ISSN 1749-3889 (print), 1749-3897 (online)
International Journal of Nonlinear Science
Vol.33(2022) No.2/3,pp.83-88

Percolation Behavior of Barabsi-Albert Network under Intentional Attack with Limited Information

Yanting Luo[1], Ting Qing[1], Fan Wang[1,2], Gaogao Dong[1*]
[1]School of Mathematical Sciences, Jiangsu University, Zhenjiang, Jiangsu 212013, P. R. China
[2]Department of Physics, Bar-Ilan University, Ramat-Gan 52900, Israel
(Received March 1 2022, accepted May 19 2022)

Abstract: Due to the wide application of the Barabsi-Albert network in real systems, its robustness research has been widely concerned by researchers. However, it is difficult to obtain the information of all nodes in the actual network, and only limited information is obtained. Inspired by this, the robustness of a single Barabsi-Albert network and two Barabsi-Albert interdependent networks under intentional attack with limited information is studied in this paper, where limited information refers to the information of only n nodes is known, where the limited information means that only n nodes' information is known. For a single Barabsi-Albert network, we analyze the effect of n on the robustness of the network. The findings show that when the known information amount does not exceed 15, the larger n is, the more vulnerable the Barabsi-Albert network is. When n is greater than 15, there is no substantial impact on the robustness of the system. For two interdependent Barabsi-Albert network networks, the effects of coupling strength q and the known information quantity n on the percolation behavior are investigated separately. When q is small, the system is extremely unstable under intentional attack with limited information. For the influence of the known information quantity n on the robustness of interdependent Barabsi-Albert networks, the results are similar to the case of a single Barabsi-Albert network. The proposed sheds light on the resilience of Barabsi-Albert network under intentional attack with limited information and provides helpful insights into designing a robust real-world system.

Keywords: Barabsi-Albert network; Percolation behavior; Network resilience; Intentional attack

1 Introduction

With the rapid development of information technology, complex networks have more and more extensive applications in the real world [1–8]. For modeling the World Wide Web and other systems, the researchers found that the degree distribution of complex networks generally follows power-law distribution, and thus proposed the Barabsi-Albert (BA) model was proposed [9]. Besides, the Barabsi-Albert model can also generate scale-free graphs with degree indices of the real graph [10]. As an algorithm for generating scale-free networks, the Barabsi-Albert model has great advantages in explaining the formation of social networks due to its growth and priority connection mechanism [11]. Based on this, the Barabsi-Albert network model has been successfully applied to many real-world fields and systems, such as biology [12], sociology [13], transportation [14], etc. [15–21].

When the system is under different attack strategies, the edges are disconnected, and the system exhibits different robustness. When the interdependent Barabsi-Albert networks, suffer an initial attack, the interdependence causes cascading failures of nodes, which leads to more failures of nodes, and even the collapse of the entire system [22]. The robustness of a single Barabsi-Albert network and two interdependent Barabsi-Albert networks has been the focus of researchers [23, 24]. Crucitti et al. found that at variance with random graphs, Barabsi-Albert network displays, both on a global and a local scale, a high degree of error tolerance and an extreme vulnerability to attacks [25]. The existing robustness research of robustness of the Barabsi-Albert network mainly discusses two types of attack strategies, including random attack [26] and targeted [27]. For the random attack strategy, it is not necessary to obtain the information of the node; while the targeted attack is a strategy based on the global information of the node. However, in actual systems, especially

*Corresponding author. *E-mail address*: gago999@126.com

large-scale interdependent networks, it is difficult for people to obtain the topology information of all nodes in the network, but only a part of them. Therefore, the researchers proposed an immune strategy that only considered the limited information in the network. It is found that only a small number of nodes in the network can be selected to achieve an epidemic prevention effect similar to the classic targeted immunity [28].

Random and targeted attack strategies do not represent the types of attack strategies experienced by actual systems. Inspired by this, we investigate the structural robustness of a single Barabsi-Albert network and two interdependent Barabsi-Albert networks from numerical simulation. When a single Barabsi-Albert network suffers from intentional attack with limited information, the influence of different information indicators on the robustness of the system is studied. And for the case of two interdependent Barabsi-Albert networks, the effects of different coupling strengths and information indicators on the robustness of the system are studied.

