Cascades Tolerance of Scale-Free Networks with Attack Cost

Chen Hong [1] **, Nai-Yu Yin** [2] **, Ning He** [1] **, Oriol Lordan** [3] *, **Jose Maria Sallan** [3]

[1] *College of Information Technology, Beijing Union University,*
Beijing 100101, P.R.China
[2] *School of Electronic and Information Engineering, Beihang University,*
Beijing 100191, P.R.China
[3] *Universitat Politècnica de Catalunya-BarcelonaTech, Colom 11,*
Terrassa 08222, Spain
E-mail: oriol.lordan@upc.edu

Received 10 April 2017

Accepted 30 August 2017

Abstract

Network robustness against cascades is a major topic in the fields of complex networks. In this paper, we propose an attack-cost-based cascading failure model, where the attack cost of nodes is positively related to its degree. We compare four attacking strategies: the random removal strategy (RRS), the low-degree removal strategy (LDRS), the high-degree removal strategy (HDRS) and the genetic algorithm removal strategy (GARS). It is shown that the network robustness against cascades is heavily affected by attack costs and the network exhibits the weakest robustness under GARS. We also explore the relationship between the network robustness and tolerance parameter under these attacking strategies. The simulation results indicate that the critical value of tolerance parameter under GARS is greatly larger than that of other attacking strategies. Our work can supply insight into the robustness and vulnerability of complex networks corresponding to cascading failures.

Keywords: Network robustness, Cascading failures, Genetic algorithm, Attack cost.

1. Introduction

Complex networks have been found to be effective to describe many networked systems in nature and society, such as the Internet, power grids and communication systems, and so on. Over the past few decades, complex network research has made great achievements in many areas [1,2], including network modeling [3,4,5], evolutionary games [6,7], optimization [8], epidemic spreading [9] and traffic dynamics [10,11,12], etc.

Because of the great importance of vulnerability and robustness for many real-world complex networks, the robustness of networks has attracted many researchers in recent years [13,14,15]. In particular, the problem of cascades with load redistribution on networked systems has aroused widespread concern [16,17,18,19]. Some important aspects of cascades have been extensively researched, including the models for describing the cascading failures [20,21,22], the defense and control strategies for cascades [23,24,25,26], the cascading models in real networks [27,28,29]. Motter et al. [20] put forward a global load-based cascading model. The authors shown that, in the case of attack triggered by breaking down a single vital node, the heterogeneity of com-

* Corresponding author: oriol.lordan@upc.edu (O. Lordan).

plex networks can make them extraordinary fragile. Subsequently, by proposing a mechanism of local weighted flow redistribution, Wang and Chen [30] studied the cascade phenomena on weighted networked systems. They found that the strongest robustness level of weighted complex network is accomplished when the link weight equals to k_ik_j, where k_i and k_j are the degrees of the vertexes linked by the edge. Recently, Wang et al. [18] proposed a simple cascade model and investigate cascade phenomena triggered by breaking down the highest-load node in complex networks. They found that the fluctuations of cascading dynamics in networks is abnormal and the resilience of networks against cascades decreases inversely when the node's capacity increases.

However, most previous works of network robustness assume that the attack cost is the same [31,32]. Actually, for many real-world networks, the removal cost of a link or a node may be quite various [33]. In this paper, the factor of attack cost is merged into the cascading failure model and the cost of breaking down a node is related to its degree. The results indicate that the network robustness against cascading failures is heavily affected by the node's attack cost, and the genetic algorithm removal strategy (GARS) displays a better performance than other attacking strategies.

This paper is organized as follows. In the section 2, we describe the attack-cost-based cascading failure model and node attacking strategies specifically. Simulation results and correspondent theoretical analysis are provided in Section 3. Finally, our conclusions are drawn in section 4.

2. The model

2.1. Network model

It is known that many real-world networks display a scale-free property, for example the Internet, WWW and transportation networks [34,35]. In this paper, we use the Barabási-Albert (BA) network [5] to explore the cascades tolerance of scale-free complex networks. The BA network is generated by growth and preferential attachment rules, which can be found in many realistic networks. Starting from m_0 fully linked nodes, at each time step one new node will be added to the BA network model. The new one is preferentially linked to m $(m \leqslant m_0)$ old ones with the probability $\Pi_i = k_i / \sum_j k_j$, where k_i is the degree of node i. In this paper, we will set the parameters of BA networks as $m_0 = m = 2$ and $N = 1000$, where N is the size of the network.

