Reachability-based Robustness of Controllability in Sparse Communication Networks

Sun, Peng; Kooij, Robert E.; Van Mieghem, Piet

DOI
10.1109/TNSM.2021.3082283

Publication date
2021

Document Version
Accepted author manuscript

Published in
IEEE Transactions on Network and Service Management

Citation (APA)

Important note
To cite this publication, please use the final published version (if applicable). Please check the document version above.
Reachability-based Robustness of Controllability in Sparse Communication Networks

Peng Sun, Robert E. Kooij, and Piet Van Mieghem

Abstract—In this paper, we propose closed-form analytic approximations for the number of controllable nodes in sparse communication networks from the aspect of network controllability, considering link-based random attack, targeted attack, as well as random attack under the protection of critical links. We compare our approximations with simulation results on communication networks. Results show that our approximations perform well for all three attack strategies as long as the fraction of removed links is small. Only when the fraction of removed links is large, our approximation for targeted attacks does not fit well with simulation results. Finally, we validate our approximations using 200 communication networks and some synthetic networks. Results show that our approximations perform well in most cases.

Index Terms—Network controllability, network robustness, reachability, communication networks.

I. INTRODUCTION

In recent years, the analysis of network controllability from a graph theoretic point of view has become an active area of research. Through the control of external inputs [1], a controllable system can be driven from any arbitrary state to any desired state in finite time. For example, a communication network can be controlled externally through input signals such as commands from control units connected to some of the work stations [2].

Most work regarding the robustness of controllability has focused on the number of controls required to maintain network controllability after link or node failures. Parekh et al. [3] proposed a complex network model called q-snapback network which has the strongest robustness of controllability due to its advantageous inherent structure with many chain and loop motifs, when compared with the multiplex congruence network and the generic scale-free network. Pu et al. [4] found that the degree-based node attack is more efficient than a random failure for degrading the controllability in random and scale-free networks. Nie et al. [5] found that the controllability of Erdős-Rényi random graphs with a moderate average degree is not very robust, whereas a scale-free network with moderate power-law exponent shows a stronger ability to maintain its controllability, when these networks are under intentional link attack. Thomas et al. [6] identified that the potency of a degree-based attack is directly related to the betweenness centrality of the edges being removed. Chen et al. [7] evaluated the effect of the number of control inputs on the controllability for random networks and scale-free networks in the process of cascading failure. Lou et al. [8] proposed a framework of hierarchical attack by means of link- or node-removal attacks and suggest to protect the critical links and nodes to maintain network controllability. Xiao et al. [9] proposed a method that modifies any given network with strict structural perturbation to make the network homogenous and effectively enhance its robustness against malicious attacks. Zhang et al. [10] optimized the robustness of interdependent network controllability by redundant design including node backup and edge backup. Sun et al. [11] proposed closed-form analytic approximations for the number of controls that are needed to maintain network controllability, where links are removed according to both random and targeted attacks.

The above work regarding the robustness of controllability assumes that the network operator has the capability to add additional controls at any location in the network in order to maintain the current network controllable after attacks or failures. In other words, the basic assumption of previous work mentioned above is that network operators have sufficient budget and quantity of resources that can be deployed in response to an attack or failure. However, a more realistic assumption is that network operators have a fixed budget and a limited quantity of resources. Moreover, the increase in additional controls is only a proxy for the most relevant information - how much of the network is still controllable (reachable) after an attack or failure. Parekh et al. [12] proposed the number of controllable nodes as a new metric to quantify the robustness of controllability under network perturbations. Thomas et al. [6] analyzed the changes in the controllability of synthetic networks from the perspective of reachability and found that scale-free networks evidence higher robustness to random failures than Erdős-Rényi networks. In this paper, we analyse and measure the robustness of network controllability in terms of reachability. In particular, we determine the maximum number of nodes that are still controllable when the number of driver nodes remains the same during the failure or attack process. Here, the driver nodes are the nodes into which the external control signals are directly injected.

This paper is organized as follows. In Section II, we introduce some basic concepts and definitions in network controllability proposed in [1]. In Section III, we analyse the role of critical links in network controllability. In Section IV, we compare the robustness of controllability for three cases: random attack, random attack under protection and targeted attack. In Section V, we propose analytic approximations for the number of controllable nodes \( N_c \) in these three cases and measure the accuracy of our approximations. Section VI concludes the paper.
II. REACHABILITY-BASED ROBUSTNESS OF CONTROLLABILITY

A. Controllability of networks

Most real systems are driven by nonlinear dynamics. However, linear dynamics is a first step towards addressing the controllability of real-world systems and provides sufficient controllability conditions for particular nonlinear cases [1]. A system is controllable if it can be driven from any initial state to any desired final state by proper variable inputs in finite time [13]. We consider a linear, time-invariant system $G(A, B)$, which is described by:

$$\frac{dx(t)}{dt} = Ax(t) + Bu(t)$$

where the $N \times 1$ vector $x(t) = (x_1(t), x_2(t), ..., x_N(t))^T$ denotes the state of the system with $N$ nodes at time $t$. The weighted matrix $A$ is an $N \times N$ matrix which describes the network topology (graph) and the interaction strength between the components as nodes in the graph. In this work, we assume that there are no self-links in the networks, which is also assumed in [1], [14]. The $N \times M$ matrix $B$ is the input matrix which identifies the $M \leq N$ driver nodes controlled by outside input signals. The $M \times 1$ vector $u(t) = (u_1(t), u_2(t), ..., u_M(t))^T$ is the input signal vector. A driver node $j \in \{1, \ldots, M\}$ has an input signal $u_j$ that is externally fed in $u_j(t)$. In [6] and [12], the $j$th external source which generates the input signal $u_j$ is named control node or input node, while the $N$ nodes in the network are named state nodes. Since each driver node is injected by an input signal generated by an external control node, the number of driver nodes equals the number of control nodes.

