ISSN 1749-3889 (print), 1749-3897 (online)
International Journal of Nonlinear Science
Vol.31(2021) No.1,pp.38-42

Network Overload due to Targeted Attack

Ruijin Du, Jie Li*, Xiaoxia Zheng, Qi Wu, Kaishun Zhang, Guangxu Guo
Center of Energy Development and Environmental Protection, School of Mathematical Sciences, Jiangsu University, Zhenjiang, Jiangsu 212013, P. R. China
(Received 5 January 2021, accepted 10 March 2021)

Abstract: In this paper, the betweenness of nodes is used as the measure of load to study the cascading failure of Erdös-Renyi network caused by overload. Based on the targeted attack strategy, the cascading failure propagation behavior of the network under different control conditions is analyzed. This is of great significance for finding the theoretical solution for the proportion of attacked nodes, which is helpful to restrain the propagation of cascading failures. The fraction of survived nodes at the end of the cascade, p_f, which is a function of the strength of the initial attack, is studied. The first order phase transition line $p_t(\alpha)$ is found, where α is the parameter of attack failure probability. The result shows that the fraction of surviving nodes at the end of the cascade, $p_f(t)$, undergoes a first-order discontinuity at $p_t(h, \alpha)$, where the tolerance parameter h is a global parameter of the system.

Keywords: Betweenness; Cascading failure; Targeted attack; ER network

1 Introduction

In June 2016, a monkey broke into the Kitara hydropower station in Nairobi, the capital of Kenya, and fell onto a transformer. It caused a widespread power outage in Kenya and led to severe economic losses to Kenyans. It is widely believed that the incident was caused by a series of cascading failures in the power grid [1]. This means that the failure of one part of the power network causes overloads in other areas of the system, leading to cascading failures in other parts of the network [2–4]. This process is repeated many times until most nodes in the network collapse or fail [5]. What is more, the network is everywhere in daily life, such as communication networks, power networks, energy networks. Although these various and complex networks are now inseparable from people's lives and work, they are not consistently stable due to a variety of factors. Therefore, studying the failure propagation mechanism due to overload can provide scientific suggestions to effectively protect real networks from cascading failures and avoid significant economic losses.

At present, experts and scholars in various fields have done a lot of research on cascading failures for various networks under different kinds of attacks strategies [6–8]. Network cascading failure models based on overload coefficient, failure probability, or surplus coefficient were proposed to control the influence of cascading failures, thereby significantly increasing the resilience of the network [9–16]. So, some experts and scholars have studied the impact of different targeted attack strategies on various networks based on real network systems, such as dangerous goods transportation networks, store networks, etc [17, 18]. Furthermore, the researchers introduced general methodologies to investigate the robustness of a single network, or interdependent networks under targeted attacks [19–25].

However, few studies focused on the cascading failure and propagation mechanism caused by betweenness overload when the network suffers targeted attack. This work studies the cascading failure of Erdös-Renyi (ER) network due to betweenness overload caused by intentional attack. By investigating the influence of attack failure probability parameter α and tolerance h on the change of the survival network size, it is expected that effective strategies can be found to prevent the occurrence and propagation of overload failure.

*Corresponding author. *E-mail address*: lj2family@126.com

IJNS.2021.03.15

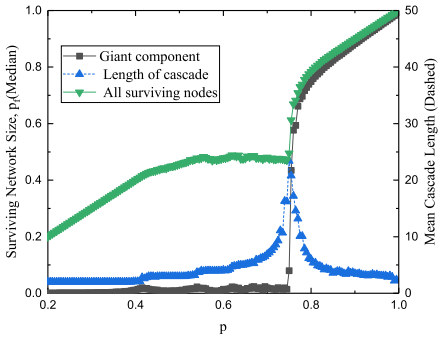

Figure 1: The surviving network size and number of cascades for an Erdös-Renyi network as a function of p for $N = 10000$ nodes. The size of the network drops suddenly at $p_t = 0.761$, when $k = 5, h = 2.5$ and $\alpha = 2.5$.

