Influence of Malfunction and Attack on Target Controllability

Liming Zhang, Zhijian Zhang [a], Yuan Chen, Qianyu Ji, Jian Wang [b]
School of Electronic Science and Engineering, Nanjing University, Nanjing, China
[a]njuzzj@nju.edu.cn, [b]wangjnju@nju.edu.cn

Abstract. Target controllability is an interesting property of complex network and attracts many researchers from different fields. However, controlling large natural or technological networks is a great challenge. But it is not feasible and sometimes unnecessary to control the entire network, hence target control seems efficient in this situation. The greedy algorithm was developed and offers a good approximation to calculate the minimum number of driver nodes, where control signals are injected, for control the target nodes in the network. Based on the target control theory, we investigate the target controllability of directed Erdős-Rényi and the Barabási-Albert networks under attack or failure. Results show that degree-based node attack is more efficient than random attacks in directed BA networks on network target controllability but the similar in directed ER networks.

Keywords: complex network; target control; controllability; structural controllability.

1. Introduction

Complex networks have received great attention from many researchers in past decades. Advances have focused on network topological characteristics and network dynamics. Complex networks consist of a large number of nodes and the complex connections between nodes, through the connections the nodes in the network somehow influence each other. A directed complex network can be regarded as a linear control system, so the problem of the controllability of the network can be solved by some controllability methods in linear system control theory. For a structural controllable system, there is always an appropriate input to drive all the nodes to reach the expected final state in a limited time for any initial state of each node in the network. However, many technological, social and biological systems have massive size and complexity which make it difficult or unnecessary to control the full network. Hence, we can choose the strategy that we just drive the target nodes to the expected state.

Many applications of target control have been developed in domain-specific areas in economic, chemical engineering, biology and epidemics [3][4][5][6]. Waarde et al. [1] studied the target control of dynamical networks based on a class of state matrices called distance-information preserving matrices. And Gao et al. [2] made further research on the target control of complex networks. They presented a greedy algorithm to approximate the set of the driving nodes, which contains the minimum number of driving nodes needed to realize the target control of a given complex network.

An actual complex network system is inevitably broken by random node failure or subjected to external attacks [7][8][9], which will increase the difficulty of control or even lead to the collapse of the entire network. In this paper, we investigate the influence of the malfunctions and degree-based attack on the target controllability of a complex network, by investigating it on the Erdős-Rényi (ER) and the Barabási-Albert (BA) networks.

The structure of the remainder of this article is as follows: we first introduce the target controllability based on the structural controllability and the control theory in linear network systems, and briefly introduce the greedy algorithm in Section II. Then, in Section III, we explain the two strategy we choose to research the influence of malfunction and attack on target controllability, and show our results of the experiment. Finally, in Section IV, we briefly summarize major findings, put forward the facing challenges and look forward to the future work.

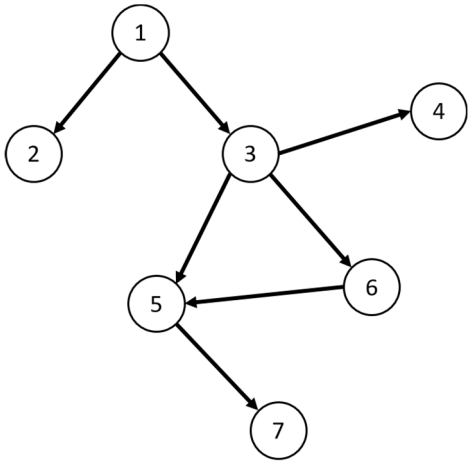

Fig 1. A Simple Network.