2 Model and results

Here, we study the robustness of a single Barabsi-Albert network and two one-to-one interdependent Barabsi-Albert networks under intentional attacks with limited information. When the system is under intentional attack with limited information, here we consider selecting the node with the largest degree from a randomly selected set of n nodes. Figure 1 shows a method of intentional attack with limited information. This process will be repeated until the nodes in the scale of $1-p$ is selected and removed.

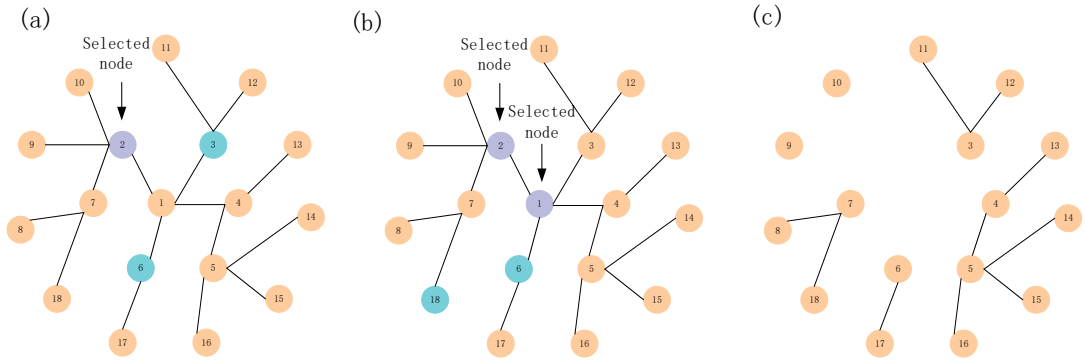

Figure 1: Schematic diagram of intentional attack with limited information. This shows the process of selecting and deleting nodes in a single network under the intentional attack of limited information. In this figure, we set $p=\frac{8}{9}$, $n=3$, that is, every time we select a node, we only know the degree information of three nodes randomly. (a) Select a node for the first time. Only knowing the degree of nodes 2, 3, and 6 will select the node with the largest degree. Given this limited information, node 2 was selected. (b) Select the node for the second time. According to the same mechanism, select node 1. (c) Select node 1 and node 2 to attack according to the degree value of nodes and then remove these nodes from the network.

For the two interdependent Barabsi-Albert networks, $1-p$ fraction of nodes in the *sub-network* A are initially attacked. Because of the interdependence, the failure spread throughout the whole system, and the system cascading failure occurred. The functional nodes in the system satisfy the following conditions: (i) belonging to its giant component of the network itself, (ii) the nodes in each sub-network do not depend on the failing nodes of other sub-networks. The cascade failure process of the interdependent network is shown in Figure 2. After the cascading failure, we study the robustness of the network by calculating the size of the giant component of the sub-networks.

2.1 Single Barabsi-Albert network

We assume that a single Barabsi-Albert network undergoes an intentional attack with limited information. After the initial attack, the functional nodes in the system are nodes belonging to its giant component. We study its robustness by calculating the size of the giant component of the system.

Figure 3(a) gives the simulation results for the single Barabsi-Albert network. As the increase of n, the network is more likely to crash. Presumably, nodes with a relatively large degree of values have a great influence on the connectivity

