ISSN 1749-3889 (print), 1749-3897 (online)
International Journal of Nonlinear Science
Vol.20(2015) No.3,pp.148-153

Attacking Mode Based on Shell Structure of Complex Networks

Gaogao Dong[1], * Huifang Hao [1], Ruijin Du [1] *, Lixin Tian [1,2]
[1] Nonlinear Scientific for Research Center, Faculty of Science, Jiangsu University, Zhenjiang, Jiangsu 212013, China
[2] School of Mathematical Sciences, Nanjing Normal University, Nanjing 210046, China
(Received 6 January 2014, accepted 2 March 2015)

Abstract: Previous research has focused on two types of initial attack: random attack and hub-targeted attack. However, in real scenarios, some system sometimes suffer from damage based on network shell. In this paper, we propose a kind of attacking model based on shell structure, which means that nodes within network malfunction shell after shell after some node (root node) fails. Additionally, we numerically study the robustness of networks with Possion degree distribution, Regular random network (RR network) and Scale-free network under this attack. We find that the critical shell, where the size of giant component approach zero, is nearly the one of two farthest shell. The result highlight the need to consider shell properties in designing robust networks.

.

Keywords: shell structure, attack, robustness

1 Introduction

In the last decades, the study of complex networks has attracted many researchers from various academic fields, such as aviation networks, electricity networks, social networks, biological networks [1–4]. With the development of technology and rapidly growth of information, scholars study actual cases to analyze the statistical characteristics and the dynamic behaviors of networks by collecting various data from internet, social networks, biological networks, communication networks, electricity networks and other complex systems [5–7]. Networks can be any tangible objects. Complex networks as a model can better understand complex systems. A complex network with non-trivial topological features that often occur in graphs modelling real systems. The study of complex networks is a young and active area of scientific research inspired largely by the empirical study of real-world networks. Recently, we summarize issues about complex networks as follows [1, 8–10]. First issue is the structure of complex networks, it not only theoretically describe the some of common properties in the real topology networks, but also introduce the relevant definitions and notations to guide the constructing of real networks [1]. And, the concepts such as, node degree, degree distributions and correlations (describing the network node characteristics) and shortest path lengths, diameter and betweenness (describing the network edge characteristics) are studied. Additionally, the rest of important notations, like clustering, which is a typical property of acquaintance networks, where two individuals with a common friend are likely to know each other. And the Motif, that is a pattern of interconnections occurring either in in graphs with the same number of nodes, links and degree distribution as the original one, but where the links are distributed at random, also very essential for complex network structure [11–13].

The next issue of complex network is spreading of epidemic and rumors on complex networks [14–16]. Currently, the research on complex network has become mature; and it has permeated various disciplines. The theory research is not only limited to Mathematics but also life discipline and engineering discipline and so on. With the study of complex network, the transmission mechanism has become one of the important branches. Propagation exists widely in nature and human life, such as virus propagation, rumor propagation. While with the closer communication among people, virus outbreak in the network and disease propagation in social network will cause enormous impact on human life and economic. Traditional virus propagation relies mainly on individual contact, including Susceptible-Infected (SI) model, Susceptible-Infected-Susceptible (SIS) model, and Susceptible-Infected-Removed (SIR) model and so on. The third focused issue

*Corresponding author. *E-mail address*: gago999@126.com, dudo999@126.com

IJNS.2015.12.15/888

of complex network by scientist is network synchronization. People studied synchronization on complex networks by applying theories of nonlinear dynamics, statistical physics, matrix analysis and computer calculating method. These researches have great significance for the understanding and practical applications of the synchronization in real networks. The real-world networks, especially the neural networks, are weighted and directed. On the other hand, synchronization results in networks of coupled networks presented should be useful for the understanding of the dynamic processing in many real-world networks [17–19].