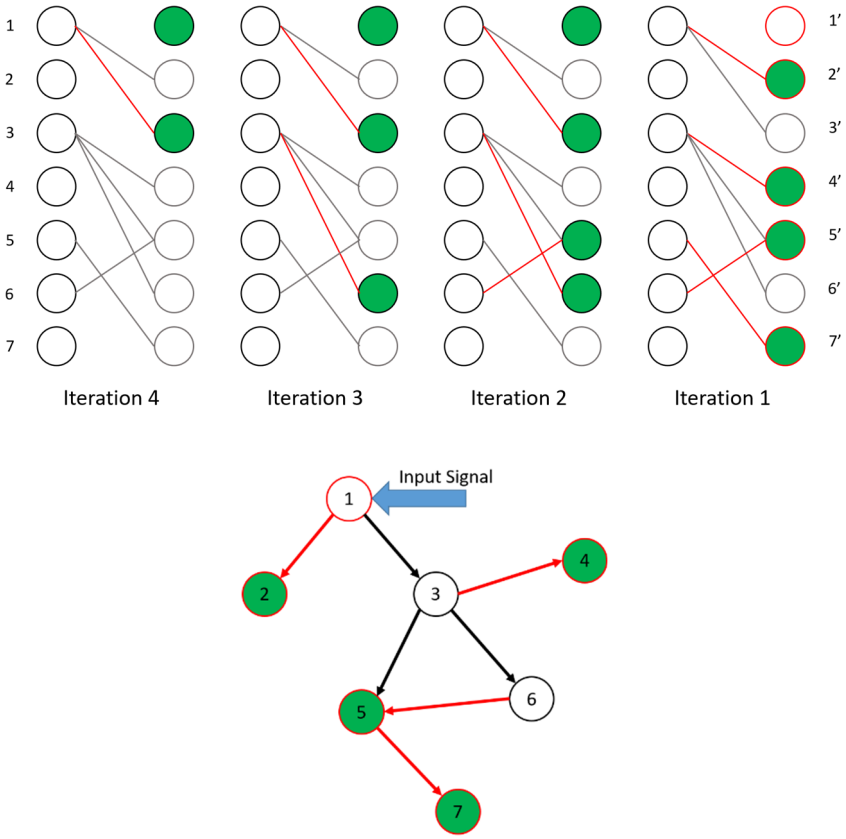

Fig 2. Process of GA for the Network in Fig.1 (No.2) and the Result of the GA (No.3)

2. Target Control

Most of the real network systems is driven by nonlinear processes, but it is impossible to write a general equation tocapture the characteristic and the rules of a real network system. Even for some network systems, such as a biological network system, we do not understand its rules. According to the control theory [10], the linear control systems are described by the equation as:

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

where $x(t)=\{x_1(t), x_2(t), \ldots, x_N(t)\}^T$, which is the state of the N nodes at time t. A is the $N \times N$ adjacency matrix of the network, in which the value is 0 or 1 presenting the connections between the

nodes. B is the $N \times M$ input matrix which presents the nodes where the input signals are imposed. The input signal vector $u(t)=\{u_1(t), u_2(t), \ldots, u_M(t)\}^T$ is the state of the input signals at time t. For the target control, it is unnecessary to satisfy the states of all nodes, we just chose a fraction f of the nodes as a target set $T = \{t_1, t_2, \ldots, t_S\}$ which is an $S \times N$ matrix where $S = fN$. Therefore, the state of a target control system can be defined as:

$$z(t)=Ty(t) \tag{2}$$

where $z(t)$ is a vector of the state of the target nodes at a given time t.

The target controllability can be seen similar with the output controllability [11], the system (A, B, T) is target controllable if and only if the dimension of the subspace $d(A, B, T)$ satisfies:

$$D(A, B, T) = rank(TB, TAB, TA^2B, \ldots, TA^{(N-1)}B) = S \tag{3}$$

This definition of the target controllability is given by Gao et al. and they propose a k-walk theory for networks with one control input and develop a greedy algorithm (GA) based on maximum matching for networks that require more than one control input. Although there are still some limitations for the GA method, but it still offers a good approximation to the minimum set of inputs sufficient for target control.

Fig.2 shows the process of GA to find the driver nodes to control the targets which are nodes $\{x_1, x_2, x_4, x_5, x_7\}$ that are highlighted in red. By solving the maximum matching problem on an induced bipartite graph, in Iteration 1 we get 4 target nodes $\{x_2, x_4, x_5, x_7\}$, which are marked as green, that are matched by nodes $\{x_1, x_3, x_5, x_6\}$ and these 4 matched nodes are the target nodes in the next iteration. After four times of iteration there is no matching or matched nodes left in the network, the unmatched nodes are finally the driver nodes. For the example directed network that is given in Fig.1, the driver node to control the targets is the node x_1.

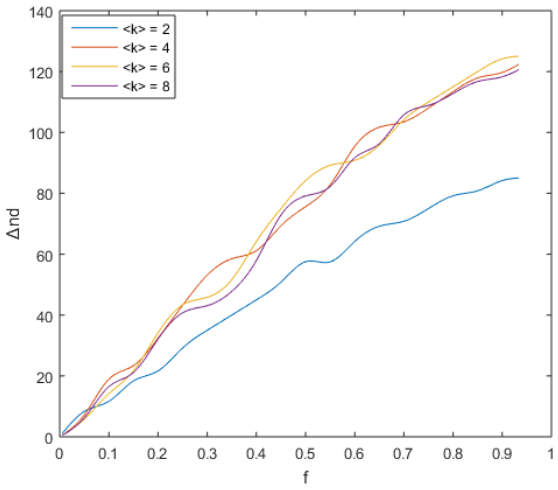

Fig 3. Random Node Failure in BA Networks.