2.2. Attack-cost-based cascading failure model

Previous models of network robustness usually assumed that the attacking cost for any node or link is unified. Actually, due to the heterogeneous practical property of nodes or links, the attack cost of them can be quite different. Following common practices [33], we use the degree of nodes to metric the attacking cost of nodes, i.e., $\rho_i = k_i$, where ρ_i is the cost to remove node i and k_i is the degree of node i. The total attack cost is normalized as:

$$\rho = \frac{\sum_{v \in Z} k_v}{\sum_{j=1}^{N} k_j}, \tag{1}$$

where k_j is the degree of node j, Z is the set of removed nodes and N is the number of nodes in the network. The robustness of networks is measured by the relative size of the largest connected cluster $G = N'/N$, where N is the size of the initial network and N' is the size of the largest connected cluster after cascades. High G values represent robust networks, while low G values correspond to vulnerable networks [20].

Previous works have shown that for BA networks the node's load scales with its degree as [36,37,38]:

$$L_i \sim k_i^{1.6}, \tag{2}$$

where k_i is the degree of node i. Here we set the load of node i as $k_i^{1.6}$. The capacity of node j is the maximum load which can be processed by node j, meaning that node j has a limited power to handle its load [20]:

$$C_j = (1+\alpha)L_j, \tag{3}$$

where α $(\alpha \geqslant 0)$ is a tolerance parameter, and L_j is the load of node j in the original network. Obviously, the tolerance parameter α denotes the power of nodes to process the extra load. The larger the value of α, the higher the security margin to resist the flow perturbations.

Next, we will introduce attacking strategies in detail.

Random removal strategy (RRS):

The procedure of RRS is described as follows. At each time step of the strategy, one node is chosen randomly from the unremoved node set of the network.

Low-degree removal strategy (LDRS):

LDRS is described as follows. At each time step a node with the lowest degree in the initial network is chosen from the unremoved node set of the network. If there are two nodes with the same degree, a node will be selected randomly.

High-degree removal strategy (HDRS):

HDRS is a widely used intentional attacking strategy [32]. Under HDRS, a node with the highest degree in the initial network is selected at each time step from the unremoved node set of the network. If there are two nodes with the same degree, we randomly chose one node.

Genetic algorithm removal strategy (GARS):

It is known that computational intelligence algorithms can effectively solve many complex optimization problems [8,39,40]. Genetic algorithm (GA) is a well-known computational intelligence algorithm [41], which was put forward in 1970s. It simulates the evolution procedure in nature and uses the operators for instance selection, crossover and mutation to achieve the enhancement of the fitness value of solutions in population.

Considering the heterogeneous attack cost of nodes and the advantage of GA algorithm, we propose an attack-cost-based attacking strategy named genetic algorithm removal strategy (GARS). In GARS, the length of each chromosome is N, where N is the number of nodes in the network. A node is denoted by a gene and the state of the node is represented by the value of binary bit corresponded to the gene, where 1 denotes the node is removed from the network while 0 denotes the node is alive. We set the crossover probability $P_c = 0.95$, the population size $n = 30$ and the maximum generation $g_m = 100$. Here, the uniform mutation is used and the mutation probability $P_m = 0.1$.

The basic procedure of GA in GARS is described as follows:

Step 1: Set $t = 1$ and the size of population $n = 30$. To speed up the optimization speed, we generate one solution (chromosome) by HDRS, one solution by LDRS and randomly generate remainder 28 solutions to compose the first generation population, P_1. Evaluating the fitness value of each solution in P_1, where the fitness is defined by the value of G after cascading failures.

Step 2: An offspring population Q_t is created as follows: (i) Using roulette wheel selection rule, we select two solutions x and y from P_t according to their fitness values. (ii) We use a crossover probability P_c to produce offspring. Calculating the ρ value of each new offspring, if the value of ρ beyond the given total cost value, then randomly select one node and recover its connection state, i.e., change the bit value of the node from 1 to 0. Iterating this procedure until the ρ value of the offspring not large than the given total cost value. Afterwards, we add these offspring to Q_t.

