag{5}$$

Next, we use Eqs. (2) and (4) to acquire the fraction of minimum number of nodes n_D after randomly removing a fraction p of nodes:

$$\begin{aligned} n_D = \frac{1}{2}(1-p)\{&\bar{G}_{in}(\omega_2) + \bar{G}_{in}(1-\omega_1) - 2 + \bar{G}_{out}(\hat{\omega}_2) + \bar{G}_{out}(1-\hat{\omega}_1) \\ &+ k(1-p)[\hat{\omega}_1(1-\omega_2) + \omega_1(1-\hat{\omega}_2)]\} + p, \end{aligned} \tag{6}$$

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

$$\omega_1 = \bar{H}_{out}(\hat{\omega}_2), \quad \omega_2 = 1 - \bar{H}_{out}(1-\hat{\omega}_1), \quad \hat{\omega}_1 = \bar{H}_{in}(\omega_2), \quad \hat{\omega}_2 = 1 - \bar{H}_{in}(1-\omega_1), \tag{7}$$

and k is half of the average degree equal to the average in-degree and the average out-degree, $k = \frac{1}{2} <k> = <k_{in}> = <k_{out}>$.

3.1.2 ER Networks

Both the in-degree distribution $P_{in}(k_{in})$ and the out-degree distribution $P_{out}(k_{out})$ of ER networks follow a Poisson distribution with average degree k [20]. Therefore, the generating functions of in-degree and out-degree are as follows,

$$G_{in}(x) = e^{-k(-x+1)}, G_{out}(x) = e^{-k(-x+1)}. \tag{8}$$

The minimum fraction of driver nodes n_D after a fraction p of nodes is randomly removed in the ER networks can be obtained through Eq. (6) as

$$n_D = p + p\omega_2 - \omega_2 + [1 - p + k(1-p)^2(1-\omega_2)]e^{k(1-p)(\omega_2-1)} \tag{9}$$

where ω_2 satisfies $1 - \omega_2 - e^{-k(1-p)e^{-k(1-p)(1-\omega_2)}} = 0$.

3.1.3 SSNs

In a SSN with the number of nodes N and average in-degree and out-degree equal to k, the in-degree distribution resembles a Poisson distribution with mean value k and the out-degree distribution follows a Dirac delta function. Then the generating functions of in-degree and out-degree distribution can be denoted as follows,

$$G_{in}(x) = e^{-k(-x+1)}, G_{out}(x) = x^k. \tag{10}$$

Based on Eq. (6), the minimum fraction of driver nodes n_D after randomly removing a fraction p of nodes can be calculated by

$$n_D = p + p\omega_2 - \omega_2 + [1 - p + (k-1)(1-p)^2(1-\omega_2)]e^{k(1-p)(\omega_2-1)} \tag{11}$$

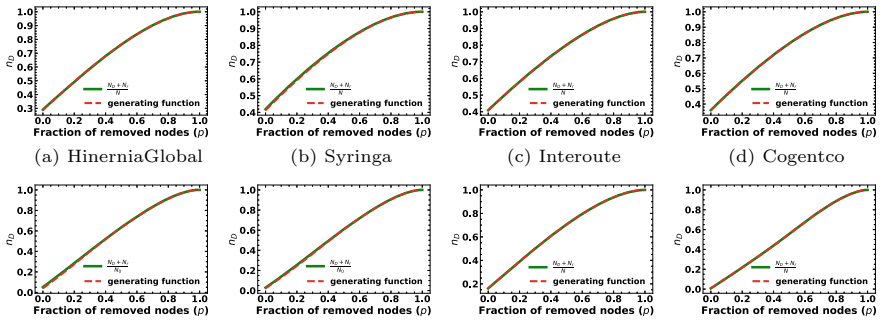
where ω_2 satisfies $1 - \omega_2 - [p + (1-p)(1 - e^{-k(1-p)(1-\omega_2)})]^{k-1} = 0$.

Note that for the real-world networks, the generating functions for the in- and out-degree distributions, can simply be obtained from the histograms of these distributions. We use the relative frequency of degree as the corresponding probability in generating functions.