As an important branch of complexity theory, complex networks theory attracts more and more scholars from various research. With rapid growth of information technologies, empirical data are getting increasingly rich. Based on the quantitative analysis of big data, theoretical research, algorithm design, practical application, and platform framework etc., the study of complex networks has flourished over the past few years. Previous studies mainly concentrated on the innovation of theory and method of isolated network. However, most real networks are coupled as interdependent networks [20–23]. Therefore, the study has some theoretical and practical significance. In this thesis, according to the coupling characteristics in real networks, we classify the coupling dependency networks into four categories: I) there only exist interdependent links, II) there exist support-dependence links between networks, III) there exist only interconnectivity links, IV) there exist interdependent and interconnect links. When the system are under random attack or targeted attack, we study the robustness of networks with theoretical and simulating analysis, by considering the nodes failure mechanisms of internal network and between two networks. The reliability of complex networks has increasing become an important issue. People make a lot of effort, but still large-scale cascading failures have occurred from time to time. Cascading failure of complex network is defined as one or a few nodes or links failure which will lead other nodes failure through the coupling relations, and it will cause the chain effect and lots of nodes failure, ever the collapse of the whole network, also vividly called ”avalanche”. As human society networking increasing, people become more and more strict with the security and reliability of complex network. Therefore, it is necessary to do research for occurrence mechanism, prevention and control of cascading failure.

Albert et al. numerically studied robustness of the Internet and of a sample of the World Wide Web change when a fraction f of the nodes are removed [4]. This behavior is in contrast with that observed for random graphs, and consistent with that of scale-free graphs. The finding highlights that scale-free networks display a surprisingly high degree of tolerance against random failures. Additionally, Crucitti et al. have used the concept of network efficiency at both global and local scales to study the effects of errors and attacks on BA and on KE structured scale-free networks [6, 7]. Besides numerical simulations, a series of analytical approaches to study tolerance to errors and attacks in complex networks have been proposed. Cohen et al. firstly analytically studied robustness of scale-free networks under randomly and intentional attack by using percolation theory respectively [10]. And, they also firstly analyze under which condition the original graph has a giant component. More recently, Shao et al. developed a percolation framework to analytically and numerically study the robustness of complex networks against such localized attack for networks with any degree distribution [2]. In particular, they investigated this robustness in Erdős-Rényi (ER) networks, random-regular (RR) networks, and scale-free (SF) networks. The results suggested that localized attack has the same effect as random attack on an ER network. An RR network, on the other hand, is always more robust against localized attack compared to random attack. They also support our model by analyzing two real-world networks, and finding that localized attacks are significantly more severe than random attacks. In fact, since interconnections between each two nodes in the network fail when the nodes fail, and others connected through them to the network will also disabled and entire network may collapse. In the real world, the effects of earthquakes, floods, or war attacks on infrastructure networks and the effects of a computer virus or malware on computer networks. This kind of attack focus to a certain point to malicious attack. And then, because of interconnections, the failure start to cause spreading of the disaster and cascading failure occurs at whole network. Inspired by this motivations, we propose the attacking mode based on shell structure of complex networks.

This article is organized as follows: in Section 2, we introduced the attacking mode based on shell structure. The main simulated results for ER, RR and SW networks under the attack are shown in section 3. Finally, this paper is concluded in Section 4.

2 Model description

In this paper, we study a kind of attacking mode based on shell structure of complex network. When some node within network are randomly chosen and fails, its neighbors and their neighbors also fail and until whole network collapse. When the system is attacked by randomly remove one node (root node) of network, Because of the interconnections between each two nodes, the links are removed continually, network breaks and form a topological structure surrounding attacking

hole. We assume that if a node in network is remain functional, it must belong to a sufficiently large mutually connected component. In fact, a large connected component, which includes a finite fraction of the nodes in each network exists only in networks of sufficiently high mean degree. We call that only nodes in the giant component remain functional. While nodes that are parts of the remaining smaller components remain keep functional, there should be a path of connectivity links connecting these small components to the giant component of the other network.