Step 3: Every solution $x \in Q_t$ is uniformly mutated with a given mutation rate P_m.

Step 4: Assign a fitness value to each solution $x \in Q_t$ according to the value of G corresponded to each solution.

Step 5: Chose n solutions from Q_t according to their fitness values and duplicate these solutions to P_{t+1}.

Step 6: If the maximum generation is reached, return the solution with the highest fitness value in the final population and terminate the algorithm, else, set $t = t + 1$ and go to Step 2.

In the GARS strategy, the removal nodes are identified by the state of binary bits in the resulting solution of GA.

For above attacking strategies, the removed node set Z is null at the beginning. At each time step a node i is selected by the given attacking strategy and the attacking cost of the node ρ_i is summed to ρ, i.e., $\rho = \rho + \rho_i$. If the ρ value is less than or equal to the given total attacking cost, then node i joins in Z set and node i and its direct links are removed simultaneously, otherwise $\rho = \rho - \rho_i$. The iteration is proceeded until ρ equals to the given total attacking cost or we can not find a suitable node to join in the set of Z.

Afterwards, the cascading failure is generated by removing the node u with the highest load in the remained largest connected component. In our model, we adopt the local weighted flow redistribution rule [30], where we tend to allocate more loads to the higher-capacity direct neighbours of failed node to prevent more nodes from overload. Specifically, the loads of the disabled node u, represented by F_u, are distributed to the nearest neighbours of node u. The extra load ΔF_j received by the neighbouring node j is defined as:

$$\Delta F_j = F_u \frac{k_j}{\sum_{l \in \Gamma_u} k_l}, \tag{4}$$

where Γ_u is the neighboring node set of node u. With regard to node j, a nearest neighbour of the failed node u, if $F_j + \Delta F_j > C_j$, then node j and its direct edges are synchronously removed, resulting in reallocation of the load of $F_j + \Delta F_j$ and probably further breaking down remaining vulnerable nodes. The procedure will be continued until there are no more overloaded nodes. At the last step, the value of G in current network will be computed.

3. Simulation results and discussion

Firstly, we study the relationship between G and the total attack cost ρ under different attacking strategies (Fig. 1). It is indicate that the value of G decreases as the value of ρ increases, indicating that the network becomes more vulnerable as the total attack cost increases. On the other hand, the value of G under GARS strategy is the lowest, illustrating that the performance of GARS is better than that of other three attacking strategies. Especially, the value of G drops quickly under GARS when the value of ρ is low, which means that in the initial attack phase the performance of GARS can be significantly improved even if we increase a small quantity of attack costs.

Next, we investigate the relationship between G and α with respect to four attacking strategies (Fig. 2(a)). Here we set the total attack cost $\rho = 0.2$. One can see that under all attacking strategies the value of G increases with the value of α increases, illustrating that the node capacity is of a more safety zone with respect to the node failure as α increases. Furthermore, the value of G under GARS is smaller than that of other strategies, which means that GARS outperforms other attacking strategies.

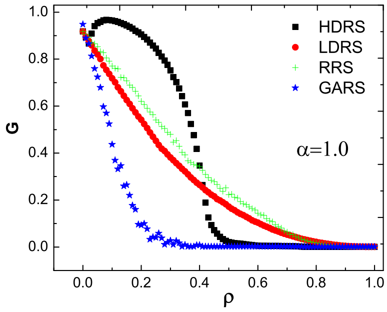

Fig. 1. G as a function of the total attack cost ρ under four attacking strategies. Here we set the parameters of BA network $N = 1000$, $m_0 = m = 2$ and $\alpha = 1.0$. The results are the average over 100 independent realizations.