The linear system defined by equation (1) is controllable, if and only if the $N \times NM$ controllability matrix

$$C = (B, AB, A^2B, ..., A^{N-1}B)$$

has full rank, i.e., $\text{rank}(C) = N$. Criterion (2) is called Kalman’s controllability rank condition [15]. The rank of matrix $C$ provides the dimension of the controllable subspace of the system. The input matrix $B$, which determines the location of driver nodes, needs to be chosen properly to assure that the controllability matrix $C$ has full rank.

So far, most of the existing studies on the robustness of controllability have measured the increase in the minimum number $N_d$ of driver nodes required as a proxy for the reduction in controllability due to a failure. This indirect approach of measuring robustness is referred to as control-based robustness. The robustness of network controllability from the perspective of reachability is also considered by a few authors, see [6] and [12]. Besides, the control-based robustness analysis of network controllability assumes that the network operator has the capability to attach any amount of additional control signals to the nodes in the network. However, network operators normally have limited budget and resources in real life, which constrains the ability to deploy external controls. Based on these considerations, we focus on the reachability-based robustness of controllability, which determines the maximum number $N_c$ of nodes that are still under control when failure or attack occurs, during which the number $N_{d0}$ of driver nodes remains the same [12]. For the reachability-based controllability, there are two cases, namely free control and fixed control [6]. In the free control case, only the number $N_{d0}$ of driver nodes remains the same, but the set of driver nodes can vary. In the fixed control case, both the number and the set of driver nodes are fixed during attacks or failures. In this paper, we only consider the free control case and delegate the fixed control to future research. For convenience, we use the term reachability to represent reachability-based controllability.

B. $R$-value and challenges

We inherit the framework and some definitions proposed for network robustness [16], [17] to investigate the robustness of reachability. The robustness of a given network determined by a service and an underlying topology is quantified by a robustness value, referred to as the $R$-value. [16]. The $R$-value is normalized to the interval $[0, 1]$. Thus, $R = 1$ reflects complete functionality in an network without failures, and $R = 0$ corresponds to the complete absence functionality in a severely damaged network. The $R$-value can be a metric, which is related to network topology and service, such as the size of the giant component [18], the effective graph resistance [19] and network efficiency [20]. In this paper, we use the normalized maximum number of controllable nodes $n_c = N_c / N$ as the $R$-value. The number $N_c$ of controllable nodes satisfies $N_{d0} \leq N_c \leq N$, and $N_{d0} / N \leq n_c \leq 1$.

An elementary challenge is an event that changes the network and thus changes the $R$-value. We assume that a sequence of changes does not coincide in time. In this paper, we confine an elementary challenge to a link removal in a failure process. A perturbation is a series of $m$ elementary changes, characterized by a sequence of $m$ corresponding $R$-values $\{R[k]\}_{0 \leq k \leq m}$, where $k = m / L$ is the fraction of removed links, $m \in \{1, \ldots, L\}$ is the number of removed links and $L$ is the number of links in the network. In this paper, we choose the maximum number $n_c$ of controllable nodes as the $R$-value and observe the impact of link removal on $n_c$. As shown in Figure 1, the maximum number $n_c$ of controllable nodes has a decreasing trend as links are removed one by one.

C. Robustness envelopes

As discussed in the previous part, any realization of failure processes can be expressed as a sequence of $R$-values denoted $\{R[k]\}_{0 \leq k \leq m}$ where $k$ is the fraction of removed links and $k \in \{1/L, 2/L, \ldots, 1\}$. Assuming that the nature of the failures is unknown and they occur independently, $R[k]$ is a random variable and can be described by its probability density function (pdf). The pdf of this $R[k]$ is computed using all subsets of $[kL]$ links in all possible perturbations. The envelope for a network $G$ is constructed using all $R[k]$ for $k \in \{1/L, 2/L, \ldots, 1\}$, where boundaries are given by the extreme $R$-values

$$R_{\min}[k] = \{\min(R[1/L]), \min(R[2/L]), \ldots, \min(R[1])\},$$

$$R_{\max}[k] = \{\max(R[1/L]), \max(R[2/L]), \ldots, \max(R[1])\}.$$
which gives the worst- and best-case of robustness metrics for a network after a given number of challenges [17]. Besides, the expected $R$-value resulting from $kL$ perturbations

$$R_{avg}[k] \in \{E(R[1/L]), E(R[2/L]), \ldots, E(R[1])\}.$$  \hspace{1cm} (5)

Since $R[k]$ defines a probability density function, we are interested in the percentiles of $R[k]$.

$$R_{\theta}[k] \in \{R_{\theta}[1/L], R_{\theta}[2/L], \ldots, R_{\theta}[1]\}$$  \hspace{1cm} (6)

where $R_{\theta}[k]$ are the points at which the cumulative distribution of $R[k]$ crosses $\theta/100$, namely if $R_{\theta}[k] = t$, then $\Pr[R[k] \leq t] = \theta/100$. We refer to $R_{\theta}[k]$ as a $\theta$-percentile and define $R_{\theta}[k] = R_{\min}[k]$, $R_{100\%}[k] = R_{\max}[k]$.

We apply the envelope to present the influence of the failure process on a network [16], [17]. The envelope profiles the pdf of the random variables of the $R$-value, which is the probability of a random variable to fall within a particular region. The area of the envelope can be regarded as the probability of a random variable to fall within a particular region. The effectiveness of attack strategies can also be measured by comparing with the worst-, best- and average performance provided by robustness envelopes.