3 Main results

At the beginning, we randomly remove a node as root node, and the fraction p_1 of first shell nodes from network are removed. And remove all the connectivity links that connected to them. Nodes in the second shell within network that connected the first shell nodes, are also removed together with all the connectivity links that connected to them. Analogously, the failure nodes in each shell will lead to further failure of nodes in network, finally resulting in cascading failures. In each step, nodes in one network are functional, either they belong to the giant component of this network, or they are connected to the giant component of other network through interconnected links. As nodes and links are removed recursively, the cascading process emerge. In fact, for network with degree distribution $P(k)$, the generating function and generation function of this branching process are given by $G_0 = \sum_{k=0}^{\infty} P(k)x^k$ and $G_1 = \frac{G_0^{'}(x)}{G_0^{'}(1)}$ respectively [24, 25]. The averaged fraction of lth nodes z_l satisfies a following recursion relation [19]

$$z_l = [G_1^{'}(1)]^{l-1} G_0^{'}(1) = [\frac{z_2}{z_1}]^{l-1} z_1 \tag{1}$$

where $z_1 = G_0^{'}(1)$ and $z_2 = G_0^{'}(1)G_1^{'}(1)$. Assuming s_1 is the fraction of first shell from randomly choosen, the remaining is $1 - s_1$.

We define r_l as the fraction of nodes outside shell l, and r_{inter} and r_{exter} represent the fraction of nodes of inside and outside lth shell and outside fraction of nodes respectively. $r_l = G_1^{l-1}(1 - s_1)$. Let p_l denotes fraction of randomly chosen unprotect nodes within l for randomly selected root node. Thus, the fraction of removing nodes from network is

$$q = \frac{1 + \sum_1^l p_l N_l}{N} \tag{2}$$

where N_l is the number of nodes in shell l.

For the ER network with poisson degree distribution $P_k = \frac{e^{-\widetilde{k}}\widetilde{k}^k}{k!}$, the corresponding generation functions are be written as $G_0 = G_1 = e^{\widetilde{k}(x-1)}$ respectively, where $\widetilde{k}$ is the average degree of network [24, 25]. When ER network under above attack, Fig1(a) shows that the fraction S_1 of giant component within remaining network as a function of r_{exter}. Additionally, We also testify Eq.(1) validity in the subgraph of Fig1(a). From Fig.1(a), we can observe that the size of giant component gradually increases as each shell are removed. And the size of giant component gradually approach zero. Therefore, we define critical threshold l_c as minimum shell, at which the size of giant component become zero when network confront with the attack. Furthermore, we notice that l_c gradually decreases as average degree $\bar{k}$ increases from Fig.1(b). Moreover, the average number L of shell for ER network can be obtained from Eq. (1). And, Fig1(b) also shown that the critical shell is basically belong to two shells of farthest distance from root node. The same results are also found for RR network as shown in Fig. 2. For the SF network with two generation functions are respectively [24–26]

$$\begin{cases} G_0(x) = \sum_m^M [(\frac{m}{k})^{\lambda-1} - (\frac{m}{k+1})^{\lambda-1}]x^k, \\ G_1(x) = \frac{\sum_m^M [(\frac{m}{k})^{\lambda-1} - (\frac{m}{k+1})^{\lambda-1}]kx^{k-1}}{\sum_m^M [(\frac{m}{k})^{\lambda-1} - (\frac{m}{k+1})^{\lambda-1}]k}. \end{cases} \tag{3}$$

Besides the simulation results are agree well with the subgraph of Fig. 1(b), we also notice that l_c gradually increases as λ increases. And l_c is the same with the L, which means that when system undergoes attack based on shell structure, only the farthest shell fail, the giant component just become zero.

