Reachability-based Robustness of Network Controllability under Node and Edge Attacks

Deven Parekh
School of Computer Science
McGill University
Montreal, Quebec
deven.parekh@mail.mcgill.ca

Derek Ruths
School of Computer Science
McGill University
Montreal, Quebec
derek.ruths@mcgill.ca

Justin Ruths
Engineering Systems & Design
Singapore University of Technology and Design
Singapore, Singapore
justinruths@sutd.edu.sg

***Abstract*—In real world applications, control is always performed without perfect knowledge, perfect models, and often, under changing conditions. Such circumstances are particularly true of complex systems. As a result, application of control theory to complex systems requires the development and implementation of control policies that are robust to unexpected and potentially malicious changes to the underlying network. This paper makes three important contributions along this direction. First, we introduce a new definition of robustness which captures realistic constraints imposed by many control problems. Second, we develop a novel algorithm for computing this robustness measure. Third, we conduct a thorough assessment of the control robustness of different synthetic networks to a wide array of attacks/network perturbations. We find that our robustness measure is behaviorally different from other robustness measurements in the literature and that the attacks considered highlight a number of ways in which network properties correlate with control robustness.**

I. Introduction

Many complex systems — biological, social as well as technological — have been studied and understood in the light of complex network topology and dynamics [1–4]. Recent work has highlighted the importance of understanding the extent to which complex networked systems are controllable [5, 6]. A controllable system can be driven from any arbitrary state to any desired state through the application of external inputs. However, like any property dependent on the structure of the system, controllability is sensitive to perturbations that occur to the network. Understanding how network controllability changes in the context of node or link failures as well as which network structure designs have control schemes that are most resilient to change is an essential part of making such theoretical formalisms practically useful.

While work on robustness in the context of control is nascent, a few papers have begun to investigate the robustness of controllability to various failures and attacks. Following broader interest in statistics surrounding the number of controls (N_c) necessary to control a complex network (e.g., [5–8]), these existing studies have primarily measured robustness as the number of additional controls (N_c) required to maintain full controllability following a change in the topology of the network [9, 10].

Such a definition of robustness effectively makes the assumption that new controls can be added to the network as components fail: e.g., such a definition of robustness assumes that one is always in a position to add more controls, only that we have a preference to add as few controls as possible. However, in practice, critical aspects of the system may be unknown, resources constrained, and regions flagged for direct control not easy to reach: thus, in many cases, controls cannot be simply added without great cost.

With this in mind, in this paper we explore an alternative definition of robustness concerned with how the number of controllable (reachable) nodes (N_r) changes due to a topological change (attack). Such a definition favors control configurations that retain control over more of the network rather than those which require fewer controls to be added to regain full controllability. In order to distinguish these notions of robustness, we refer to the existing definition as *control-based* and our proposed definition as *reachability-based robustness* (CR and RR, respectively). Different systems and conditions will determine which of these definitions will be appropriate to use - but certainly both capture practical constraints and objectives.

This paper makes three core contributions. First, we formalize reachability-based robustness. This formalization involves the development of a highly non-trivial algorithm which has been alluded to in literature, but (to our knowledge) has never before been flushed out or published [11, 12]. Second, using random models, we establish how control-based and reachability-based definitions of robustness differ (and are similar) both over different types of networks and different types of attacks. Where attacks are concerned, we consider a much more comprehensive set than has been evaluated elsewhere in the literature. Specifically, we assess all standard node and edge attacks which depend on first-order degree properties. This extensive set of attacks constitutes our third contribution and reveals that there are significantly more nuanced factors determining the most effective attacks (and most robust configurations) than what is currently reported in the literature. Moreover, our study raises a number of questions about the relationship of robustness to network structure in general and to the nature of cacti - the control structures that govern the control of complex systems.

II. Background

Existing work and the present paper employ the formalism of structural controllability in order to make the computation of control properties tractable for large-scale systems [13]. Here we first briefly review structural controllability and then discuss prior work on the robustness of controllability.

A. Structural Controllability

For a linear time-invariant control system without intrinsic node dynamics, the state of a node $x_i(t)$ is governed by the equation,

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{1}$$

where $x(t) = [x_1(t), x_2(t), ..., x_N(t)]^T$ is the vector denoting the state of the N nodes at time t, A is the $N \times N$ adjacency matrix of the network for which the component a_{ij} is the edge weight from node x_j to node x_i. The $N \times m$ matrix B indicates nodes where the input control signals are applied. The system (A, B) is controllable if and only if the controllability matrix

$$C = [B, AB, A^2B, ..., A^{N-1}B] \tag{2}$$

has full rank, i.e., $rank(C) = N$. Because this rank is computationally infeasible to compute for large-scale networks, we adopt tools from structural control to make the analysis tractable. It can be shown that if the system is structurally controllable, it is controllable for almost all choices of edge weights except for some pathological cases [5]. Given a network connectivity encoded in A, the number and location of the minimum control inputs to fully control a network can be found using maximum unweighted matching [5]. Using edges in the matching, stems and cycles can be formed which together compose the control cacti structure (see [5] for terminology).