![Fig. 1](image-url) The impact of link removal on the normalized maximum number $n_c$ of controllable nodes in a communication network DFN (German optical backbone X-WiN network) with $N = 58$ and $L = 87$.

III. ANALYSIS OF CRITICAL LINKS

Liu et al. [1] proved that the minimum number $N_d$ of driver nodes needed for structural controllability, where the external signals are injected to control the directed network, can be obtained through the “maximum matching” of the network. Define the source node of a directed link as the node from which the link originates and the target node as the node where the link terminates. A maximum matching of a directed network is a maximum set of links that do not share source or target nodes [21], which is illustrated in Figure 2(a). Such links are coined “matching links”. Target nodes of matching links are matched nodes and the other nodes are unmatched nodes. In order to find the maximum number of matching links, so as to determine the minimum number $N_d$ of driver nodes, a directed network $G$ with $N$ nodes and $L$ links can be converted into a bipartite graph $B_{N,N}$ with $2N$ nodes and $L$ links, as shown in Figure 2(b). A maximum matching in a bipartite graph can be obtained efficiently by the Hopcroft-Karp algorithm [22]. The unmatched nodes in a maximum matching constitute a minimum set of driver nodes.

A. The role of critical links in maximum matching

Links in a network can be classified into three categories: critical, redundant, and ordinary [1]. A link is critical if its removal increases the minimum number of driver nodes $N_d$ by 1 to remain in full control of the system. A link is redundant if it never belongs to a maximum matching. A link is ordinary if it is neither critical nor redundant. In Figure 2(a), link $a$, $b$, $c$ and $d$ (highlighted in red) are critical links, the removal of any one of them will increase the number of driver nodes by 1, while link $e$ is redundant. The influence of the removal of critical links can be explained by the maximum matching. As shown in 2(b), all the critical links $a$, $b$, $c$, $d$ belong to the maximum matching of size 4. If any one of them is removed, there is no alternative link to take its place in the maximum matching. Thus, a new unmatched node will appear and the number of driver nodes will increase by 1. Besides, critical links are conditional and should be updated during attacks. For example, link $c$ is no longer a critical link in the resulting network after link $b$ is removed.

In our previous work [11], we proposed closed-form analytic approximations for the minimum number $N_d$ of driver nodes needed to fully control networks, where links are removed according to both random and targeted attacks.

![Fig. 2](image-url) (a) Driver nodes and matching links in a directed network $G$. (b) The corresponding bipartite graph with 10 nodes and 5 links. By using the Hopcroft-Karp algorithm, a maximum set of matching links $\{a,b,c,d\}$ can be found in the bipartite graph. The target nodes $\{2,-,3,-,4,-,5-\}$ of the matching links are matched nodes. The other target node $\{1-\}$ is an unmatched node, therefore it is also driver node.

B. The role of critical links in the structure of control

Parekh et al. [12] found the control structure which consists of a backbone of directed paths, called stems, each driven by an independent control. These paths can then control cycles that are inherently self-regulatory. However, ultimately these stems dictate the need for controls; There must be one control node for each stem in the system in order to guarantee that all nodes in the network are controllable (reachable). In this
paper, we use the algorithm proposed in [6] to find the control structure in the network:

1) Determine the number $M$ of control nodes by the maximum matching introduced in Section III.A.
2) Preprocess the network by adding the fixed number of control nodes and then placing links from each control node to every state node, after which there are $N$ nodes and $E$ links in the network. Then, for all $i, j = 1, \ldots, N$ and $k = 1, \ldots, M$:
   a) Split the nodes into a pair of positive and negative nodes $x_i \Rightarrow x_i^+, x_i^-$, $u_k \Rightarrow u_k^+, u_k^-$.  
   b) Add unit-weight links $(x_i^+, x_j)$ and $(u_k^+, x_j)$ if the link $(x_i, x_j)$ and $(u_k, x_j)$ exist in the network, respectively.
   c) Add zero-weight links $(x_i^+, x_i^-)$ and $(u_k^+, u_k^-)$.
   d) Add a weight $W \geq E$ to all links.
3) Use the weighted maximum matching on the bipartite graph generated by step 2 and find a set of matched links. The control structure is then formed by mapping the matched links in the original network.

Finally, the number of controllable nodes equals the number of matched nodes in the control structure. Although the concept of critical links was first proposed in control-based controllability analysis which focuses on the number $N_d$ of driver nodes, critical links also play an important role in reachability-based controllability. We found that the removal of a critical link usually decreases the number of controllable nodes by 1 in most cases when the network is sparse. In this paper, we use the concept of critical links to derive analytical approximations for the decrease in the number $N_c$ of controllable nodes upon link removal.

IV. NUMBER OF CONTROLLABLE NODES UNDER ATTACKS

In this section, we analyze the normalized number of controllable nodes for three different attack scenarios: (a) random attack, (b) targeted attack and (c) random attack under protection. In a random attack, links are removed from the network uniformly at random. In a targeted attack, we assume that the attacker knows the location of critical links and removes critical links uniformly at random. After all critical links are removed, the attacker randomly removes other links. In a random attack under protection, the network operator takes measures to protect the critical links such that only non-critical links are removed randomly.