The critical value α_c is the lowest value of safety capability to prevent networks from global cascades [42,43,44]. When $\alpha < \alpha_c$, the giant cluster disappears, reflecting that the global cascading failure emerges. While in the case of $\alpha > \alpha_c$, the global cascade will not emerge. In the inset of Fig. 2(a), we depict the critical value α_c under four attacking strategies. This shows that the value of α_c with respect to GARS is the highest, showing the weakest network robustness under GARS. To explore the influence of the network size on the critical value α_c, we plot the relationship between G and α under GARS with different network sizes (Fig. 2(b)). This indicates that the value of α_c decreases as the network size increases, reflecting that under GARS the network robustness increases with its size. Due to the fixed maximum generation of GA in GARS, the larger the network size, the harder it is for GARS to find outstanding nodes for attack.

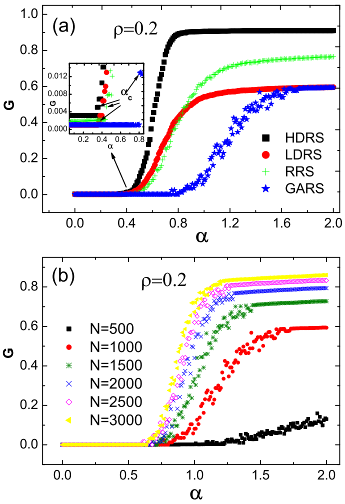

Fig. 2. (a) G as a function of the tolerance parameter α under four attacking strategies. The inset shows the critical value α_c for different attacking strategies, where network size $N = 1000$. (b) G versus the tolerance parameter α under GARS for different network sizes ($N = 500, 1000, 1500, 2000, 2500, 3000$). Here we set $\rho = 0.2$ and BA scale-free networks with $m_0 = m = 2$ are used. The results are the average over 100 independent realizations.

To explore the effect of total attack cost on the performance of GARS, we plot G versus α with respect to GARS for different total attack costs ($\rho = 0, 0.2, 0.4, 0.6, 0.8$). The results illustrate that the robustness of networks decreases as ρ value increases (Fig. 3), indicating that the total attack cost is of a vital effect on the cascades tolerance of complex networks. When $\rho \geqslant 0.6$, the relative size of the largest connected cluster $G \approx 0$, reflecting that the network is completely disintegrated. In the case of $\rho = 0$, the value of $G \approx 1$ when the value of α is high, which means that the network can be well protected even if GARS attacking strategy is used.

Finally, we investigate the relation between G and ρ for different values of tolerance parameter ($\alpha = 0, 0.5, 1.0, 1.5, 2.0$). The results show that the network robustness increases as α value increases, meaning that larger tolerance parameters will make networks more stronger to defend cascades even attack cost is taken into account. Besides, in the case of $\alpha = 0$ and 0.5, the network is quite vulnerable even though the value of ρ is very small ($\rho \leqslant 0.05$).

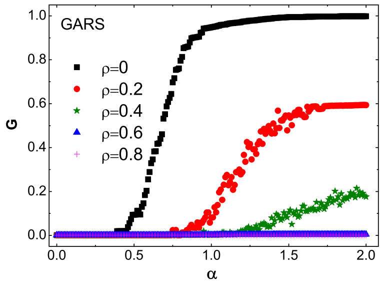

Fig. 3. G as a function of α under GARS for different total node attack costs. BA scale-free networks with $N = 1000$ and $m_0 = m = 2$ are used. The results are the average over 100 independent realizations.

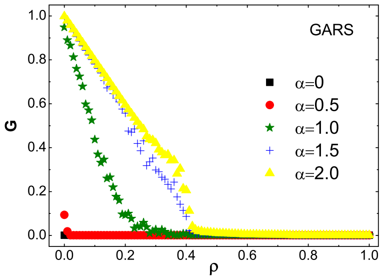

Fig. 4. G as a function of the total attack cost ρ under GARS for different tolerance parameters. Here we set $N = 1000$ and $m_0 = m = 2$. The results are the average over 100 independent realizations.

4. Conclusion

In this paper, we have proposed an attack-cost-based cascading failure model and compared four attacking strategies, where attack costs correspond to the degree of nodes. The results show that attack costs are of important impacts on the cascades tolerance of networks and the genetic algorithm removal strategy (GARS) can make networks more weaker than other three attacking strategies. We investigate the relationship between the network robustness and tolerance parameter when attack costs are taken into account. It is found that the critical value of tolerance parameter under GARS is much larger than that of other strategies and decreases as the network size increases. We also explore the relationship between the network robustness and attack costs under different values of tolerance parameter. The simulation results indicate that, for low values of tolerance parameter, the network is quite fragile even though the value of total attack cost is very small.