B. Prior Work on Robustness of Controllability

To our knowledge, all existing studies of robustness of controllability have measured the increase in the minimum number of controls required as a proxy for the reduction in controllability due to a failure. We refer to this as *control-based robustness* (CR). Liu et al. [5] showed that sparse and heterogeneous networks are difficult to control and provided a method to observe robustness under edge failures by calculating fraction of critical, redundant and ordinary edges which are classified as such based on change in N_c upon their removal. Pu et al. [10] investigated the behavior of controllability of various networks under random, targeted, and cascading failures of nodes. They found that degree-based attacks are more effective (damaging) than random attacks for directed Erdős-Rényi (ER) and directed scale-free (SF) networks. Furthermore, they observed that a larger number of links and greater network homogeneity increases the robustness of network controllability. Finally, Nie et al. [9] analyzed robustness of control under random and targeted cascading failures. They report that ER networks with smaller average degrees are more robust against a highest-load cascading attack while SF networks with smaller power-law exponents are more vulnerable than those with large exponents. Furthermore, random attacks are more effective than targeted attacks for less heterogeneous networks under moderate edge removal rates.

III. Methods and Data

In this section, we define reachability-based robustness, the algorithmic means by which it is calculated, and the network models as well as the attacks which will be used to empirically assess the attributes of the both control- and reachability-based robustness.

A. Reachability-based Robustness

As mentioned previously, here we investigate a robustness measure that focuses on how much of the network *remains under control* in the presence of an attack. Unlike control-based robustness, in our measure, no new controls are added. The original set of controls designed for the original network remain in place (except those whose nodes were removed by the attack, if any). Our measure of robustness asks how many nodes are *still* under control after the perturbation to the network topology. To assess the robustness as the perturbation becomes increasingly severe, we consider average controllability ($\widehat{N}_r$), given by the area under the *controllability curve* in Figures 3 & 4, for the perturbation ranging from affecting 0 to 50% of the network (nodes or edges, depending on the attack). In this study, we show this area graphically (see Figure 7) but in large-scale work, this area could be summarized numerically and subjected to more quantitative analysis.

Notice, however, that our formulation thus far requires a particular initial assignment of controls to nodes in the network (called the *control configuration*). In order to obtain a robustness measure for a network, we sample multiple control configurations for the network and report the robustness score $\widehat{N}_r$ averaged over these configurations. Though the choice of configurations can be arbitrary, in this study we used a sample of 10 different configurations that can fully control an unperturbed network. This choice of configurations (those that can fully control the network) enables us to compare reachability-based robustness to control-based robustness.

Returning to the issue of computing our robustness value for a network, however, we still have a problem. Specifically, how do we compute the number of nodes in an arbitrary network controlled by an arbitrary control configuration (the need for handling an "arbitrary" network stems from the fact that a perturbation could affect a network in any number of ways)? In order to do this, we require a simple and efficient algorithm for finding the cacti control structure given a fixed set of controls. While this problem of finding the generic dimension of controllable subspace has been discussed in literature [11, 12], quite remarkably, a clear algorithmic approach appears to be missing. Presenting this algorithm is the first of our contributions.

To understand the problem, consider the example in Figure 1(a), which shows a network G with two controls X and Y attached to driver nodes A and B. The number of minimum

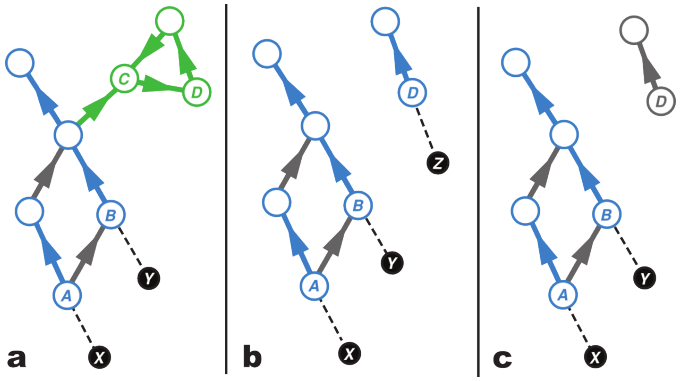

Fig. 1: **(a)** An example network G with driver nodes A and B. Stems are highlighted in blue, cycles in green **(b)** N_c increases by 1 as node C is removed and cycle is broken into a stem which requires a new control Z **(c)** N_r decreases by 3 as node C is removed and stem starting with D becomes uncontrollable

controls N_c is 2 while number of controllable nodes N_r is 8. Figure 1(b) demonstrates an increase in N_c after node C is removed from G. After removal of C, in order to fully control the network, a new control Z needs to be attached to the unmatched node D. Thus, N_c increases to 3. On the other hand, Figure 1(c) shows the decrease in controllable nodes N_r given the same set of controls (X and Y) as before percolation. The value of N_r reduces to 5 since the stem starting with node D is no longer reachable using controls X and Y.