We compare the normalized number $n_c$ of controllable nodes for these three attacks in 10 sparse communication networks [23] [24]. Table I presents the properties of the 10 communication networks: the number $N$ of nodes, the number $L$ of directed links, the initial minimum number $N_{d0}$ of driver nodes and the number $L_c$ of critical links. For a directed network, the average degree $E[D] = 2L/N$, which also equals the sum of the mean out- and in-degree per node. The first 8 networks are small. The other two networks are relatively large, which are an order larger than the average size of the other 8 communication networks. Besides, the last network has a higher average degree, which is more than twice that of the other networks. The number $L_c$ of critical links can be determined by applying the Hopcraft-Karp algorithm $L$ times, by considering all $L$ networks that are obtained by removing exactly one link from the original network. As expected, Figure 3 shows that random attack under protection performs the best among the three attack scenarios in maintaining the reachability of the networks. Moreover, we also conclude from Figure 3:

1) In the case of random attack under protection, the slope of the decrease in $n_c$ is almost 0 in the beginning for all networks. This emphasizes the importance of protecting critical links.
2) The targeted attack is the most harmful: when the fraction of removed links is smaller than the fraction of critical links, the decrease in $n_c$ is almost linear in the fraction of removed links. When all the critical links are removed, the slope of the decrease in $n_c$ is almost 0 in all 8 networks. Considering the set of critical links is determined from the initial network, this indicates that the set of critical links of a network does not significantly change during the attack process when the fraction of removed links is small.
3) The performance of random attack is between targeted attack and random attack under protection. After all links are removed, the normalized number of controllable nodes equals $N_{d0}/N$.
4) Critical links have a significant impact on the number $N_c$ of controllable nodes upon link removal, which plays a key role to derive analytical approximations for the number $N_c$ of controllable nodes.

We also use robustness envelopes to evaluate the effectiveness of the three attack strategies. As shown in Figure 3, the curves for random attack under protection are quite close to the boundaries represented by the 90-percentile $R_{90\%}$ of all networks, which means that random attack under protection outperforms 90% realizations of random attack. The curves for targeted attack are much lower than the lower bound of envelopes especially when the fraction of removed links is small in all networks, which again underlines the harm of targeted attack.

<table>
<thead>
<tr>
<th>Networks</th>
<th>$N$</th>
<th>$L$</th>
<th>$E[D]$</th>
<th>$N_{d0}$</th>
<th>$L_c$</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFN</td>
<td>58</td>
<td>87</td>
<td>3.0</td>
<td>25</td>
<td>14</td>
</tr>
<tr>
<td>Colt</td>
<td>153</td>
<td>177</td>
<td>2.3</td>
<td>58</td>
<td>38</td>
</tr>
<tr>
<td>DeltaCom</td>
<td>113</td>
<td>161</td>
<td>2.8</td>
<td>37</td>
<td>43</td>
</tr>
<tr>
<td>GeCe</td>
<td>140</td>
<td>193</td>
<td>2.6</td>
<td>58</td>
<td>49</td>
</tr>
<tr>
<td>TataNld</td>
<td>145</td>
<td>186</td>
<td>2.6</td>
<td>52</td>
<td>48</td>
</tr>
<tr>
<td>UsCarrier</td>
<td>158</td>
<td>189</td>
<td>2.4</td>
<td>53</td>
<td>66</td>
</tr>
<tr>
<td>Cogentcc</td>
<td>197</td>
<td>243</td>
<td>2.5</td>
<td>71</td>
<td>72</td>
</tr>
<tr>
<td>Uninet2010</td>
<td>74</td>
<td>101</td>
<td>2.7</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>Kdl</td>
<td>754</td>
<td>895</td>
<td>2.4</td>
<td>272</td>
<td>287</td>
</tr>
<tr>
<td>Web [24]</td>
<td>643</td>
<td>2280</td>
<td>7.0</td>
<td>324</td>
<td>108</td>
</tr>
</tbody>
</table>

V. APPROXIMATIONS FOR THE NUMBER OF CONTROLLABLE NODES

In the previous section, we compared the number of controllable nodes for the three attack scenarios by using a large amount of simulations. In this section, we deduce analytical
Approximations to quantify the robustness of reachability, expressed in terms of the normalized number $n_c$ of controllable nodes, for the three attack scenarios. Then, we evaluate the accuracy of the analytical approximations in 8 small networks, 2 large networks as well as more sparse communication networks. Lastly, we also use synthetic networks to measure the performance of our analytical approximations. Our approximations will be based upon the concept of critical links introduced in [1].

A. Number of controllable nodes under random attacks

1) The fraction $l$ of removed links is less than the fraction $l_c$ of critical links

Given a network with $N$ nodes and $L$ links, the initial number $N_c$ of controllable nodes equals $N$. The number $L_c$ of critical links can be determined by the method we introduced in Section IV.

As discussed in Section III.B, the number $N_c$ of controllable nodes decreases by at least one when a critical link is removed. However, we found that the number $N_c$ of controllable nodes only decreases by one for every critical link that is removed in each of the 10 sparse communication networks in Table I. Thus, we heuristically assume that after removing a critical link, the number $N_c$ of controllable nodes decreases by one. If we denote the number of removed links by $m$, then the fraction of removed links $l = \frac{m}{L}$. The fraction of critical links $l_c$ satisfies $l_c = \frac{L_c}{L}$. We consider the case $l \leq l_c$, where $m$ links are removed uniformly at random under the assumption that the number of removed links obeys $m \leq L_c$. Now assume that these $m$ links $i$ links are critical ($i \leq m$) and, hence, $m - i$ links are non-critical. We assume that the set of critical links is nearly unchanged when the fraction of removed links is small. Invoking the fact that after removing a critical link, the number $N_c$ of controllable nodes decreases by one, thus, when $i$ critical links are iteratively removed one by one, the number $N_c$ of controllable nodes decreases by one in each iteration. For the $m - i$ non-critical links, the number $N_c$ of controllable nodes remains the same based on our assumption that the set of critical links is unchanged when the fraction of removed links is small. Since there are \( \binom{L_c}{i} \) possible ways to choose $i$ critical links from $L_c$ critical links and there are \( \binom{L - L_c}{m - i} \) possible ways to choose $m - i$ non-critical links from $L - L_c$ non-critical links, the contribution to the decrease in $N_c$ is \( \binom{L_c}{i} \binom{L - L_c}{m - i} \). The average decrease $N_c^*$ of the number $N_c$ of controllable nodes after randomly removing $m$ links, is the sum of this expression for all $i = 1, 2, \ldots, m$ divided by \( \binom{L}{m} \).