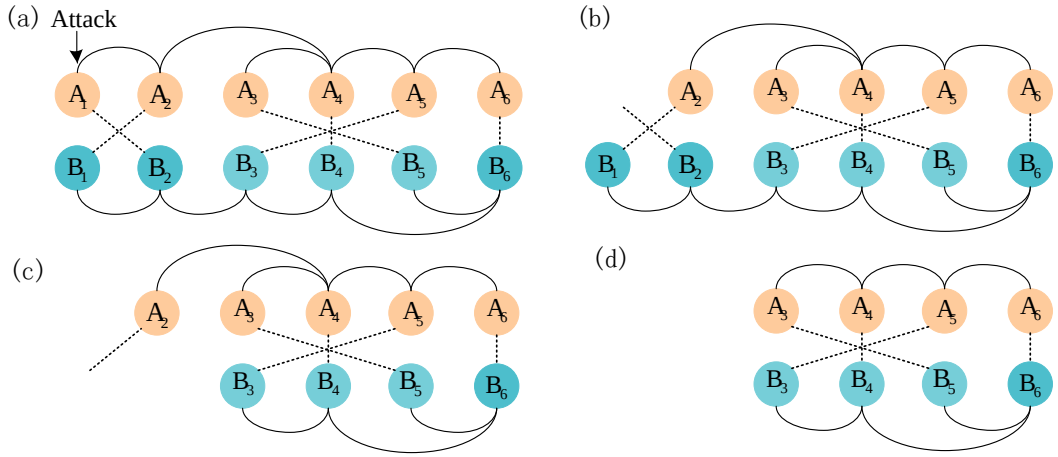

Figure 2: Schematic illustration of the cascade process of the coupled *sub-network* A and *sub-network* B with small sizes $N_A = N_B = 6$. The curve and dash lines describe connectivity links within both sub-networks and support links between sub-networks, respectively. The support-dependence relationship between nodes in *sub-network* A and *sub-network* B is random. At the initial stage, nodes A_1 are initially attacked (black arrows) and become nonfunctional, as shown in (a). In the first stage of sub-network A only functional nodes A_2, A_3, A_4, A_5, and A_6, which belong to the giant component of sub-network A and are supported by at least an effective support link, are preserved (b). In the first stage of sub-network B, only nodes B_3, B_4, B_5, and B_6 subject to the condition of being functional nodes, are kept (c). In (d), the corresponding links attaching fail nodes are removed, then only node A_2 fails because of lacking a support link. Furthermore, no more nodes fail in the cascade of failures, and the system reaches a stable state after this step.

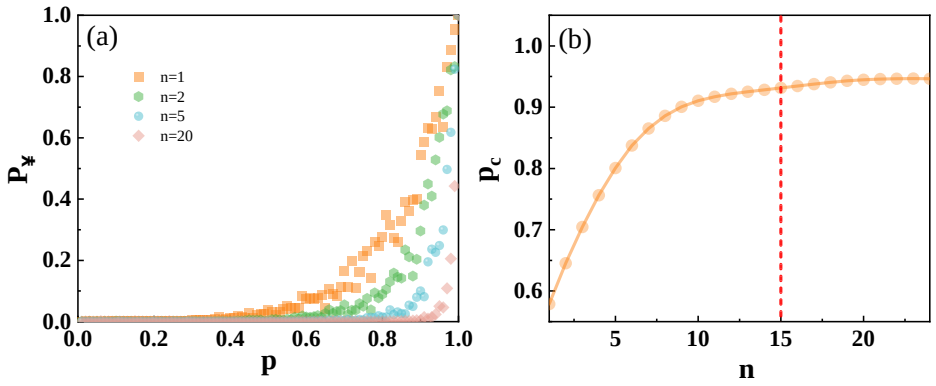

Figure 3: A single Barabsi-Albert network under intentional attack with limited information. (a) P_∞ as a function of p for different n. (b) The critical threshold p_c as a function of n. Simulation results are the averaged data over 100 independent realizations with $N = 10^5$.

of the network. Figure 3(b) once again emphasizes the importance of the group size of n. When the known amount of information does not exceed 15, the more the n is, the more fragile the Barabsi-Albert network is. When n is greater than 15, it has no substantial influence on the stability of the system. If we want to weaken the connection of the Barabsi-Albert network, we don't need to know too much information, only the degree of 15 nodes in each group is enough. This means that when n is greater than 15, the connectivity of the system can easily be completely interrupted.

2.2 Two interdependent Barabsi-Albert networks

We suppose that Barabsi-Albert *sub-network* A and *sub-network* B are partially interdependent, where $q_{AB} = q_{BA} = q$ is the proportion of interdependent nodes between *sub-network* A and *sub-network* B.

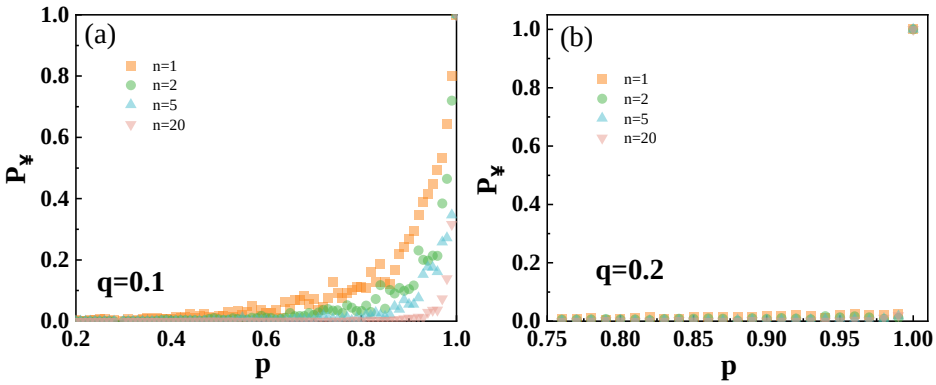

Figure 4: Two interdependent Barabsi-Albert networks under intentional attack with limited information. P_∞ as a function of p for different n with $q = 0.1$ (a), $q = 0.2$ (b). Simulation results are the averaged data over 100 independent realizations with $N_A = N_B = N = 10^5$.