In order to calculate N_r given controls X and Y, Hosoe's theorem can be used [11]. Consider the linear system given in Equation 1 as a graph $G(A, B)$, the generic dimension of the controllability matrix C (Equation 2) is given as

$$rank(C) = \max_{G_{sub} \in G} |E(G_{sub})| \tag{3}$$

where G_{sub} is the set of all stem/cycle disjoint subgraphs of the $G(A, B)$ that are reachable from controls B and $|E(G_{sub})|$ is the number of edges in the subgraph G_{sub}. Though the proof of the theorem is well presented, a algorithm to calculate the rank is missing. On the other hand, Poljak [12] gives a graph-theoretic proof of the theorem, which describes a method to calculate the rank in Equation 3 as well as the cacti structure by finding a maximum-weighted cycle partition in a modified version of graph $G(A, B)$. However,

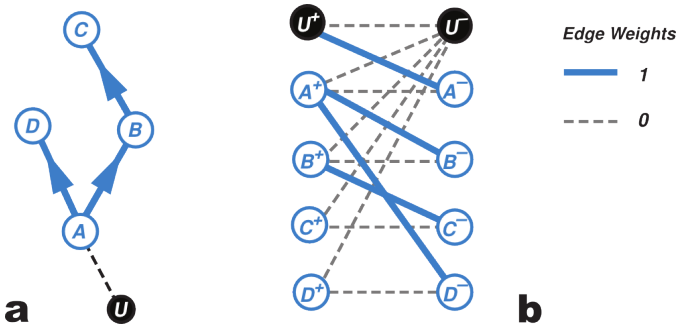

Fig. 2: **(a)** An example network G with $N = 5$ nodes with external control node U attached to driver node A **(b)** Bipartite graph with $2N$ nodes, a pair of +ve and -ve nodes for each node in G.

the solution presented therein involves solving an integer linear program, which requires sophisticated linear program solvers. In contrast, we employ a simpler graph-theoretic algorithm. We convert the problem of finding maximum-weighted cycle partition into that of finding perfect maximum-weighted matching in a bipartite graph created from $G(A, B)$ (see Algorithm 1 and Figure 2). Using Fibonacci Heap in the implementation, we have the time complexity of the algorithm to be $\mathcal{O}(NL+mN^2+4N^2log2N)$ where N and L are number of nodes and edges in $G(A, B)$ respectively and m is the number of controls.

Algorithm 1 Algorithm to find Cacti for fixed controls

Input: Network G, Control node set C (G includes nodes in C and edges to driver nodes)
Output: Cacti representing control structure

$G' \leftarrow G - x$, x not reachable from C // using Depth First Search
Create a Bipartite Graph G_B with:
  ▷ $2|V(G')|$ nodes, a pair of +ve and -ve nodes for each node in G'
for all edge (u, v) in G' **do**
  Add an edge (u^+, v^-) to G_B with weight 1
end for
for all control node c in C **do**
  $d \leftarrow Neighbor(c)$ // d is driver node
  Add an edge (c^+, d^-) to G_B with weight 1
  for all node x in G' such that x is not in C **do**
    Add an edge (x^+, c^-) to G_B with weight 0
  end for
end for
for all node u in G' **do**
  Add an edge (u^+, u^-) to G_B with weight 0 // self loop
end for
// Add large enough weight to make it a perfect matching
Add weight W to all edges in G_B such that $W > \sum weight(e), \forall e \in Edges(G_B)$
Perform weighted maximum matching algorithm on G_B to get a matching M
Map edges in M back to edges in G and join them to form stems and cycles of cacti.
Number of controllable nodes is number of matched nodes in cacti // control nodes in C are not matched

B. Network Models and Data

In this work we focus our study on synthetic network models. Because the formation mechanisms of these synthetic models are known to us, they offer an opportunity to establish connections between the robustness of controllability in networks that have features which are frequently observed in nature. One of the distinguishing features of this work over the current work on the robustness of network controllability is our broader survey of synthetic network models. Previous work has established that while these models share some

common statistics (e.g., scale-free degree distribution) they show significant differences in their control properties [6].

In this study, all networks have $N = 1000$ nodes; average degrees $k = 2, 4, 6, 8, 10, 12$ were considered except for duplication divergence networks, in which the formation mechanisms yields networks with highly varied average degree. These average degree values represent already a highly conservative approximation of the average degrees seen in real world networks. In all results presented, each realization of network type and parameter values is generated with 10 different instances to provide a notion of expected (average) behavior. Even with this rather small level of averaging, for $N = 1000$ the error bars are very small in most cases, underscoring that our results are stable and this approach is sufficient to observe the expected control properties of these networks. The network models are described below.

Erdős-Rényi (ER) Using random connection model described in [14], the random networks were generated until the number of edges (E) was within an acceptable tolerance: $|E - kN| < 0.001kN$. The homogeneity of ER networks typically leads to networks that have very few controls with relatively long stems and cycles.

Barabási-Albert (BA) These networks were generated using preferential attachment model presented in [15]. BA networks are inherently acyclic, which limits the range of the effect that a control can have in the network. Therefore, BA networks are characterized by a large number of controls and short stems and cycles.