\[
N_c^* = \frac{\sum_{i=1}^{m} \binom{L_c}{i} \binom{L - L_c}{m - i}}{\binom{L}{m}}
\]  

(7)

Using \( \binom{L_c}{i} = \binom{L_c}{L_c - i} \) and Vandermonde’s formula 
\( \sum_{j=0}^{k} \binom{a}{j} \binom{b}{k - j} = \binom{a + b}{k} \) for any number $a$ and $b$, we obtain

\[
L_c \sum_{i=0}^{m} \binom{L_c - i}{i} \binom{L - L_c}{m - i} = L_c \binom{L - 1}{m - 1}.
\]

Finally, dividing this expression by \( \binom{L}{m} \), leads to the average decrease of controllable nodes

\[
N_c^* = lL_c
\]  

(8)

When the fraction of removed links is less than, or equal to $l_c$, we obtain

\[
N_c = N - lL_c
\]  

(9)
We then normalize the number \(N_c\) of controllable nodes to the fraction \(\frac{N_c}{N}\) of the minimum number of controllable nodes and denote the obtained approximation as \(n_{c,rand}\):

\[
n_{c,rand} = \frac{N - L_c}{N} \tag{10}
\]

2) The fraction \(l\) of removed links is larger than the fraction \(l_c\) of critical links

Considering that in most cases \(l_c\) is quite small, we also estimate the normalized maximum number \(n_c\) of controllable nodes when the fraction \(l\) of removed links is larger than the fraction \(l_c\) of critical links. For \(l \geq l_c\), we heuristically propose a simple closed-form approximation for \(n_{c,rand}\):

\[
n_{c,rand} = al^2 + bl + c \tag{11}
\]

where the parameters \(a\), \(b\) and \(c\) will be determined by boundary conditions. For the first two boundary conditions we assume that, for \(l = l_c\), Eq.(11) has the same value and the same derivative as Eq. (10). This leads to the equations \(N - l_cL_c = N(al^2 + bl + c)\) and \(-L_c = N(2al_c + b)\), respectively. Finally, if we remove all links, i.e. \(l = 1\), only \(N_{d0}\) nodes can be controlled. This gives the boundary condition \(N_{d0}/N = a + b + c\). Solving for \(a\), \(b\) and \(c\) and combining with the approximation Eq.(10), we obtain the following approximation for \(n_{c,rand}\) for all values of \(l\):

\[
n_{c,rand} = \begin{cases} 
\frac{N - L_c}{N} & l \leq l_c \\
al^2 + bl + c & l \geq l_c
\end{cases} \tag{12}
\]

with \(a = -\frac{N - N_{d0} - L_c}{N(l_c - 1)^2}\), \(b = -\frac{L_c}{N} - 2al_c\), and \(c = (N_{d0} + L_c)/N + a(2l_c - 1)\). Eq.(12) represents a closed-form approximation for \(n_c\), which only depends on \(N, L, N_{d0}\) and \(L_c\). The computational complexity of the approximation is \(O(\sqrt{NL^2})\), which is needed for the computation of \(L_c\).

We compare the approximation Eq.(12) with simulation results for the 8 communication networks. Figure 4 illustrates that the approximation both under- and overestimates the value of \(n_c\). For moderate values of the fraction of removed links, the approximation exhibits a very good fit for the communication networks. For some networks, such as Deltacom, GtsCe, TataNld and Uninett2010, our approximation Eq.(12) fits well with the simulation results regardless of the fraction of removed links.

The performance of our approximations are also measured by three performance indicators:

1) \(r^*\) denotes the absolute value of the relative error at \(l = 0.2\). We choose the value 0.2 reflecting a relatively large fraction in terms of link-based failures or attacks.

2) \(l^*\) represents the smallest value of \(l\), where the relative error between the approximation and the simulated mean exceeds 5%.

3) \(\gamma\) denotes the fraction of the interval \([0,l_c]\) for which the absolute value of the relative error between the approximation and the mean simulated value does not exceed 5%. The value of \(\gamma\) is computed by \(K\) different values of the fraction of removed links, i.e., \(v_1, v_2, ..., v_K\), are evenly determined in the interval \([0, l_c]\). Let \(n^*_c(v_i)\) and \(n_c(v_i)\) denote the mean simulated \(n_c\) and the approximation (10) at the fraction of removed links \(l = v_i\), respectively. Thus, in terms of the indicator function \(1_x\) that equals 1 if the condition \(x\) is true, otherwise it is zero,

\[
\gamma = \frac{1}{K} \sum_{i=1}^{K} 1_{\left|\frac{n^*_c(v_i) - n_c(v_i)}{n^*_c(v_i)}\right| \leq 5\%}
\]

Table II gives the three performance indicators for Eq.(12). As shown in the table, when the fraction of removed links is less than 0.2, the absolute relative error between Eq.(12) and the simulated mean is less than 5% for all 8 networks. For most networks, such as Deltacom, GtsCe, TataNld, UsCarrier, Cogentco and Uninett2010, Eq.(12) still fits well with simulation results regardless of the fraction of removed links. For the worst performing networks, DFN and Colt, 87% and 81% of the links can be removed before the absolute relative error exceeds 5%, respectively. When the fraction of removed links is less than the fraction \(l_c\) of critical links, the absolute value of the relative error between the approximation and the mean simulated value is always less than 5%. Thus, \(\gamma\) equals 100% for all networks.