The simulation results are shown in Figure 4. Figure4 (a-b) shows the relationship between the giant component P_∞ and attacking strength p under different coupling strengths q. Moreover, with the increase of coupling strength q, the system has experienced a second-order phase change to a first-order phase change. In a word, different q leads to different phase transition behaviors. To further study its regularity, we study the relationship between p_c and q, as shown in Figure 5(a). When $q \geq 0.2$, the system will crash, while n has little effect on the robustness of the system. The weak coupling strength also makes the system more vulnerable to attack and difficult to protect.

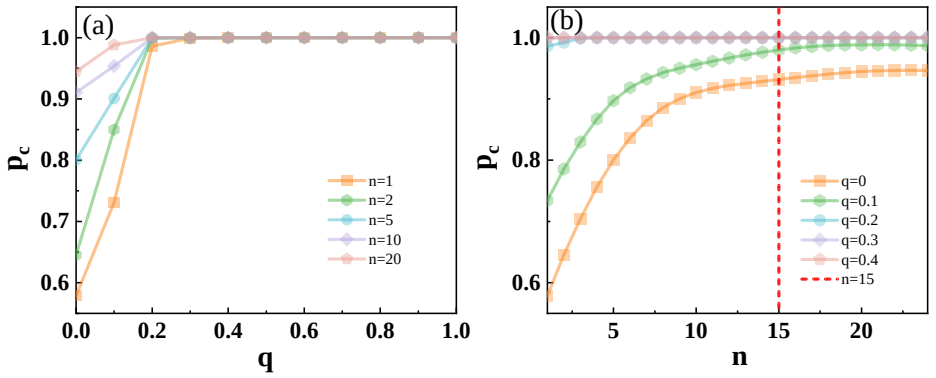

Figure 5: Two interdependent Barabsi-Albert networks under intentional attack with limited information. (a) p_c as a function of q for different n. (b) p_c as a function of n for different q. Simulation results are the averaged data over 100 independent realizations with $N_A = N_B = N = 10^5$.

In addition, Figure 4(a-b) shows that the larger n, the faster the system instinctively crashes. To further explore the impact of the attack on the system, Figure 5(b) graphically shows the functional relationship between the critical point p_c and n for *sub-network* A. The figure shows that when $q < 0.2$, different n has a significant impact on the robustness of the system, but when $q \geq 0.2$, the system almost crashes. At the same time, with the increase of n, the influence of n on

the robustness of the system is gradually weakened. In addition, Figure 5(b) indicates that when the group size n reaches about 15, the robustness of the system is almost unchanged even if more information of nodes can be known. When n is more than 15, the robustness of the system under this attack strategy is very similar to that under the classical directed attack [29].

3 Conclusions

In this paper, we investigate the robustness of Barabsi-Albert network under intentional attack with limited information, which is different from the previous attack strategy. It is of great practical significance to study the attack strategies with limited information of nodes. For a single Barabsi-Albert network and two interdependent Barabsi-Albert networks, when they are attacked by intentional attacks with limited information, it is found that the larger n is, the system is more vulnerable. However when $n > 15$, the impact on the robustness of the system is not obvious. However, under the same conditions, two interdependent Barabsi-Albert networks are more fragile than a single BA network. Overall, the results reveal that when n reaches a critical value, p_c does not increase with n. The findings of this work can help to better understand real-world complex systems, design resilient infrastructure and propose effective risk prevention strategies.

Acknowledgments

This research is supported by grants from the National Natural Science Foundation of China (Grants 61973143, 71690242, 71974080, and 11731014), the National Key R&D Program of China under Grant 2020YFA0608601, Young backbone teachers of Jiangsu Province and Jiangsu Postgraduate Research and Innovation Plan in 2021 (Grant No. KYCX21_3371).

References

[1] L. Chen, K. Hattaf and J. Sun. Optimal control of a delayed slbs computer virus model. *Physica A: Statistical Mechanics and its Applications*, 427(2015):244–250.