3. Malfunction and Attack

Here we investigate the behavior of the network controllability under to different kinds of situation: random node failure and degree-based attack. When a node malfunctions or is attacked by external factors, the structure of the network will change. Therefore, as a result, the target controllability will change due to the change of the network structure. We assume a simple strategy that when a node malfunctions, the edges connected to the node are removed from the network, but the node itself is still in the network, so that the size of the network doesn't change after attacks or failures. Hence,

even if the target node malfunctions or is under attack, it is still regarded to be able to be under control by an extern input. Here we study directed EA networks and directed BA networks and find out how the malfunction and the attack influences the target controllability of a complex network.

Therefore, we measure the number of the driver nodes n_d that satisfies the target control for the network at different fraction of the broken nodes in the whole network. We compare each n_d with n_{d0}, which presents the number of the driver nodes before the network is attacked or broken, as $\Delta n_d = n_{d0} - n_d$. The value of Δn_d shows the changes of the target controllability in the broken network. The larger Δn_d is, the lower the target controllability is. And for each test we generate a network with 200 nodes and randomly select 20% of the nodes, which equals 40, as the target nodes, then run the test for several times and calculate the average value.

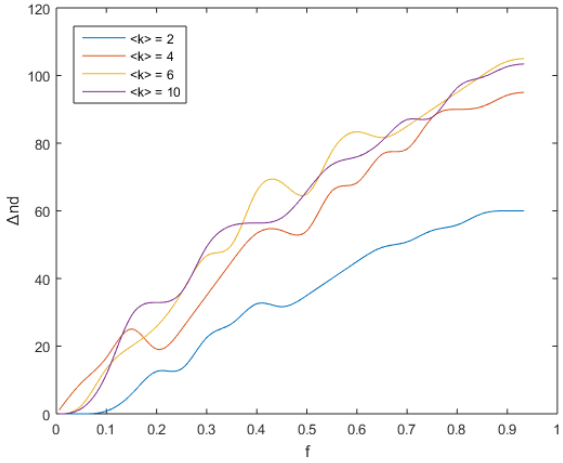

Fig 4. Random Node Failure in ER Networks.

3.1 Random Node Failure

In this part, we study the target controllability of the network when some of the nodes in the network malfunction. At each step, we randomly choose some of the nodes in the network and remove the edges of these nodes, and then we use the GA to obtain the number of the driver nodes.

Obviously as the fraction f of the failed nodes increases, the target controllability will reduce. As shows in *Fig. 1* and *Fig. 2*, for both BA and ER networks, the target controllability reduces smoothly. And when we remove over 80 percent of nodes in the network, the value of Δn_d reaches a limit, because too many failed nodes have broken the network into pieces and we have to directly control the target nodes. For the situation of the average degree <k> = 2 in both networks, the Δn_d is smaller than the other situations. This is because the connection is sparser in this situation than other situations of <k> more than 2 and the initial n_{d0} is bigger than the other situations.

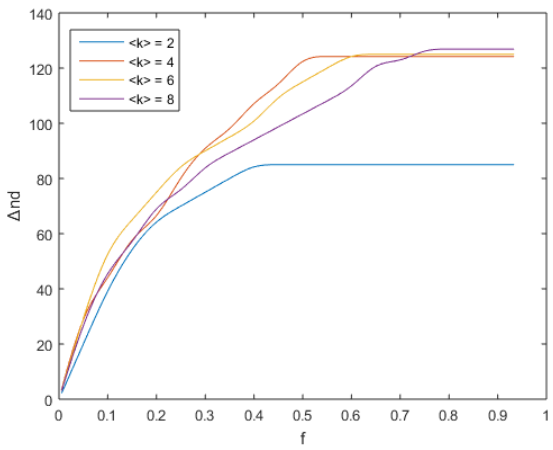

Fig 5. Degree-based Attack in BA Networks.

3.2 Degree-based Attack

In this part, we investigate the target controllability of the network under attacks, here we studied the degree-based attack. In the degree-based attack, at each step we attack the nodes with the largest degree, remove the edges connected to them and calculate the number of the driver nodes.