Acknowledgments

The work is supported by the National Natural Science Foundation of China (Grant Nos. 61370138, 61572077), Beijing Municipal Natural Science Foundation (Nos. 4152017, 4162027), Characteristic Subject Research Projects of Beijing Union University (KYDE40201701) and New Starting Point Projects of Beijing Union University (Zk10201602).

References

1. M. E. J. Newman, The Structure and Function of Complex Networks, *SIAM Rev.* **45** (2003) 167-256.
2. S. Boccaletti, G. Bianconi, R. Criado, C. I. del Genio, J. Gómez-Gardeñes, M. Romance, I. Sendiña-Nadal, Z. Wang and M. Zanin, The structure and dynamics of multilayer networks, *Physics Repprts* **544** (2014) 1-122.
3. P. Erdös and A. Rényi, On the evolution of random graphs, *Publ. Math. Inst. Hung. Acad. Sci.* **5** (1960) 17-60.
4. D. J. Watts and S. H. Strogatz, Collective dynamics of śmall-worldńetworks, *Nature* **393** (1998) 440-442.
5. A. L. Barabási and R. Albert, Emergence of Scaling in Random Networks, *Science* **286** (1999) 509-512.
6. Z. Wang, A. Szolnoki and M. Perc, Self-organization towards optimally interdependent networks by means of coevolution, *New J. Phys.* **16** (2014) 033041.
7. W.-B. Du, X.-B. Cao, M.-B. Hu and W.-X. Wang, Asymmetric cost in snowdrift game on scale-free networks, *EPL* **87** (2009) 60004.
8. W.-B. Du, Y. Gao, C. Liu, Z. Zheng and Z. Wang, Adequate is better: particle swarm optimization with limited-information, *Appl. Math. Comput.* **268** (2015) 832-838.
9. G. Yan, T. Zhou, J. Wang, Z.-Q. Fu and B.-H. Wang, Epidemic spread in weighted scale-free networks, *Chin. Phys. Lett.* **22** (2005) 510-513.
10. G. Yan, T. Zhou, B. Hu, Z.-Q. Fu and B.-H. Wang, Efficient routing on complex networks, *Phys. Rev. E* **73** (2006) 046108.
11. Y.-X. Xia, N.-J Liu and H. H. C. Iu, Oscillation and chaos in a deterministic traffic network, *Chaos Soliton. Fract.* **42** (2009) 1700-1704.
12. C. Hong, Effective usage of global dynamic information for network traffic, *Physica A* **424** (2015) 242-247.
13. R. Albert, H. Jeong and A.-L. Barabási, Error and attack tolerance of complex networks, *Nature* **406** (2000) 378-382.
14. S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley and S. Havlin, Catastrophic cascade of failures in interdependent networks, *Nature* **464** (2010) 1025-1028.
15. Y.-X. Xia, W.-P. Zhang, X.-J. Zhang, The effect of capacity redundancy disparity on the robustness of interconnected networks, *Physica A* **447** (2016) 561-568.
16. J.-W. Wang, E.-H. Sun, B. Xu, P. Li and C.-Z. Ni, Abnormal cascading failure spreading on complex networks, *Chaos Soliton. Fract.* **91** (2016) 695-701.
17. R.-R. Liu, W.-X. Wang, Y.-C. Lai and B.-H. Wang, Cascading dynamics on random networks: Crossover in phase transition, *Phys. Rev. E* **85** (2012) 026110.
18. J.-W. Wang, L. Cai, B. Xu, P. Li, E.-H. Sun and Z.-G. Zhu, Out of control: Fluctuation of cascading dynamics in networks, *Physica A* **462** (2016) 1231-1243.
19. J.-W. Wang, Mitigation of cascading failures on complex networks, *Nonlinear Dyn.* **70** (2012) 1959-1967.
20. A. E. Motter and Y.-C. Lai, Cascade-based attacks on complex networks, *Phys. Rev. E* **66** (2002) 065102(R).
21. D. J. Watts, A simple model of global cascades on random networks, *Proc. Natl. Acad. Sci. U.S.A.* **99** (2002) 5766-5771.
22. R.-R. Liu, M. Li, C.-X. Jia and B.-H. Wang, Cascading failures in coupled networks with both inner-dependency and inter-dependency links, *Sci. Rep.* **6** (2016) 25294.
23. A. E. Motter, Cascade control and defense in complex networks, *Phys. Rev. Lett.* **93** (2004) 098701.
24. M. Schäfer, J. Scholz and M. Greiner, Proactive robustness control of heterogeneously loaded networks, *Phys. Rev. Lett.* **96** (2006) 108701.
25. H. Zhao and Z.-Y. Gao, Cascade defense via navigation in scale free networks, *Eur. Phys. J. B* **57** (2007) 95-101.
26. J.-W. Wang, Robustness of complex networks with the local protection strategy against cascading failures, *Saf. Sci.* **53** (2013) 219-225.
27. R. Albert, I. Albert and G. L. Nakarado, Structural vulnerability of the North American power grid, *Phys. Rev. E* **69** (2004) 025103.
28. J.-W. Wang and L.-L. Rong, Cascade-based attack vulnerability on the US power grid, *Saf. Sci.* **47** (2009) 1332-1336.
29. J.-W. Wang and L.-L. Rong, Robustness of the western United States power grid under edge attack strategies due to cascading failures, *Saf. Sci.* **49** (2011) 807-812.
30. W.-X. Wang and G.-R. Chen, Universal robustness characteristic of weighted networks against cascading failure, *Phys. Rev. E* **77** (2008) 026101.
31. R. Cohen, K. Erez, D. ben-Avraham and S. Havlin, Resilience of the Internet to Random Breakdowns,