<table>
<thead>
<tr>
<th>Networks</th>
<th>(r^*)</th>
<th>(l^*)</th>
<th>(\gamma)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFN</td>
<td>0.78%</td>
<td>0.87%</td>
<td>100%</td>
</tr>
<tr>
<td>Colt</td>
<td>1.23%</td>
<td>0.81%</td>
<td>100%</td>
</tr>
<tr>
<td>Deltacom</td>
<td>1.08%</td>
<td>1.00%</td>
<td>100%</td>
</tr>
<tr>
<td>GtsCe</td>
<td>1.20%</td>
<td>1.00%</td>
<td>100%</td>
</tr>
<tr>
<td>TataNld</td>
<td>0.45%</td>
<td>1.00%</td>
<td>100%</td>
</tr>
<tr>
<td>UsCarrier</td>
<td>1.17%</td>
<td>1.00%</td>
<td>100%</td>
</tr>
<tr>
<td>Cogentco</td>
<td>0.98%</td>
<td>1.00%</td>
<td>100%</td>
</tr>
<tr>
<td>Uninett2010</td>
<td>1.24%</td>
<td>1.00%</td>
<td>100%</td>
</tr>
</tbody>
</table>

B. Number of driver nodes under targeted attacks

1) The fraction \(l\) of removed links is smaller than the fraction \(l_c\) of critical links

We assume that, as long as the number of removed links \(m \leq L_c\), the removal of each link decreases the number \(N_c\) of controllable nodes by one. Consequently, when the number of removed links is smaller than \(L_c\) (the fraction \(l\) of removed links is smaller than \(l_c\)), the approximation for the minimum number \(N_c\) of driver nodes decreases linearly with the fraction \(l\) of removed links. When the number of removed links equals the number \(L_c\) of critical links, the minimum number \(N_c\) of driver nodes equals \(N - L_c\). Thus, when the fraction \(l\) of removed links is no more than the fraction \(l_c\) of critical links, we obtain the following approximation for \(n_c\):

\[
n_{c,crit} = \frac{N - IL}{N} \tag{13}
\]

2) The fraction \(l\) of removed links is larger than the fraction \(l_c\) of critical links

We now construct an approximation when the number of removed links is larger than \(L_c\) (the fraction \(l\) of removed links is larger than \(l_c\)), in a similar way as in the previous
section. Again assuming that for \( l \geq l_c \) it holds that \( n_c \) is quadratic in \( l \), we obtain \( n_{c,\text{crit}} = dl^2 + el + f \). Boundary conditions are now obtained from the assumptions that the parabola passes through \((1, N_{d0}/N)\) and \((l_c, (N - L_c)/N)\) and has a zero derivative at the latter point. This leads to the following approximation for \( n_c \) for all values of \( l \):

\[
 n_{c,\text{crit}} = \begin{cases} 
  \frac{N - lL}{N} & \text{for } l \leq l_c \\
  dl^2 + el + f & \text{for } l > l_c
\end{cases} 
\] (14)

with \( d = -\frac{N - N_{d0} - l_cL}{N(l_c-1)^2} \), \( e = -2dl_c \), and \( f = N_{d0}/N + d(2l_c - 1) \).

In Figure 5, we compare our approximation Eq.(14) with simulation results. Simulation results show that the difference in the curve trend at \( l = l_c \) is due to the fact that until \( l = l_c \) only critical links are targeted causing a faster descent in the number of controllable nodes. We observe that the approximation Eq.(14) fits well with simulation results when the fraction of removed links is sufficiently small in these communication networks. In some networks, such as DFN and UsCarrier, Eq.(14) is close to simulation results even when the fraction of removed links is relatively large. When the fraction of removed links is getting larger, the difference between our approximation Eq.(14) and simulation results is relatively large. However, approximation Eq.(14) always seems to overestimate the impact of targeted attack on the normalized maximum number \( n_c \) of controllable nodes, hence, approximation Eq.(14) can be considered a worst-case approximation.

Comparing with the targeted attack, we quantify the performance of the approximation Eq.(14) in Table III. For DFN and Colt, Eq.(14) is a very good approximation when the fraction of removed links is less than \( l_c \). Eq.(14) performs the best for DFN, 23% of the links can be removed before the absolute relative error exceeds 5%. Eq.(14) does not perform well for TataNld.

**TABLE III**

<table>
<thead>
<tr>
<th>Networks</th>
<th>( r^* )</th>
<th>( l^* )</th>
<th>( \gamma )</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFN</td>
<td>4.53%</td>
<td>0.23</td>
<td>100%</td>
</tr>
<tr>
<td>Colt</td>
<td>4.88%</td>
<td>0.21</td>
<td>97.81%</td>
</tr>
<tr>
<td>Deltacom</td>
<td>7.52%</td>
<td>0.18</td>
<td>67.42%</td>
</tr>
<tr>
<td>GtsCe</td>
<td>5.06%</td>
<td>0.19</td>
<td>74.80%</td>
</tr>
<tr>
<td>TataNld</td>
<td>10.11%</td>
<td>0.12</td>
<td>46.51%</td>
</tr>
<tr>
<td>UsCarrier</td>
<td>3.26%</td>
<td>0.22</td>
<td>63.04%</td>
</tr>
<tr>
<td>Cogentco</td>
<td>8.75%</td>
<td>0.18</td>
<td>60.81%</td>
</tr>
<tr>
<td>Uninet2010</td>
<td>8.86%</td>
<td>0.19</td>
<td>71.08%</td>
</tr>
</tbody>
</table>