3.2 Validation

We ran simulations on the various networks described in Sect. 2. Specifically, for each communication network, we do 10,000 realizations, and in each realization, we remove a node randomly at each step until all nodes have been removed. For each kind of synthetic network, we heuristically choose two pairs of parameters: ER networks with $N = 50$, $p = 0.07$ and $N = 100$, $p = 0.04$ and SSNs with $N = 10^4$, $k = 2$ and $N = 10^4$, $k = 5$. In each realization, we generate a synthetic network, given its parameters, and remove nodes one by one randomly. After removing a node, we recalculate the minimum fraction of driver nodes using the maximum matching algorithm. However, as our SSNs have a large number of nodes, we remove 1% of the original number of nodes at each step. We do 10,000 realizations for each synthetic network as well. Then we obtain the average minimum fraction of driver nodes. The green lines in Fig. 1 show the simulation results.

Since we know each network's in-degree and out-degree distributions, we can compute the minimum fraction of driver nodes of a network according to the equations mentioned above for the minimum fraction n_D. The results obtained using the



(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)

Fig. 1 The minimum fraction of driver nodes n_D during random node removal in different kinds of networks. The green lines are calculated by the maximum matching algorithm over 10,000 realizations. The red dashed lines are obtained by the analytical methods

generating functions of the degree distributions are depicted as red dashed lines in Fig. 1.

The results are shown in Fig. 1. As the predicted values in the red lines and the simulated values virtually overlap, we conclude that the analytical approximations for network controllability in the case of random node removals are very accurate. The reason for this is that, after removing a fraction p of the nodes at random, we still have expressions for the generating functions of the in- and out-degree distributions, see Eq. (5).

4 Minimum Fraction of Number of Driver Nodes Under Targeted Node Removals

Degree centrality has been deeply investigated in the context of network robustness [24]. Nodes with a high degree have a large influence on network functioning and might be assumed to have a high probability of being attacked. We will explore how to analytically approximate network controllability during targeted degree-based node removals.

We assume that for node attacks, the probability of attacking a node, is proportional to some power of its degree. Because we consider directed graphs $\mathcal{G}(N, L)$, with node set $\mathcal{N}$, there are three types of node degree: in-degree, out-degree and total degree. In this paper we will only consider node attacks based upon total degree. If we denote the probability of removing node i with total degree k_i as p_i, we have $p_i = \frac{{k_i}^\alpha}{\sum_{j\in\mathcal{N}} {k_j}^\alpha}$. For $\alpha = 0$, each node has the same probability of being removed, hence for this case targeted node removal corresponds to random node removal, as discussed in Sect. 3. If $\alpha > 0$, the node with a larger degree has a higher probability of being removed; when $\alpha < 0$, the node with the smaller degree has a higher probability of being removed. In this section, we focus on analyzing the results with $\alpha > 0$. Specifically, we consider two cases: $\alpha = 1$ and $\alpha = 10$.

4.1 Analytical Approximation

4.1.1 Case: $\alpha = 1$

The main challenge is to obtain expressions for the generating functions for the in- and out-degree distributions after removing a fraction p of the nodes through attacks. In general, it is not possible to obtain the generating function both for the in- and the out-degree distribution, after a fraction p of nodes has been attacked. Therefore we have to come up with a heuristic to deal with this. Here we will map the targeted node attack process (based upon total degree) into a random node attack process. We suppose that the generating functions of in-degree distribution and out-degree distribution change to those corresponding to random node removal, but such that

the total number of links after randomly removing a fraction $\bar{p}$ of nodes is equal to the total number of links after targeted removal of a fraction p of the nodes. As reported in [24], the fraction $\bar{p}$ can be calculated by

$$\bar{p} = 1 - \frac{f G'_\alpha(f)}{< k >}, \tag{12}$$

where $f \equiv G_\alpha^{-1}(1-p)$, $G_\alpha(x) \equiv \sum_k p_k x^{k^\alpha}$ and $< k >$ is the average total degree of the initial network and p_k is the probability of total degree k. If $\alpha = 1$, $G_\alpha(x) \equiv \sum_k p_k x^k$, which is the generating function for the total degree distribution. For ER networks, the generating function of total degree is $G(x) = e^{-<k>(-x+1)}$ and for SSNs, the generating function of total degree is $G(x) = x^{\frac{<k>}{2}} e^{-\frac{<k>}{2}(-x+1)}$.