4 Conclusions

In summary, we proposed a attacking model based on shell structure of complex networks, which means that the nodes of shell far from root node also fails. Additionally, we also numerically study robustness of complex networks under the

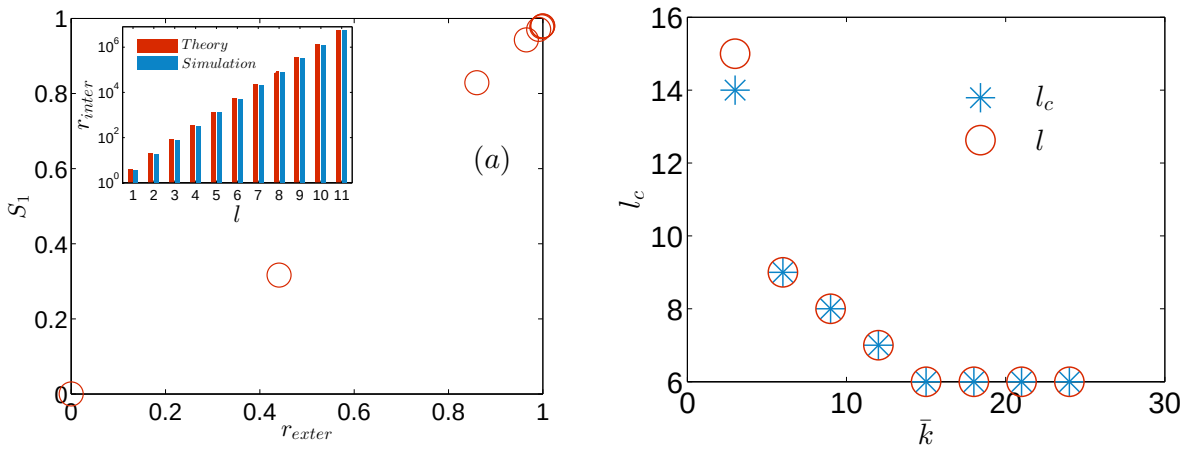

Figure 1: (a) For ER network, the simulations result of the size of the giant component S_1 versus r_{exter} with different parameters for ER network. (a) $\widetilde{k} = 4$, $l = 11$ and the number of nodes the number of nodes $N = 10^7$. Otherwise, comparison between Eq.(1) and simulations of r_{inter} as a function of l are shown in subgraph. (b) The critical shell l_c as a function of $\bar{k}$ with $N = 10^6$, where L denotes the furthest shell from root node. The simulation results are averaged over $N = 10^7$ realizations for (a), the other are 10^3 realizations in the simulations.