2 Model and General Results

Targeted attacks usually attack nodes with certain properties, such as nodes with the maximum degree or minimum degree [23, 24]. The probability of attack failure for node k_i is $W_\alpha(k_i)$, where α is the parameter of attack failure probability. The expression is as follows [11, 20, 25]:

$$W_\alpha(k_i) = \frac{k_i^\alpha}{\sum_{i=1}^{n}(k_i^\alpha)}, \alpha \in (-\infty, +\infty). \tag{1}$$

When $\alpha > 0$, nodes with a higher degree are more vulnerable and intentionally attacked. When $\alpha < 0$, nodes with higher degrees are defended so that those nodes have a lower probability to fail. When $\alpha = 0$, $W_0 = \frac{1}{N}$. Each node has the same probability of being attacked [12, 20].

Here the Motter-Lai model [5, 9, 10] is used to explore the effect of targeted attack on ER network due to betweenness overload. The betweenness value reflects the importance of the node in a network system. A network is constructed and b_i^0 is defined as the initial betweenness of nodes i. Here set $B_i = (1 + h)b_i^0$ as the maximum betweenness that a node can withstand, where h , the tolerance parameter, is a global parameter of the system.

The fraction $1 - p$ of nodes in the network is failed due to targeted attacks, and the betweenness of each node in the remaining network will be recalculated. The node is removed if its betweenness is greater than B_i, then recalculate the betweenness of nodes in the remaining network. This process is continued until the nodes in the network no longer fail due to overload, then the number of surviving nodes $p_f(\alpha)$ is finally determined. The network is intact, and most of the surviving nodes belong to a giant component p_∞. The remaining surviving nodes are separated from the giant component p_∞ and will have very low betweenness, because they connect to fewer nodes [5]. Since these nodes do not contribute to the global connectivity of the network, only nodes in the giant component are focused. When $p < p_t$, the giant component p_∞ disappears, but the fraction of survived nodes p_f remains finite. We will study numerically the effects of targeted attack on the network, exploring the parameter values leading to the collapse of the network.

We study the network behavior when the attack size is close to the "threshold attack p_t" [5]. The attacked network will survive when $p > p_t$. On the contrary, the network will collapse. After the initial attack, the betweenness value of the node that ends at the highest betweenness is close to its limit, and the network will fail. At this point, the failure of one node can cause the collapse of the whole system. The attack creates conditions for the cascade, and the cascading failures will not end until the network is collapsed.

This paper mainly studies ER network, $G(n, \rho)$, which is a network with n nodes, and any two nodes are connected independently by probability ρ. Since the network has n nodes, there are at most C_n^2 edges in the network, and the possibility of each connected edge is ρ. Thus the expectations of edges in ER network $G(n, \rho)$ can be calculated as [26]:

$$C_n^2\rho = \frac{2\rho}{n(n-1)}. \tag{2}$$

For typical tolerance $h = 2.5$ and $\alpha = 2.5$, we find that, as a function of the size of the initial attack $(1 - p)$, the network undergoes a first-order phase transition at a value of p denoted as p_t. At this point, even the failure of one

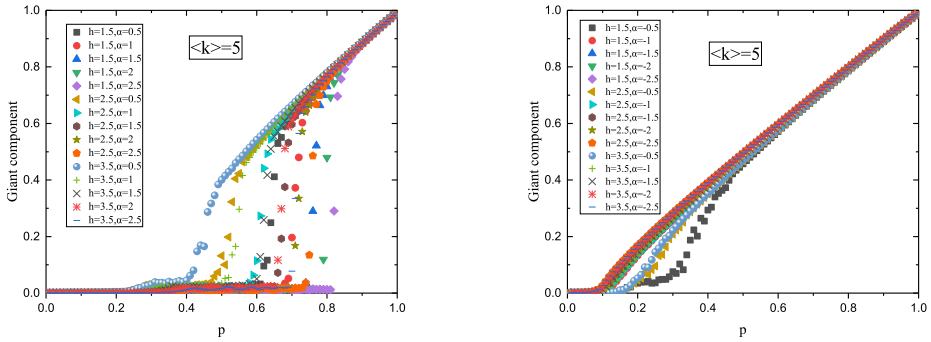

Figure 2: The size of the giant component under targeted attack in Erdös-Renyi network by adjusting the attack probability parameter α and tolerance h.