4.1.2 Case: $\alpha = 10$

The interesting part of parameter α is that when α approaches ∞, the order of removed nodes follows the rank of node degree values in descending order. At each step, the node with the largest degree will be removed. In the simulations, we adopted large values of α, and we found that the results for $\alpha = 10$ are the same as the results for $\alpha = 100$, which means the result for $\alpha = 10$ is representative for the case $\alpha = \infty$.

We want to develop an analytical method to estimate the corresponding network controllability for $\alpha = 10$. We map the fraction p of removed nodes under targeted attacks for $\alpha = 10$ onto the effective proportion $\bar{p}$ of nodes under random node attack. Under the attack strategy to remove the largest degree node at each step, total degree of all removed nodes can be obtained according to the degree distribution after giving the removed fraction p. The effective proportion $\bar{p}$ is the total degree of all removed nodes normalizing by the total degree of all nodes in the initial network, which can be calculated as $\bar{p} = \frac{\sum_{k=k_{max}}^{k=\bar{k}} p_k N k}{N<k>} = \frac{\sum_{k=k_{max}}^{k=\bar{k}} p_k k}{<k>}$, where the largest degree value is denoted as k_{max}, the probability of removed nodes with degree k is denoted as p_k and degree $\bar{k}$ satisfies $\sum_{k=k_{max}}^{k=\bar{k}} p_k = p$. Similarly, except removed probability $p_{\bar{k}}$, other probability p_k is equal to probability $P(k)$ in the generating function. Then the minimum number of driver nodes can be approximated by replacing argument p by $\bar{p}$ in Eqs. (5)–(6).

4.2 Validation

4.1.2 $\alpha = 1$

We choose the same network set to do simulations under targeted node removal, based on total degree. When using the maximum matching algorithm to calculate

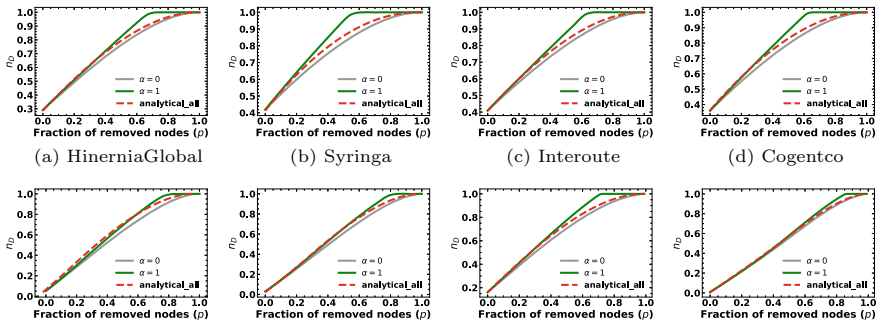
the minimum fraction of the number of driver nodes, we recalculate the fraction value n_D after removing nodes for each kind of targeted attack with $\alpha = 1$. We do 10,000 realizations for each communication network and 1000 realizations for each synthetic network. The simulation results are presented as green lines in Fig. 2. For the analytical method, we employ the effective fraction of removed nodes $\bar{p}$ acquired by Eq. (12). Red lines in Fig. 2 represent the analytical results. We also show the simulation results under random node removals in grey lines in Fig. 2.

We find that the analytical results are a reasonable fit with the simulations, especially for small values of the fraction p of attacked nodes. It indicates that the proposed method of calculating the effective proportion $\bar{p}$ is inaccurate in the late removal stage.