Local Attachment (LA) The networks were created using local attachment model [16], where N nodes are added incrementally with m edges each. Of the m edges, r are connected randomly from a new node to existing nodes in network, while remaining $m - r$ edges are connected to neighbors of randomly chosen nodes. Clustering can be added to the network by increasing the fraction $m - r$. We calculate r as $r = (1 - c)m$, where different clustering values were chosen as $c = 0, 0.25, 0.5, 0.75$. LA networks are also acyclic and tend to exhibit similar control characteristics.

Duplication Divergence (DD) In duplication-divergence model, a node is duplicated and its edges are kept with a probability s [17]. Initial directed network which undergoes duplication is taken as the network with an edge from both 0 to 1 and 1 to 0. Values for probability of duplication $s = 0.1, 0.3, 0.5, 0.7, 0.9$ were considered. DD networks have the most diverse control profiles of the synthetic networks surveyed here.

C. Types of Attacks

While attacker models could potentially employ different kinds of knowledge about the system, we focus on a scenario in which attackers have access to fundamental structural information: the degree of the nodes in the network. Pósfai et al. [7] explored the role that various relative degree relationships determine properties of network controllability. With this as guidance, we consider such relative degree relationships in our study of robustness of network controllability.

For targeted node attacks, we select the node to be attacked based on its in-degree, out-degree, or total degree. A node may be important, in the context of control, with high in-degree because it is a node through which many potential paths may pass or with high out-degree because it has the potential to propagate the influence of a control to many neighbors. With regard to edge attacks, we consider the degree information of the source (s) and target (t) nodes of the edge. We considered the following five attacks which are functions of the degree of s and t. Edges were selected in descending order of the score returned by a given function.

- ▷ **in-in deg:** $in\_degree(s) + in\_degree(t)$
- ▷ **in-out deg:** $in\_degree(s) + out\_degree(t)$
- ▷ **out-in deg:** $out\_degree(s) + in\_degree(t)$
- ▷ **out-out deg:** $out\_degree(s) + out\_degree(t)$
- ▷ **total deg:** $total\_degree(s) + total\_degree(t)$

These combinations explore the extent to which an edge is important due to being a funnel (in-in), being a source (out-out), being a bridge (in-out), or other such functions. Finally, because we are interested in the contrast between random failures and targeted attacks, we also evaluate a random node and edge percolation "attack".

IV. Results

In this section we summarize how we generated results that show effects of node and edge attacks on reachability- and control-based robustness for different networks. We explain the plots involved and highlight key observations that can be made from plots.

While the node- and edge-based attacks differ to some extent, the approach to assessing robustness (both numerically and visually) was consistent across network models and attack types. As seen in Figures 3 and 4, we take the control configuration to be a minimum control set required to control the original (unperturbed) network. Because the minimum controls guarantee complete controllability, the fraction of controllable nodes, $n_r = N_r/N = 1$, before the percolation process begins. With each step, 5% of nodes/edges are removed up to at total of 50% percolation. As opposed to Pu et al. [10], we do not keep any node in network after it is removed (or fully disconnected as is the case when edges are removed), so that the change in N_r reflects also the change in network size. Because the number and location of the controls cannot change, when the nodes they directly connect to are removed, that control will lose it's connection to the network and no longer be able to contribute to controlling the networks. Figures 3 and 4 show the change in the fraction of controllable nodes n_r for different networks with respect to node/edge percolation with different attacks.

A. Initial Observations

Node attacks. There are a few important observations that can be inferred from the plots in Figure 3. Unlike [10], we find that degree-based attacks are not always more effective (more damaging) than random attack. For example, in the case of