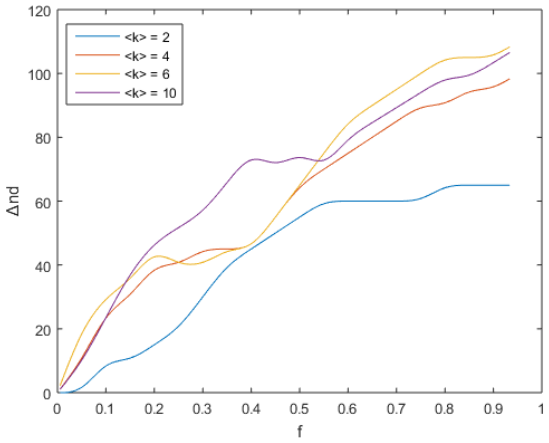

Fig 6. Degree-based Attack in ER Networks.

As shows in the *Fig. 3*, the degree-based attack has obvious influence on BA networks. When the fraction f is smaller than 0.1, the target controllability reduces fast, and the speed of the target controllability reduction slows down as the fraction f getting larger, and finally reach the limit value, which approximatively equals $n_{d0} + n_t$, which is the number of the target nodes. As the value of average degree <k> increasing, it reaches the limit value at a larger f. However, for the EA networks in *Fig. 4*, the reduction of the target controllability is similar as the random node failure strategy.

EA network is a stochastic network. The distribution of its node degree satisfies Poisson distribution, so the EA network has high homogeneity, which means that all the nodes have a relatively same influence on the network characteristics. As the degree of the nodes in an EA network can be considered as the same, so the random node failure and the degree-based attack have a similar influence on the target controllability. However, BA network is a scale-free network, the distribution of its node degree satisfies power-law distribution, which means BA network has a strong heterogeneity. Most of the nodes in BA networks have a small degree while a few nodes have higher degrees and become the cores of the whole network. The degree-based attack directly remove the core nodes in the network, and leads to a stronger change of the network structure than EA network thereby affecting the target controllability of the network and the value Δn_d reaches a limit earlier.

4. Conclusion

In this paper, we study the influence on the target controllability when the directed EA and BA network meets random node failure and the degree-based attack. Obviously, the broken nodes and edges will reduce the target controllability, and degree-based attack is more efficient in directed BA networks. However, there still plenty of research should be done. We only study the target controllability of the linear network systems based on the structural control theory, actually a real complex network is much more complex. The difficulty is not just how to describe a real network, the malfunctions and attacks are also complex and indefinite, even the broken of one node may cause a cascading failure in the network and finally break down the whole network.

In the future, we will further study on the influence of the cascading failure on the target controllability, and try to develop effective method to improve the robustness of the network target controllability.

Acknowledgments

This work was supported by State Key Laboratory of Smart Grid Protection and Control in China, the Key R&D Program of Jiangsu Province industry prospect and common key technologies (No.BE2015022), the Funded Project of Satellite Communication and Navigation Collaborative Innovation Center of Jiangsu Province (No. SatCN-201410, No. SatCN-201407).

References

[1]. H. J. van Waarde, M. K. Camlibel and H. L. Trentelman, "A Distance-Based Approach to Strong Target Control of Dynamical Networks," in IEEE Transactions on Automatic Control, vol. PP, no. 99, pp. 1-1.

[2]. Gao J, Liu Y Y, Dsouza R M, et al. Target control of complex networks[J]. Nature Communications, 2014, 5:5415.

[3]. Galbiati, Marco, Delpini, et al. The power to control[J]. Nature Physics, 2013, 9(3):126-128.

[4]. Baldea M, Daoutidis P. Model reduction and control of reactor–heat exchanger networks[J]. Journal of Process Control, 2006, 16(3):265-274.

[5]. Kuchtey J, Fulton S A, Reba S M, et al. Interferon-alphabeta mediates partial control of early pulmonary Mycobacterium bovis bacillus Calmette-Guerin infection.[J]. Immunology, 2006, 118(1):39-49.

[6]. Cohen R, Havlin S, Benavraham D. Efficient Immunization Strategies for Computer Networks and Populations[J]. Physical Review Letters, 2003, 91(24):247901.

[7]. Pu C L, Pei W J, Michaelson A. Robustness analysis of network controllability[J]. Physica A: Statistical Mechanics and its Applications, 2012, 391(18): 4420-4425.

[8]. Wang H, Huang J, Xu X, et al. Robustness of Complex Networks against Attacks Guided by Damage[J]. arXiv preprint arXiv:1105.0275, 2011.

[9]. Motter A E. Cascade control and defense in complex networks[J]. Physical Review Letters, 2004, 93(9):098701.

[10]. Boyd S, El Ghaoui L, Feron E, et al. Linear matrix inequalities in system and control theory[M]. Society for industrial and applied mathematics, 1994.

[11]. Lin C T. Structural controllability[J]. IEEE Transactions on Automatic Control, 1974, 19 (3): 201-208.