Phys. Rev. Lett. **85** (2000) 4626-4628.

32. P. Holme, B. J. Kim, C. N. Yoon and S. K. Han, Attack vulnerability of complex networks, *Phys. Rev. E* **65** (2002) 056109.
33. B.-J. Zheng, D. Huang, D.-Y. Li, G.-S. Chen and W.-F. Lan, Some scale-free networks could be robust under selective node attacks, *EPL* **94** (2011) 28010.
34. J. Zhang, X.-B. Cao, W.-B. Du and K.-Q. Cai, Evolution of Chinese airport network, *Physica A* **389** (2010) 3922-3931.
35. W.-B. Du, B.-Y. Liang, G. Yan, O. Lordan and X.-B. Cao, Identifying vital edges in Chinese air route network via memetic algorithm, *Chinese Journal of Aeronautics* **30** (2017) 330-336.
36. K.-I. Goh, B. Kahng and D. Kim, Universal behavior of load distribution in scale-free networks, *Phys. Rev. Lett.* **87** (2001) 278701.
37. K.-I. Goh, E. Oh, B. Kahng and D. Kim, Betweenness centrality correlation in social networks, *Phys. Rev. E* **67** (2003) 017101.
38. K. Park, Y.-C. Lai and N. Ye, Characterization of weighted complex networks, *Phys. Rev. E* **70** (2004) 026109.
39. K. De Long, Learning with Genetic Algorithms: An Overview, *Mach. Learn.* **3** (1988) 121-138.
40. A. Konak, D. W. Coit and A. E. Smith, Multi-objective optimization using genetic algorithms: A tutorial, *Reliability Eng. Sys. Saf.* **91** (2006) 992-1007.
41. J. H. Holland, Adaptation in Natural and Artificial System, *Ann Arbor: The University of Michigan Press* (1975).
42. L. Zhao, K. Park and Y.-C. Lai, Attack vulnerability of scale-free networks due to cascading breakdown, *Phys. Rev. E* **70** (2004) 035101(R).
43. L. Zhao, K. Park, Y.-C. Lai and N. Ye, Tolerance of scale-free networks against attack-induced cascades, *Phys. Rev. E* **72** (2005) 025104 (R).
44. Z.-X. Wu, G. Peng, W.-X. Wang, S. Chan and E. W.-M. Wong, Cascading failure spreading on weighted heterogeneous networks, *J. Stat. Mech.* **5** (2008) P05013.