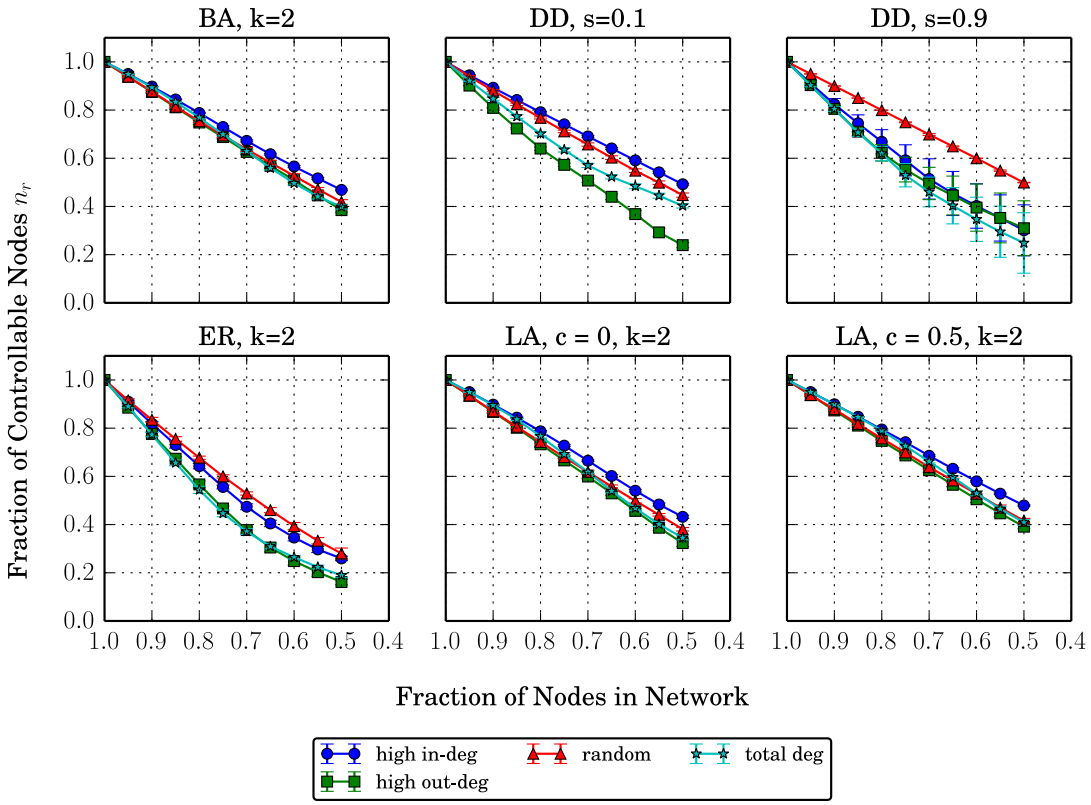

Fig. 3: The robustness of control structures in the four network models to degree node-based attacks. Due to space limitations, only the results for one parameter choice are shown — these are representative of all other parameter choices.

BA and LA networks, random attack does nearly the same as the most effective, high out-degree, attack. In the case of DD and ER networks random attack is the least effective. We also find significant variations among different types of degree-based attacks. High out-degree attacks stands out as being the most effective in most of the networks, while high in-degree and total degree attacks show considerable difference in effectiveness across network types. These differences underscore the importance of evaluating various metrics for robustness of network controllability.

Edge attacks. As seen in Figure 4, the in-out degree attack initially starts out being less effective than a random attack but after a few steps, it rapidly degrades controllability. This effect can be better explained by observing the change in the number of strongly connected components (SCC) as well as the change in average stem/cycle lengths (described next). Also noteworthy is that out-in degree and total degree are almost always least effective, while random attack maintains average effectiveness. This further confirms our proposition that degree-based attacks exhibit varying effectiveness relative to random attack for different networks and suggesting the role of more nuanced network features in the phenomena.

B. Connected Components and Stem Lengths

In order to understand the behavior of attacks on robustness we analyzed how the number of strongly-connected components N_{SCC} and average stem length vary under particular edge attacks (see Figure 6). Average stem length is the weighted mean of lengths of stems in the cacti control structure, which gives an idea of how an attack changes the cacti. Since BA and LA networks are acyclic, N_{SCC} remains constant at 1000 hence not shown in the figures. While for ER networks, we can see that the effectiveness of an attack is correlated with an increase in N_{SCC}. It can be observed that the in-out degree attack rapidly creates a larger number of SCCs than other attacks. Also, there is a strong correlation between change in average stem length shown in Figure 6(b) & 6(c) and change in controllable nodes shown in Figure 4. For example, the in-out attack, which tends to be the most effective, also tends to create shorter stems on average after percolation.

V. Discussion

A. Robustness definitions have different behavior

Figures 5(a) and (b) show how the number of controllable nodes, N_r (or fraction $n_r = N_r/N$), decreases and the number of minimum controls, N_c, increases for BA and ER networks