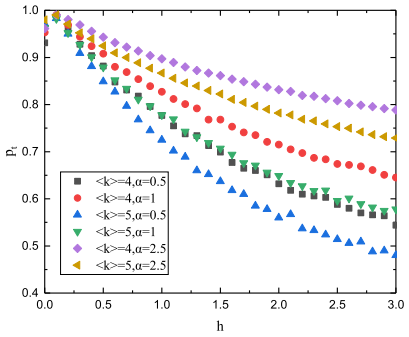

Figure 3: The minimum initial survivability of a catastrophic attack p_t as a function of the tolerance h in Erdös-Renyi network.

additional node can lead to a series of failures that cause the network to be destroyed (Figure 1). The fraction of nodes in the giant component after cascading failure can be found because of the first-order phase transition [5]. Besides, we can find numerical value p_t in the areas of two peaks. They represent the size of the large and small fraction surviving nodes, and they are equal when the first-order transition occurs [19].

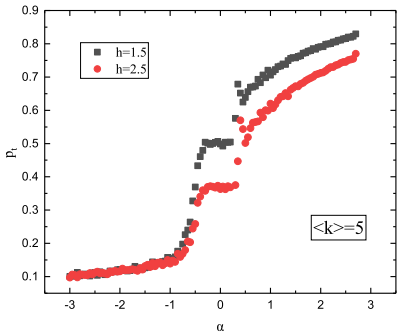

Figure 4: The minimum initial survivability of a catastrophic attack p_t, as a function of tolerance α in Erdös-Renyi network.

The relationship between the size of the threshold initial attack p_t, tolerance h and α of ER network is studied. Fig. 2 shows the data with different values of h and α in the case of ER network. To explore how the size of the initial attack

p_t depends on the values of tolerance h and α well, ER networks with the same total number of nodes and average degree but different h and α are applied for the study. We find that the threshold initial attack p_t decreases as h increases at the same α. The higher the initial attack p_t , the worse the robustness of the network.

In addition, the influence of the increase in tolerance parameter h on the threshold initial attack p_t for networks with different average degrees is investigated. As we expected, as the tolerance h increases, the threshold p_t of the network with the same α but greater average degree decreases, that is, the network becomes more resilient, as shown in Fig.3. Fig.4 demonstrates that as α increases, the threshold initial attack p_t of network with the same average degree and smaller h, becomes larger, that is to say, the system becomes less robust.

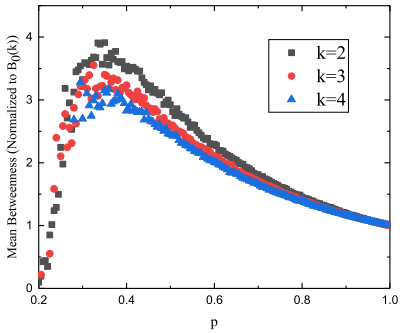

Figure 5: The mean betweenness of nodes as a function of p for Erdös-Renyi network. $B_0(k)$ is the mean betweenness of nodes with degree k.

In ER network, because nodes have different degrees, and initial loads, they also have different maximum loads. For nodes with low initial degrees, their betweenness values are small, thus the maximum load is relatively low. As shown in Fig. 5, the initial attack cause the ratio of low-degree nodes to increase more than the high-degree nodes. Therefore, in the initial stage of the cascade process, the low-degree nodes fail first, and then cause the network to fragment further.

3 Conclusion

We have studied the effect of targeted attack on ER network due to betweenness overload. h and α play important roles in controlling the propagation of Erdös-Renyi network cascading. When other conditions remain unchanged, the greater the tolerance h, the less likely the cascading failure will occur; on the contrary, the greater the possibility of failure. If other conditions are stable, an increase of α will make the system more vulnerable.

The degree of the node is the main factor that determines its betweenness and overload risk. This shows the vulnerability of nodes with more neighbors and nodes with lower initial degrees in ER network. The result gives us a better understanding of the critical point of the phase transition from the first order to second order, as well as the influence of network degree, degree distribution, network size, and tolerance parameters on network stability. The initial degree k, attack failure probability α and tolerance h can be adjusted to control the cascading failure spread of ER network to avoid collapse.

Acknowledgments

This research is supported by grants from the National Natural Science Foundation of China (Grant Nos. 71974080, 61973143, 71690242 and 11731014), the National Key Research and Development Program of China (Grant No. 2020YFA0608601) and Student Research Project of Jiangsu University (Grant No. 19A279).

References

[1] Albert R., Albert I., Nakarado G. L.. Structural vulnerability of the North American power grid. Physical Review E. 2004, 69(2):025103.

[2] Dong G., Xiao H., Wang F., Du R., Shao S., Tian L., Stanley H. E., Havlin S.. Localized attack on networks with clustering. New Journal of Physics. 2019, 21(1).