4.2.2 $\alpha = 10$

Analogously, we do the simulations with $\alpha = 10$ under total degree targeted node removal, 10000 realizations for each communication network and 1000 realizations for each synthetic network. The simulation results are shown in the green lines. We present the analytical results in red lines. The simulation results of network controllability under random node attacks are depicted in grey lines. The results with $\alpha = 10$ of total degree target node removal are shown in Fig. 3.

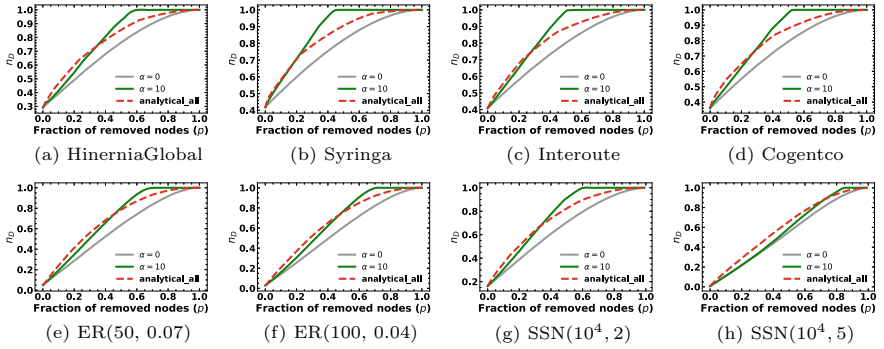
The proposed approaches for the case $\alpha = 10$ can approximate network controllability in a closed-form but do not perfectly fit the simulation results. The analytical result lines are first above the targeted attack lines, then below the targeted attack lines but still above the random attack lines, until the fraction of removed nodes approaches one.



(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)

Fig. 2 The minimum fraction of driver nodes n_D during targeted node removal based on the total degree with $\alpha = 1$ in different kinds of networks. The green and grey lines are the average n_D calculated by the maximum matching algorithm over 10,000 realizations of real networks and 1000 realizations of synthetic networks. The grey lines are the results of simulations under random node removal ($\alpha = 0$), and the green lines are the results of removing nodes with probability based on the degree with $\alpha = 1$. The red dashed lines are obtained by the analytical approximation approach



(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)

Fig. 3 The minimum fraction of driver nodes n_D during targeted node removal based on the total degree with $\alpha = 10$ in different kinds of networks. The green and grey lines are the average n_D calculated by the maximum matching algorithm over 10,000 realizations of real networks and 1000 realizations of synthetic networks. The grey lines are the results of simulations under random node removal ($\alpha = 0$), and the green lines present the results of removing nodes with probability based on the degree with $\alpha = 10$. The red dashed lines are obtained by the analytical approximation methods

5 Conclusion and Discussion

In this study, we propose analytical methods, based on generating functions, to compute the minimum fraction of the number of driver nodes in directed networks, subject to node removals. We find that the analytical methods fit simulation results very well for random node removals. Moreover, we develop analytical methods for two cases during targeted node removal based on different degrees. One is the probability of a removed node in proportion to the degree, and the other is that a node with the largest degree tends to be removed. We find that the proposed analytical methods for targeted node removal fit the simulation results reasonably well, in particular for small values of the fraction of removed nodes.

In the future, we aim to extend our results by also considering node attacks, based on the in-degree or the out-degree of nodes, and localized node attacks, as in [24]. Also, we would like to validate our results on a larger set of networks, both synthetic and real-world networks, such as scale-free networks, small-world networks and power grids.

References

1. Wu, L., Li, M., Wang, J.-X., Wu, F.-X.: Controllability and its applications to biological networks. J. Comput. Sci. Technol. **34**(1), 16–34 (2019)
2. Rinaldi, M.: Controllability of transportation networks. Transp. Res. Part B Methodol. **118**, 381–406 (2018). [Online] Available: https://www.sciencedirect.com/science/article/pii/S0191261518301930