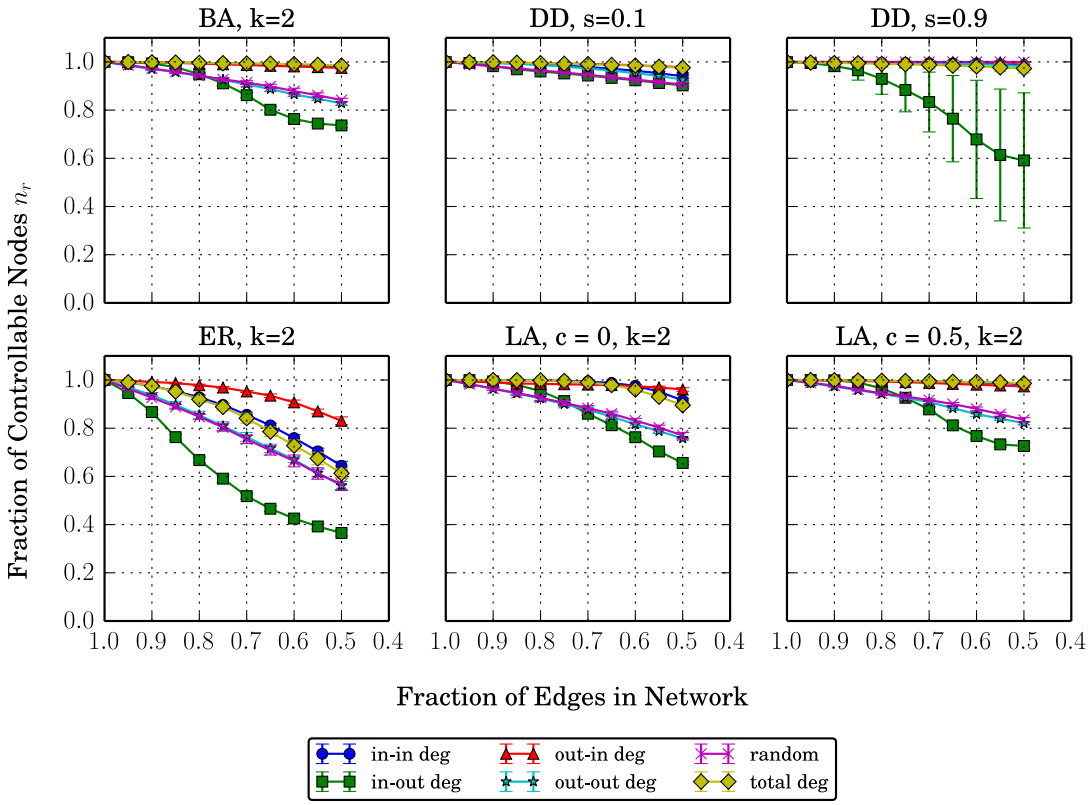

Fig. 4: The robustness of control structures in the four network models to degree edge-based attacks. Due to space limitations, only the results for one parameter choice are shown — these are representative of all other parameter choices.

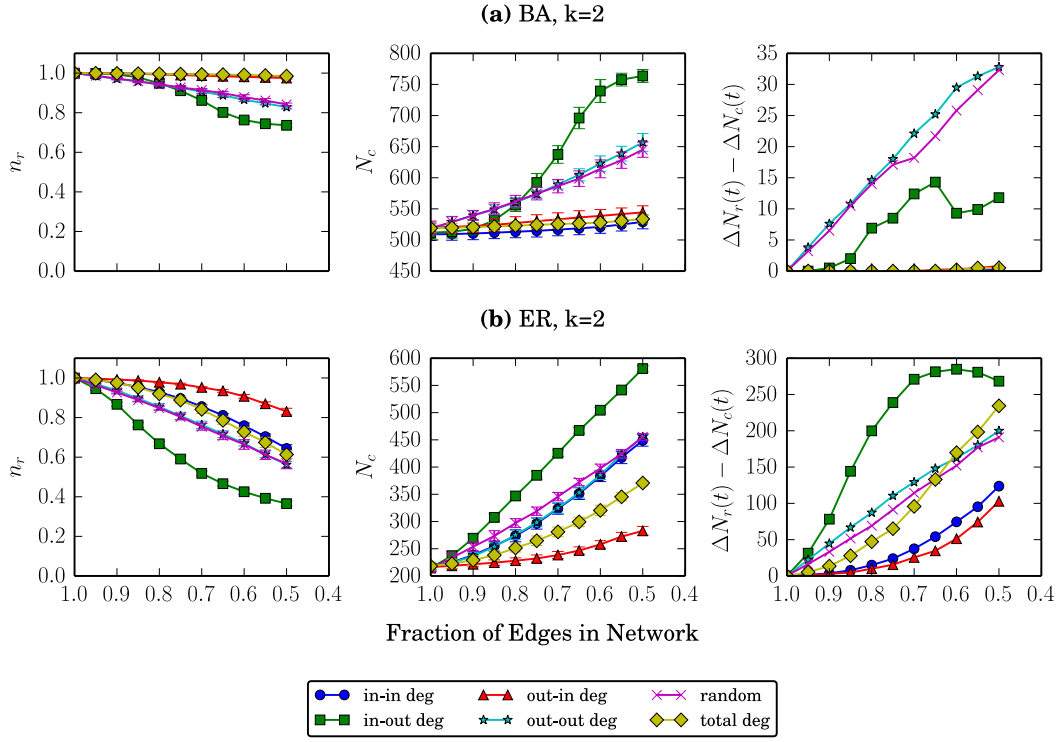

Fig. 5: Comparison showing Reachability- and Control-based robustness measures for ER an BA networks. $n_r = N_r/N$ is fraction of controllable nodes and N_c is minimum number of controls required for full controllability