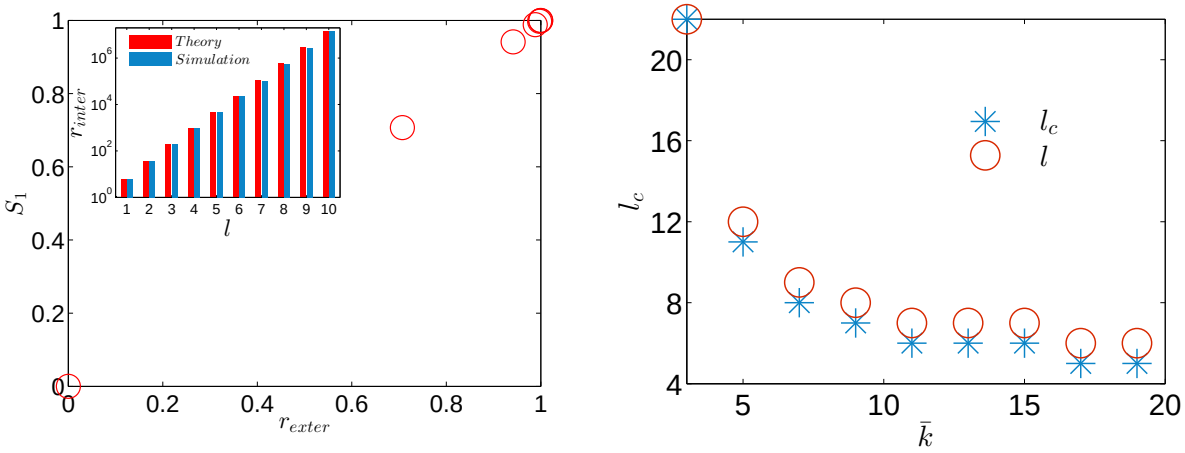

Figure 2: (a) For RR network, the simulations result of the size of the giant component S_1 versus r_{exter} with different parameters for ER network. (a) $\widetilde{k} = 4$, $l = 11$ and the number of nodes the number of nodes $N = 10^7$. Otherwise, comparison between Eq.(1) and simulations of r_{inter} as a function of l are shown in subgraph. (b) The critical shell l_c as a function of $\bar{k}$ with $N = 10^6$, where L denotes the furthest shell from root node. The simulation results are averaged over $N = 10^7$ realizations for (a), the other are 10^3 realizations in the simulations.

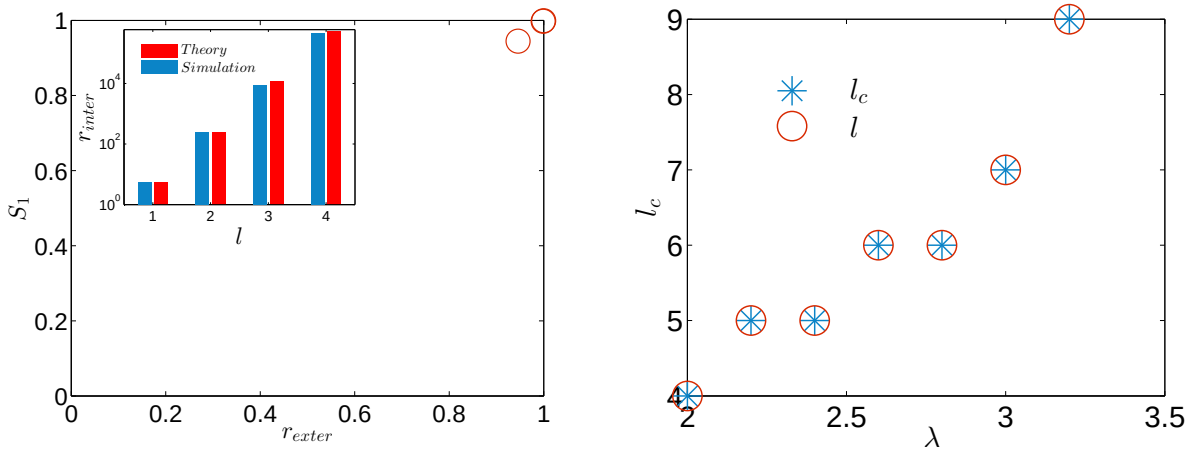

Figure 3: (a) For SF network, the simulations result of the size of the giant component S_1 versus r_{exter} with different parameters for ER network. (a) $\widetilde{k} = 4$, $l = 11$ and the number of nodes the number of nodes $N = 10^7$. Otherwise, comparison between Eq.(1) and simulations of r_{inter} as a function of l are shown in subgraph. (b) The critical shell l_c as a function of λ with $N = 10^6$, where L denotes the furthest shell from root node. The simulation results are averaged over $N = 10^7$ realizations for (a), the other are 10^3 realizations in the simulations.

attack by taking ER, RR, SF networks as examples. Moreover, we find that the shell, where the giant component become zero is almost one of two farthest shells from root node. The results highlight that increasing connection density that have been found to useful to significantly improve robustness of networks.