[3] Dong G., Gao J., Du R., Tian L., Stanley H. E., Havlin S.. Robustness of network of networks under targeted attack. Physical Review E: Statistical. 2013.

[4] Dong G., Gao J., Tian L., Du R., He Y.. Percolation of partially interdependent networks under targeted attack. Physical Review E. 2011.

[5] Kornbluth Y., Barach G., Tuchman Y., Kadish B., Cwilich G., Buldyrev S. V.. Network overload due to massive attacks. Physical Review E. 2018, 97(5):052309.

[6] Zhao L., Park K., Lai Y.. Attack vulnerability of scale-free networks due to cascading breakdown. Physical Review E Statal Nonlinear & Soft Matter Physics. 2004, 70(3):035101.

[7] Gallos L. K., Cohen R., Argyrakis P., Bunde A., Havlin S.. Stability and topology of scale-free networks under attack and defense strategies. Physical Review Letters. 2005, 94(18):188701.

[8] Shao S., Huang X., Stanley H. E., Havlin S.. Percolation of localized attack on complex networks. New Journal of Physics. 2015, 17(2):1-11.

[9] Motter A. E., Lai Y.. Cascade-based attacks on complex networks. Physical Review E Statal Nonlinear & Soft Matter Physics. 2002, 66(6):065102.

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

[11] Gallos L. K., Cohen R., Liljeros F., Argyrakis P., Bunde A., Havlin S.. Attack strategies on complex networks. Lecture Notes in Computer Science. 2006, 3993:1048-1055.

[12] Buldyrev S. V., Parshani R., Paul G., Stanley H. E., Havlin S.. Catastrophic cascade of failures in interdependent networks. Nature. 2010, 464(7291):1025-8.

[13] Crucitti P., Latora V., Marchiori M.. Model for cascading failures in complex networks. Physical Review E Statal Nonlinear & Soft Matter Physics. 2003, 69(4 Pt 2):045104.

[14] Li W., Cui X., Deng S., Xiao W.. Cascade of failures in interdependent networks under targeted attack and defense of interdependent links. Computer Engineering and Applications. 2014.

[15] Chen Z., Du W., Cao X., Zhou X.. Cascading failure of interdependent networks with different coupling preference under targeted attack. Chaos Solitons & Fractals the Interdiplinary Journal of Nonlinear ence & Nonequilibrium & Complex Phenomena. 2015, 80:7-12.

[16] Cheng Z., Cao J., Hayat T.. Cascade of failures in interdependent networks with different average degree. International Journal of Modern Physics C. 2014, 25(05):167.

[17] Zhang P., Cheng B., Zhao Z., Li D., Lu G., Wang Y., Xiao J.. The resilience of interdependent transportation networks under targeted attack. EUROPHYS LETT. 2013.

[18] Zhang P., Cheng B., Zhao Z., Li D., Lu G., Wang Y., Xiao J.. The robustness of interdependent transportation networks under targeted attack. EUROPHYS LETT. 2013.

[19] Lowinger S., Cwilich G. A., Buldyrev S. V.. Interdependent lattice networks in high dimensions. Physical Review E. 2016, 94(5):052306.

[20] Huang X., Gao J., Buldyrev S. V., Havlin S., Stanley H. E.. Robustness of interdependent networks under targeted attack. Physical Review E Statal Nonlinear & Soft Matter Physics. 2011, 83(6):065101.

[21] Ricard V. S., Marti R. C., Bernat C. M., Sergi V.. Robustness of the European power grids under intentional attack. Physical Review E Statal Nonlinear & Soft Matter Physics. 2007, 77.

[22] Albert R., Jeong H., Barabsi A.. Error and attack tolerance of complex networks. Nature. 2000.

[23] Callaway D. S., Newman M. E. J.. Network robustness and fragility: percolation on random graphs. Physical Review Letters. 2000, 85(25):5468.

[24] Vespignani A.. Complex networks: the fragility of interdependency. Nature. 2010.

[25] Yuan X., Dai Y., Stanley H. E., Havlin S.. K-core percolation on complex networks: comparing random, localized and targeted attacks. Physical Review E. 2016, 93(6):062302.

[26] Leskovec J., Kleinberg J. M., Stanley H. E., Faloutsos C.. Graphs over time: densification laws, shrinking diameters and possible explanations. Eleventh ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2005.