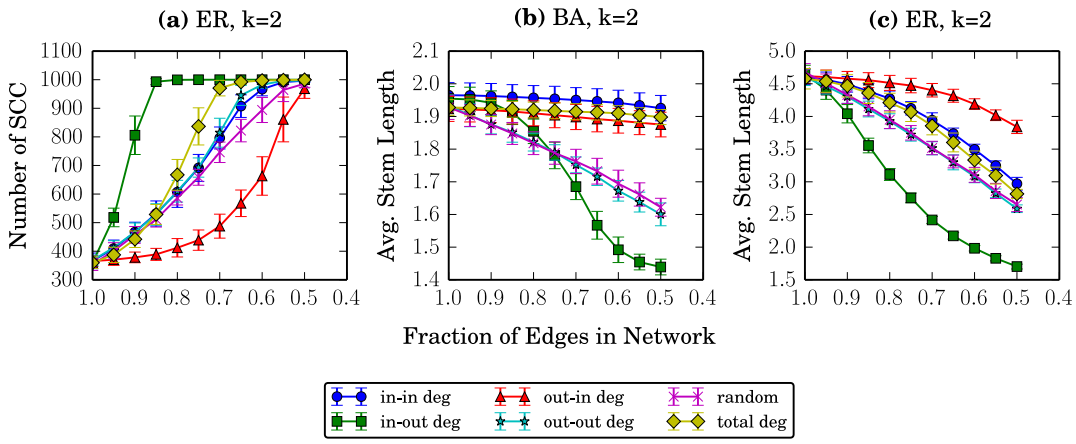

Fig. 6: Variation in number of strongly connected components and average stem length under edge attacks

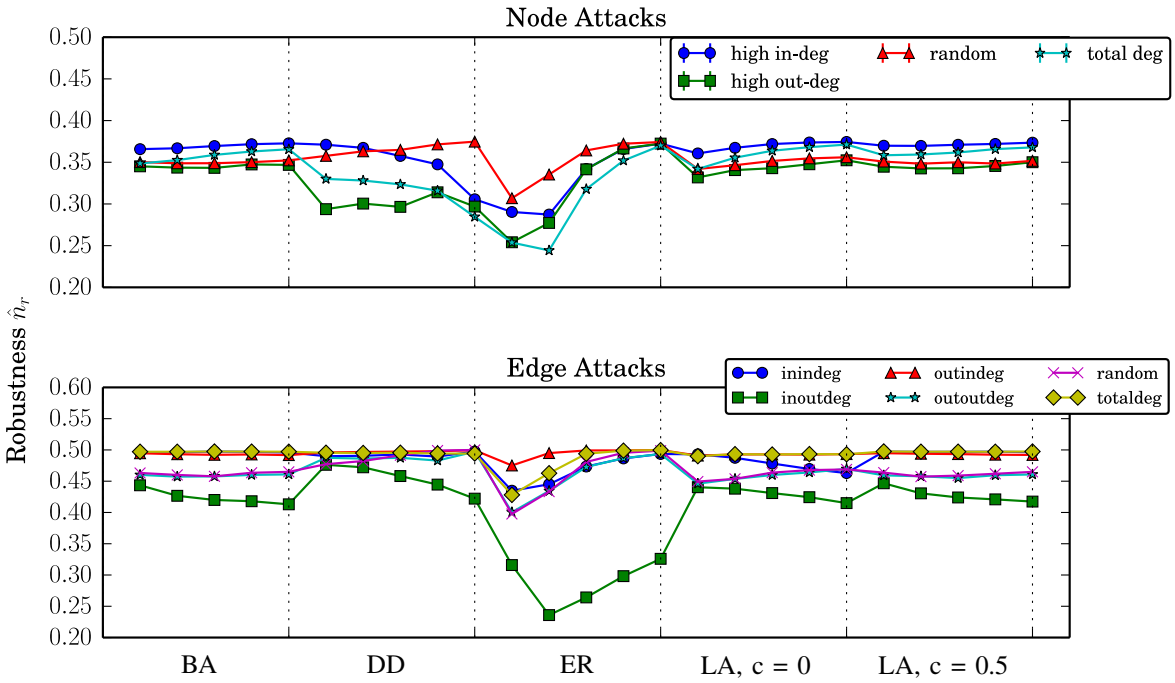

Fig. 7: Reachability-based robustness for all networks grouped by type. Five data points, each for an average degree k=2,4,6,8,10 (or probability s=0.1, 0.3, 0.5, 0.7, 0.9 in case of DD) is shown for each network type.

under edge percolation. In order to verify whether changes in N_r tell us a different story about robustness of networks than changes in N_c, in Figure 5(a) and (b) we also plotted $\Delta N_r(t) - \Delta N_c(t)$ for each percolation step t, where $\Delta N_r(t) = N_r(0) - N_r(t)$ and $\Delta N_c(t) = N_c(t) - N_r(0)$. The intuition here is to capture increase in N_c after percolation and compare it with decrease in N_r. We can see that in case of BA network, difference between the decrease in N_r and the increase in N_c for some attacks is almost negligible. While for more effective attacks such as in-out degree attack, there is a greater decrease in N_r for a given increase in N_c. This gap between N_r and N_c widens greatly in case of ER network. This strongly suggests that N_r (reachability) based measures reveal different aspects of network vulnerability to particular node- and edge-based attacks compared with measures using N_c.

B. Robustness dependence on network types

Figure 7 highlights the extent to which different network types have different responses to various attacks. The fact that the robustness scores $\widehat{N}_r$ (or fraction $\widehat{n}_r = \widehat{N}_r/N$) differ indicates that clustering, degree homogeneity, the presence of cycles, and other higher-order network features may impact a particular network's vulnerability to attack. While an investigation into the nature of these signature differences is beyond the scope and length of this paper, we can highlight a number of intriguing trends which deserve attention in future work.