3. Solimine, P.C.: Network controllability metrics for corruption research. In: Corruption Networks, pp. 29–50. Springer (2021)
4. Kalman, R.E.: Mathematical description of linear dynamical systems. J. Society Ind. Appl. Math. Ser. A Control **1**(2), 152–192 (1963) [Online]. Available: https://doi.org/10.1137/0301010
5. Lin, C.-T.: Structural controllability. IEEE Trans. Autom. Control **19**(3), 201–208 (1974)
6. Jia, J., van Waarde, H.J., Trentelman, H.L., Camlibel, M.K.: A unifying framework for strong structural controllability. IEEE Trans. Autom. Control **66**(1), 391–398 (2021)
7. Olshevsky, A.: Minimal controllability problems. IEEE Trans. Control Netw. Syst. **1**(3), 249–258 (2014)
8. Liu, Y.-Y., Slotine, J.-J., Barabási, A.-L.: Controllability of complex networks. Nature **473**(7346), 167–173 (2011)
9. 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 **7**(6), 1–5 (2012)
10. Van Mieghem, P., Doerr, C., Wang, H., Hernandez, J.M., Hutchison, D., Karaliopoulos, M., Kooij, R.: A framework for computing topological network robustness. Delft Univ. Technol. Rep. **20101218**, 1–15 (2010)
11. Pu, C.-L., Pei, W.-J., Michaelson, A.: Robustness analysis of network controllability. Phys. A Stat. Mech. Appl. **391**(18), 4420–4425 (2012) [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378437112003135
12. Lu, Z.-M., Li, X.-F.: Attack vulnerability of network controllability. PLOS ONE **11**(9), 1–27 (2016) [Online]. Available: https://doi.org/10.1371/journal.pone.0162289
13. Wang, L., Zhao, G., Kong, Z., Zhao, Y.: Controllability and optimization of complex networks based on bridges. Complexity, pp. 1–10 (2020) [Online]. Available: https://ideas.repec.org/a/hin/complx/6695026.html
14. Sun, P., Kooij, R.E., Van Mieghem, P.: Reachability-based robustness of controllability in sparse communication networks. IEEE Trans. Netw. Serv. Manage. **18**(3), 2764–2775 (2021)
15. Lou, Y., Wang, L., Chen, G.: A framework of hierarchical attacks to network controllability. Commun. Nonlinear Sci. Numer. Simul. **98**, 105780 (2021)
16. 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. **113**, 078701 (2014) [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.113.078701
17. Lou, Y., Yang, D., Wang, L., Tang, C.-B., Chen, G.: Controllability robustness of Henneberg-growth complex networks. IEEE Access **10**, 5103–5114 (2022)
18. Zhang, Z., Yin, Y., Zhang, X., Liu, L.: Optimization of robustness of interdependent network controllability by redundant design. PLOS ONE **13**(2), 1–17 (2018) [Online]. Available: https://doi.org/10.1371/journal.pone.0192874
19. Dhiman, A., Sun, P., Kooij, R.: Using machine learning to quantify the robustness of network controllability. In: Machine Learning for Networking, pp. 19–39. Springer International Publishing (2021) [Online]. Available: https://doi.org/10.1007/978-3-030-70866-5_2
20. Chen, A., Sun, P., Kooij, R.E.: The recoverability of network controllability. In: 2021 5th International Conference on System Reliability and Safety (ICSRS), pp. 198–208. IEEE (2021)
21. Komareji, M., Bouffanais, R.: Resilience and controllability of dynamic collective behaviors. PLOS ONE **8**(12), 1–15 (2013) [Online]. Available: https://doi.org/10.1371/journal.pone.0082578
22. Knight, S., Nguyen, H.X., Falkner, N., Bowden, R., Roughan, M.: The internet topology zoo. IEEE J. Sel. Areas Commun. **29**(9), 1765–1775 (2011) [Online]. Available: https://networks.skewed.de/net/internet_top_pop
23. Shao, J., Buldyrev, S.V., Braunstein, L.A., Havlin, S., Stanley, H.E.: Structure of shells in complex networks. Phys. Rev. E **80**, 036105 (2009) [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevE.80.036105
24. 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. Netw. Netw. Last Frontier Complex. 3–36 (2014)