**C. Number of driver nodes under random attacks with protection**

For this scenario, we assume that a fraction of links \( l_c \) is protected, then we can only attack a fraction \( 1 - l_c \) of the links. We now construct an approximation for the number \( N_{c,\text{prot}} \) of controllable nodes when the attack is random under protection. We heuristically assume that the fraction \( n_{c,\text{prot}} \) of controllable nodes is quadratic in \( l \), we obtain \( n_{c,\text{prot}} = pl^2 + ql + r \). Boundary conditions are now obtained from the assumptions that the parabola passes through \((1, N_{d0}/N)\) and \((0, 1)\) and has a zero derivative at the latter point. This leads to the following approximation for \( n_c \) for all values of \( l \):

\[
 n_{c,\text{prot}} = pl^2 + ql + r
\] (15)

with \( p = N_{d0}/N - 1 \), \( q = 0 \), and \( r = 1 \).
Fig. 5. The normalized maximum number of controllable nodes \( n_c \) as a function of the fraction of removed links \( l \) in communication networks under targeted attacks. The results for each fraction \( l \) is based on 1000 simulations. In each sub-figure, the vertical dashed line marks the position where \( l = l_c \).

However, only a fraction \( 1 - l_c \) of links are removed in the simulation for this scenario. Thus, we still remove critical links uniformly at random after all non-critical links are removed, in order to compare the simulation results and our approximation Eq.(15) in the same interval \([0, 1]\). Figure 6 shows that for moderate values of the fraction of removed links, the approximation exhibits an excellent fit for simulation results. For some networks, such as TataNld, UsCarrier and Cogentco, our approximation Eq.(15) fits well with the simulation results regardless of the fraction of removed links.

Similarly, the performance of our approximation Eq.(15) is measured by three performance indicators. As shown in Table IV, when the fraction of removed links is less than 0.2, the absolute relative error between Eq.(15) and the simulated mean is less than 5% for all 8 sparse communication networks. For some networks, such as UsCarrier and Cogentco, even when the fraction of removed links is large (0.62 and 0.58, respectively), Eq.(15) still fits well with simulation results. Even for the worst performing network, DFN, 28% of the links can be removed before the absolute relative error exceeds 5%.

**D. Verification by large networks**

We use the last two large networks, Kdl and Web, from Table I to further evaluate the accuracy of our approximations. The simulations setting is slightly different from the previous part. The fraction \( l \) of removed links is ranging from 0.1 to 1 with a step 0.1, considering the high computational complexity by using all fraction \( l \) ranging from 0 to 1. As shown in Figure 7, the approximation Eq.(12) for the random attack and Eq.(15) for the random attack with protection perform well in estimating the fraction \( n_c \) of driver nodes. We also find that the approximation Eq.(14) for targeted attack fits well with simulation results when the fraction of removed links is sufficiently small. Though the approximation Eq.(14) does not perform well when the fraction of removed links is large, approximation Eq.(14) can be considered a worst-case approximation. Considering the Kdl network and the 8 small networks have similar average degree, the above observation implies that the size of the network does not significantly influence the performance of our approximations. By contrast, Figure 8(a) and (c) show that the approximation Eq.(12) for the random attack and Eq.(15) for the random attack with protection do not perform well for the Web network which has a larger average degree than the above networks. In a network with a higher average degree, there are more alternate matchings which make it more likely for the critical links to change as links are removed. As a result, our approximations do not perform well since our assumption is that the set of critical links is nearly unchanged when the fraction of removed links is small. However, since most communication networks are sparse [25] [26] [27], we can expect that our approximations are applicable for most communication networks.

We then quantify the performance of the approximations for the network Kdl and Web in Table V and VI, respectively.
Results show that the network Web has larger $r^+$ values than the network Kdl in all three attacks, which also indicates that our approximation perform better in the networks with lower average degree.

**TABLE V**

<table>
<thead>
<tr>
<th>Types of attacks</th>
<th>$r^+$</th>
<th>$\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random attack</td>
<td>2.36%</td>
<td>100%</td>
</tr>
<tr>
<td>Targeted attack</td>
<td>7.54%</td>
<td>53.65%</td>
</tr>
<tr>
<td>Random attack with protection</td>
<td>3.67%</td>
<td>92.84%</td>
</tr>
</tbody>
</table>

**TABLE VI**

<table>
<thead>
<tr>
<th>Types of attacks</th>
<th>$r^+$</th>
<th>$\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random attack</td>
<td>13.78%</td>
<td>100%</td>
</tr>
<tr>
<td>Targeted attack</td>
<td>9.21%</td>
<td>54.16%</td>
</tr>
<tr>
<td>Random attack with protection</td>
<td>5.25%</td>
<td>100%</td>
</tr>
</tbody>
</table>

**E. Verification by more communication networks**

We further use the dataset available at a specialized database - the Internet Topology Zoo [23] to select more communication networks and verify the accuracy of our approximations. The networks in the dataset initially are not directed, however, we use the information available in two attributes, i.e., source node and target node, to make these networks directed. After excluding networks with extremely small size, we have 200 communication networks.

For each attack strategy, we calculate the values of the three performance indicators for all 200 communication networks and then get the average value for each indicator. As shown in Table VII, the approximation Eq.(12) for the random attack and Eq.(15) for the random attack with protection perform well in estimating the fraction $n_c$ of driver nodes. For the targeted attack, the approximation Eq.(14) fits well with simulation results when the fraction of removed links is sufficiently small.