- *Clustering does not affect robustness to node attacks.* Notice that BA networks and LA networks with high clustering tend to exhibit similar behavior for all node attacks. LA networks have both a scale-free degree distribution and clustering - thus the similarity in behavior suggests that the addition of clustering does not affect the overall vulnerability to node attacks.
- *Degree distribution.* Even though both LA with zero clustering and ER are both random models, the former creates acyclic networks and exhibits greater resistance to attacks than ER which is more homogeneous than LA and consists of cycles.
- *Average degree sometimes can play a role.* While space does not permit visualizations, our analysis indicates that, under node attacks, $\widehat{N}_r$ does not show much variability across different average degrees except for the case of ER networks. In the case of ER networks, robustness increases with average degree (likely due to presence of more edges).
  Similarly for edge attacks, there is only slight change in $\widehat{N}_r$ with increasing average degree, except for the case of ER networks. It is surprising to find that the in-out degree attack in fact is more effective with increase in average degree. In-out degree attack is systematically the most effective attack for all networks, as well as across different average degrees.

C. Robustness dependence on attack types

While this point has already been indirectly explored above, it is worth highlighting that Figure 7 (as well as the other results figures) demonstrate the variable effect a given attack can have. Interestingly, in some instances, node attacks have more-or-less equivalent robustness scores; whereas in others, the same attacks can have very different and highly variable robustness scores. This perspective suggests that, in addition to understanding how particular network structures achieve differential degrees of robustness; another fruitful approach might consider the means by which different attacks achieve similar (or different) robustness levels across a wide array of networks.

VI. Conclusion

The robustness of control structures will be an important consideration when applying theory governing the control of complex systems. In this paper we have proposed a new measure of robustness which we consider to capture many of the constraints that arise when controlling real-world systems. We find that this measure functionally differs from existing measures in the literature and that, when subjected to a variety of node- and edge-based attacks, yields trends that suggest ways in which network properties relate to the robustness of control structures.

References

[1] M. Newman, A.-L. Barabási, and D. J. Watts, *The structure and dynamics of networks*. Princeton University Press, 2006.

[2] R. Milo, S. Shen-Orr, S. Itzkovitz, N. Kashtan, D. Chklovskii, and U. Alon, "Network motifs: simple building blocks of complex networks," *Science*, vol. 298, no. 5594, pp. 824–827, 2002.

[3] S. P. Borgatti, A. Mehra, D. J. Brass, and G. Labianca, "Network analysis in the social sciences," *science*, vol. 323, no. 5916, pp. 892–895, 2009.

[4] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of modern physics*, vol. 74, no. 1, p. 47, 2002.

[5] Y.-Y. Liu, J.-J. Slotine, and A.-L. Barabási, "Controllability of complex networks," *Nature*, vol. 473, no. 7346, pp. 167–173, 2011.

[6] J. Ruths and D. Ruths, "Control profiles of complex networks," *Science*, vol. 343, no. 6177, pp. 1373–1376, 2014.

[7] M. Pósfai, Y.-Y. Liu, J.-J. Slotine, and A.-L. Barabási, "Effect of correlations on network controllability," *Scientific reports*, vol. 3, 2013.

[8] T. Jia, Y.-Y. Liu, E. Csóka, M. Pósfai, J.-J. Slotine, and A.-L. Barabási, "Emergence of bimodality in controlling complex networks," *Nature communications*, vol. 4, 2013.

[9] S. Nie, X. Wang, H. Zhang, Q. Li, and B. Wang, "Robustness of controllability for networks based on edge-attack," *PloS one*, vol. 9, no. 2, p. e89066, 2014.

[10] C.-L. Pu, W.-J. Pei, and A. Michaelson, "Robustness analysis of network controllability," *Physica A: Statistical Mechanics and its Applications*, vol. 391, no. 18, pp. 4420–4425, 2012.

[11] S. Hosoe, "Determination of generic dimensions of controllable subspaces and its application," *Automatic Control, IEEE Transactions on*, vol. 25, no. 6, pp. 1192–1196, 1980.

[12] S. Poljak, "On the generic dimension of controllable subspaces," *Automatic Control, IEEE Transactions on*, vol. 35, no. 3, pp. 367–369, 1990.

[13] C.-T. Lin, "Structural controllability," *Automatic Control, IEEE Transactions on*, vol. 19, no. 3, pp. 201–208, 1974.

[14] P. Erdős and A. Rényi, "On Random Graphs, I," *Publicationes Mathematicae*, vol. 6, pp. 290–297, 1959.

[15] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *science*, vol. 286, no. 5439, pp. 509–512, 1999.

[16] M. O. Jackson and B. W. Rogers, "Meeting strangers and friends of friends: How random are social networks?" *The American economic review*, pp. 890–915, 2007.

[17] I. Ispolatov, P. Krapivsky, and A. Yuryev, "Duplication-divergence model of protein interaction network," *Physical review E*, vol. 71, no. 6, p. 061911, 2005.