Acknowledgments

This work was supported by National Natural Science Foundation of China (Grant Nos. 61403171, 71403105, 71303095), National Natural Science Foundation of Jiangsu Province (Grant Nos. BK20140569, BK20130535), National Natural Science Foundation of Jiangsu Province (Grant Nos. 14KJB120001, 13KJB120001), Jiangsu Postdoctoral Science Foundation (Grant No. 1402077B, 1501100B) and Senior talents Foundation of Jiangsu University (Grant Nos. 14JDG143, 14JDG144), China Postdoctoral Science Foundation Grant No. 2015M581738.

References

[1] S. Boccaletti et al. Hwang Complex networks: Structure and dynamics. *Physics Reports*. 424(2006): 175 - 308.
[2] S. Shao et al. Percolation of localized attack on complex networks. *New J. Phys.* 023049(2015): 17.
[3] J. Shao et al. Structure of shells in complex networks. *Phys. Rev. E* 36105(2009): 80.
[4] R. Albert et al. Statistical Mechanics Of Complex Networks *Rev Mod Phys* 74(2002): 47.
[5] R. Cohen et al. Attacks and Cascades in Complex Networks *Phys. Rev. Lett.* 4626(2000): 85.
[6] C. Crucitti et al. Efficiency of scale-free networks: error and attack tolerance. *Physica A* . 320(2003): 622-642.
[7] P. Crucitti et al. Error and attack tolerance of complex networks. *Physica A* . 340(2004): 388-394.
[8] E. Ben-Naim et al. Complex Networks, Springer, Berlin. *IEEE Contr. Syst. Mag.* 21(2004): 11-25.
[9] D. J. Watts and S. H. Strogatz. Collective dynamics of small-world networks. *Nature*. 393(1998): 440.
[10] M. Kitsak et al. Identification of Influential Spreaders in Complex Networks. *Nat. Phys.* 6(2010): 888-893
[11] A. -L. Barabási and R. Albert. Emergence of scaling in random networks. *Science*. 286(1999): 509.
[12] L. A. N. Amaral et al. Classes of Small-World Networks. *Proc. Natl. Acad. Sci. USA* . 97(2000): 11149-11152.
[13] D. Markovic et al. Self-Avoiding Walks on Random Networks of Resistors and Diodes. *Physica A*. 144(1987): 1-16.
[14] M. E. J. Newman and D. J. Watts. Renormalization group analysis of the small-world network model. *Phys. Lett. A*. 263(1999): 341-346.
[15] A. -L. Barabási et al. Deterministic scale-free networks. *Physica A*. 299(2001): 559-564.

[16] R. Albert and A. -L. Barabási. Statistical mechanics of complex networks. *Rev. Mod. Phys.* 74(1)(2002): 47-97.
[17] Y. Chen et al. Percolation Theory Applied to Measures of Fragmentation in Social Networks. *Phys. Rev. E*. 75(2007): 046107.
[18] D. Li et al. Dimension of spatially embedded networks *Nature Phys.* 7(2011): 481.
[19] M. E. J. Newman. The structure and function of complex networks. *SIAM Review.* 45(2)(2003): 167-256.
[20] D. J .Watts. Small World:The dynamics of Networks between Order and Randomness. *Princeton University Press.* 1999.
[21] T. Konno. An imperfect competition on scale-free networks,. *Physica A* (2013).
[22] Z. Lu et al. Deterministic scale-free small-world networks of arbitrary order. *Physica A* . 392(2013): 3555-3562.
[23] S. Havlin et al. Optimal Path in Random Networks with Disorder: A Mini Review [Proc. Kolkata Conf on Networks], *Physica A*. 346(2004): 82-92.
[24] G. Dong et al. Percolation of partially interdependent networks under targeted attack. *Phys. Rev. E*. 85(2012): 016112.
[25] G. Dong et al. Robustness of network of networks under targeted attack. *Phys. Rev.E* . 87(2013): 052804.
[26] D. Zhou et al. Percolation of Partially Interdependent Scale-free Networks. *Phys. Rev. E* . 87(2013): 052812.