[2] X. Gao et al. Detecting method for crude oil price fluctuation mechanism under different periodic time series. *Applied energy*, 192(2017):201–212.

[3] R. Du et al. Identifying the peak point of systemic risk in international crude oil importing trade. *Energy*, 176(2019):281–291.

[4] R. Du et al. A complex network perspective on interrelations and evolution features of international oil trade, 2002–2013. *Applied Energy*, 196(2017):142–151.

[5] X. Sun et al. Energy implications of china's regional development: new insights from multi-regional input-output analysis. *Applied energy*, 196(2017):118–131.

[6] M. Jiang et al. Factors driving global carbon emissions: A complex network perspective. *Resources, Conservation and Recycling*, 146(2019):431–440.

[7] J. Fan et al. Network analysis reveals strongly localized impacts of el niño. *Proceedings of the National Academy of Sciences*, 114(2017)(29):7543–7548.

[8] J. Meng et al. Percolation framework to describe el niño conditions. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 27(2017)(3):035807.

[9] A.-L. Barabási and R. Albert. Emergence of scaling in random networks. *science*, 286(1999)(5439):509–512.

[10] H. Park and M.-S. Kim. Lineageba: A fast, exact and scalable graph generation for the barabási-albert model. In 2021 IEEE 37th International Conference on Data Engineering (ICDE), 540–551. IEEE. 2021.

[11] P. ZHOU et al. Simulation of online learning interaction relation network based on ba model.

[12] M. Alizadeh, C. Cioffi-Revilla and A. Crooks. Generating and analyzing spatial social networks. *Computational and Mathematical Organization Theory*, 23(2017)(3):362–390.

[13] T. F. Alves et al. The diffusive epidemic process on barabasi–albert networks. *Journal of Statistical Mechanics: Theory and Experiment*, 2021(2021)(4):043203.

[14] D. P. Chassin and C. Posse. Evaluating north american electric grid reliability using the barabási–albert network model. *Physica A: Statistical Mechanics and its Applications*, 355(2005)(2-4):667–677.

[15] G. Bianconi. Mean field solution of the ising model on a barabási–albert network. *Physics Letters A*, 303(2002)(2-3):166–168.

[16] S. V. Buldyrev et al. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(2010)(7291):1025–1028.

[17] M. A. Sumour and M. M. Shabat. Monte carlo simulation of ising model on directed barabasi–albert network. *International Journal of Modern Physics C*, 16(2005)(04):585–589.

[18] T. F. Móri. The maximum degree of the barabási–albert random tree. *Combinatorics, Probability and Computing*, 14(2005)(3):339–348.

[19] A. Fronczak et al. Higher order clustering coefficients in barabási–albert networks. *Physica A: Statistical Mechanics and its Applications*, 316(2002)(1-4):688–694.

[20] K. Suchecki and J. A. Hołyst. Ising model on two connected barabasi-albert networks. *Physical Review E*, 74(2006)(1):011122.

[21] J. Gomez-Gardenes and Y. Moreno. Local versus global knowledge in the barabási-albert scale-free network model. *Physical Review E*, 69(2004)(3):037103.

[22] F. Tan, Y. Xia and Z. Wei. Robust-yet-fragile nature of interdependent networks. *Physical Review E*, 91(2015)(5):052809.

[23] N. Dehmamy, A.-L. Barabási and R. Yu. Understanding the representation power of graph neural networks in learning graph topology. *Advances in Neural Information Processing Systems*, 32(2019).

[24] L. Tu et al. The relationship between the topology and synchronizability of partially interdependent networks. *EPL (Europhysics Letters)*, 119(2017)(4):40004.

[25] P. Crucitti et al. Efficiency of scale-free networks: error and attack tolerance. *Physica A: Statistical Mechanics and its Applications*, 320(2003):622–642.

[26] P. Crucitti et al. Error and attack tolerance of complex networks. *Physica A: Statistical mechanics and its applications*, 340(2004)(1-3):388–394.

[27] J. Wang, C. Jiang and J. Qian. Robustness of internet under targeted attack: a cascading failure perspective. *Journal of Network and Computer Applications*, 40(2014):97–104.

[28] Y. Liu et al. Efficient network immunization under limited knowledge. *National Science Review*, 8(2021)(1):nwaa229.

[29] X. Huang et al. Robustness of interdependent networks under targeted attack. *Physical Review E*, 83(2011)(6):065101.