**TABLE VII**

<table>
<thead>
<tr>
<th>Types of attacks</th>
<th>$r^+$</th>
<th>$\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random attack</td>
<td>4.26%</td>
<td>0.47</td>
</tr>
<tr>
<td>Targeted attack</td>
<td>10.44%</td>
<td>0.11</td>
</tr>
<tr>
<td>Random attack with protection</td>
<td>3.52%</td>
<td>0.23</td>
</tr>
</tbody>
</table>

**F. Verification by synthetic networks**

In this section, we test our approximations on two types of synthetic networks, the directed Erdős-Rényi (ER) random network $G_p(N)$ and the Barabási-Albert (BA) scale-free network $BA(N, M_0, M)$. When generating the directed Erdős-Rényi random network $G_p(N)$ with $N$ nodes, the probability that every node has an outbound link to the other nodes is $p$. We generate the scale-free network $BA(N, M_0, M)$ by using the Barabási-Albert (BA) model, where $N$ is the number of nodes, $M$ is the number of out-going links for each new node added to the current network. We assume that initially the network consists of a complete digraph on $M_0$ nodes, where $M_0$ equals $M$. In the initial complete digraph, every pair of distinct nodes is connected by a pair of unique links (one in each direction). New nodes are added to the network one at a time. Each new node is connected to $M$ existing nodes with a probability that is proportional to the number of links that the existing nodes already have.
In our simulations, we generate Erdős-Rényi (ER) random networks $G_{p}(N)$ with $N = 100$, $p = 0.05$ and $N = 10000$, $p = 0.0003$, Barabási-Albert (BA) networks with $N = 200$, $M = M_0 = 2$ and $N = 10000$, $M = M_0 = 1$. Figure 9 shows that the approximation Eq.(12) for the random attack performs well in estimating the fraction $n_c$ of controllable nodes in both types of synthetic networks when the fraction of removed links is small. Figure 10 shows that the approximation Eq.(14) for the targeted attack performs well as long as the fraction of removed links is relatively large ($l = 0.2$).

Next we quantify the performance of each approximation for synthetic networks. As shown in Table VIII, IX and X, the approximation Eq.(12) for random attack and Eq.(15) for random attack with protection fit well with simulation results even when the fraction $l$ of removed links is large. The approximation Eq.(14) does not perform well if the fraction $l$ of removed links is small. Figure 11 shows that the approximation Eq.(14) can be considered an approximation for the worst-case scenario.

### Table VIII: Performance Indicators for the Approximation $n_{c,rand}$ for Synthetic Networks

<table>
<thead>
<tr>
<th>Types of networks</th>
<th>$\gamma$</th>
<th>$\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>ER: $G_{0.05}(100)$</td>
<td>3.27%</td>
<td>100%</td>
</tr>
<tr>
<td>BA: $N=200$, $E[D]=4$</td>
<td>6.78%</td>
<td>100%</td>
</tr>
<tr>
<td>ER: $G_{0.0003}(10000)$</td>
<td>8.95%</td>
<td>85.54%</td>
</tr>
<tr>
<td>BA: $N=10000$, $E[D]=2$</td>
<td>7.63%</td>
<td>96.23%</td>
</tr>
</tbody>
</table>

### Table IX: Performance Indicators for the Approximation $n_{c,crit}$ for Synthetic Networks

<table>
<thead>
<tr>
<th>Types of networks</th>
<th>$\gamma$</th>
<th>$\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>ER: $G_{0.05}(100)$</td>
<td>12.64%</td>
<td>71.97%</td>
</tr>
<tr>
<td>BA: $N=200$, $E[D]=4$</td>
<td>17.36%</td>
<td>63.91%</td>
</tr>
<tr>
<td>ER: $G_{0.0003}(10000)$</td>
<td>23.56%</td>
<td>54.28%</td>
</tr>
<tr>
<td>BA: $N=10000$, $E[D]=2$</td>
<td>16.28%</td>
<td>46.76%</td>
</tr>
</tbody>
</table>

### VI. Conclusion

In this study, we analyzed the role of critical links in network controllability. Simulation results on communication...
TABLE X

PERFORMANCE INDICATORS FOR THE APPROXIMATION $n_{c,\text{prot}}$ FOR SYNTHETIC NETWORKS

<table>
<thead>
<tr>
<th>Types of networks</th>
<th>$r^*$</th>
<th>$\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>ER: $G_{0.05}(100)$</td>
<td>5.21%</td>
<td>100%</td>
</tr>
<tr>
<td>BA: $N=200$, $E[D]=4$</td>
<td>8.63%</td>
<td>100%</td>
</tr>
<tr>
<td>ER: $G_{0.0003}(10000)$</td>
<td>4.16%</td>
<td>100%</td>
</tr>
<tr>
<td>BA: $N=10000$, $E[D]=2$</td>
<td>6.94%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Fig. 9. The normalized maximum number of controllable nodes as a function of the fraction of removed links $l$ in synthetic networks under random attacks. The results for each fraction $l$ is based on 10000 simulations.

(c) ER: $G_{0.0003}(10000)$, $E[D]=3$  (d) BA: $N=10000$, $E[D]=2$

Fig. 10. The normalized maximum number of controllable nodes as a function of the fraction of removed links $l$ in synthetic networks under targeted attacks. The results for each fraction $l$ is based on 10000 simulations.

(c) ER: $G_{0.0003}(10000)$, $E[D]=3$  (d) BA: $N=10000$, $E[D]=2$

Fig. 11. The normalized maximum number of controllable nodes $n_c$ as a function of the fraction of removed links $l$ in synthetic networks under random attacks with protection. The results for each fraction $l$ is based on 10000 simulations. In each sub-figure, the vertical dashed line marks the position where $l = 1 - l_c$.

ACKNOWLEDGEMENT

This research was supported by the China Scholarship Council (No. 201706220115).

REFERENCES
