Enhancing the Scale-Free Network's Attack Tolerance

Zehui Qu[1,2] , Pu Wang[2,3], and Zhiguang Qin[1]

[1] University Electronic Science and Technology of China (UESTC), Chengdu, SC, 610054, China
zehui.qu@gmail.com
[2] Center for Complex Network Research, Department of Physics, Biology and Computer Science, Northeastern University, Boston, MA 02115, USA
[3] Center for Complex Network Research and Department of Physics, University of Notre Dame, Notre Dame, IN 46556, USA

Abstract. Despite the large size of most communication systems such as the Internet and World Wide Web (WWW), there is a relatively short path between two nodes, revealing the networks' small world characteristic which speeds the delivery of information and data. While these networks have a surprising error tolerance, their scale-free topology makes them fragile under intentional attack, leaving us a challenge on how to improve the networks' robustness against attack without losing their small world merit. Here we try to enhance scale-free network's tolerance under attack by using a method based on networks' topology re-constructing.

Keywords: Complex network, scale-free network, network, robustness, intentional attack.

1 Introduction

Small world and scale free are widely observed in most communication systems, such as the Internet, the World Wide Web (WWW) and Wireless Sensor Network (WSN) [Albert et.al 1999; Albert and Barabsi 2002]. The small world property of these communication networks is characterized by their short average path length [Watts and Strogatz 1998], which guarantees the efficient delivery of information and data. Usually, in these networks nodes are not uniformly distributed but follow a power-law distribution [Barabsi and Albert 1999], implying that these networks are scale-invariant without a 'typical' node (a Gaussian distribution has a mean node). The scale-free property which is rooted in network's inhomogeneous connectivity distribution seriously reduces the network's attack survivability, making scale-free not a good candidate topology for communication systems [Albert and Barabsi 2002; Callaway et.al 2002]. However, small world is not the causality of scale-free; for example, a random network which has a Gaussian degree distribution can also be a small world network [Albert and Barabsi 2002]. This fact and the feasibility of re-constructing the communication systems' topological structure enable us to construct an ideal communication network with message delivery efficiency and strong attack tolerance.

J. Zhou (Ed.): Complex 2009, Part II, LNICST 5, pp. 1823–1826, 2009.

2 Method and Algorithm

There are some candidacy methods to archive our goal. For instance, rewired the network, add a links or node as less as possible, replace the hub as a special sub graph.

We re-construct the network by combined several methods and detaching hub's neighbor nodes with the increasing of average path length less than one.

The idea of network rewiring algorithm is proposed as following: a. Find out the largest hub which has the maximum degree in the network. b. Select the pivot node which connects to the hub and has the minimum degree. c. Delete the link between the pivot node and the largest hub and connect the pivot node to the node with the second smallest degree. Then set a 'nonHubChanged' tag to these two nodes to avoid redo the change work. d. If the connectivity of the network has changed then redo the rewire process by selecting another minimum degree node as the pivot node. The new pivot's selection rule is: select the node with a degree equal to less than the old pivot's degree. e. If the connectivity of the network dose not change after rewired, go to a again. Otherwise go to f. f. Set a 'hubChanged' tag to the hub. If still have some nodes without any changed tag. Selected anther node as hub in remained set nodes. Then go to d.

After re-linked, the degrees of the hubs have been reduced without increasing the network's average same degree.

In Fig. 1, we show a subset network of WWW and the rewired network based on our algorithm. We can see that the average path length of the network only increased less than one, however, the in P(k) k- has a sharp decrease, implying that we successfully decrease the network's scale-free property by not losing its small world characteristic.

The parameter Sg/So is wildly used to describe the robustness of networks. Where Sg is the size of the largest component in the network after damaged network and So is the largest component size of original network. We observe this

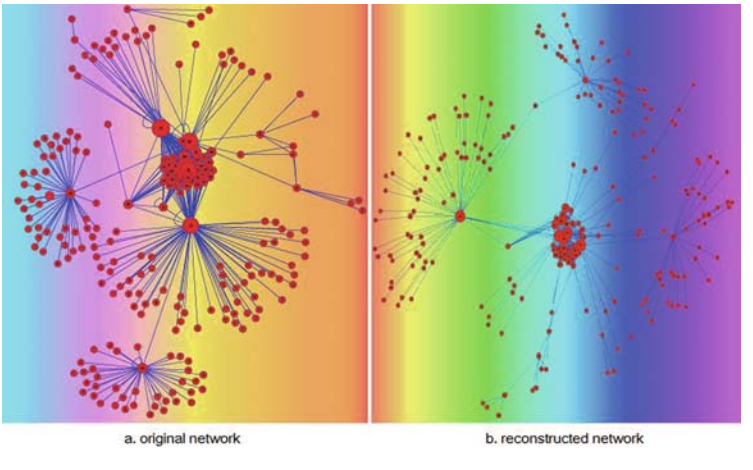

Fig. 1. Sub network of WWW and its re-constructed network

parameter as changing the links in subset network of WWW and the original one as Fig 2 shows:

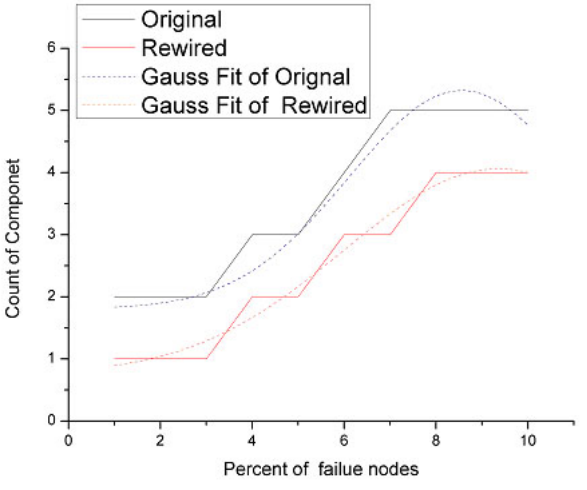

Fig. 2. Attack the top degree nodes

We randomly remove nodes from the original and rewired network. We find that both the original network and the rewired network have the same components until removed 30.

On the contrary, after removing the top three percent degree nodes, the original network are divided into two parts. But the rewired network is still connected. This means under intended attack, the rewired network is stronger than original one.

3 Conclusion

In this paper, we proposed an algorithm to enhance robustness of complex communication networks under intentional attacks. We considered the scale free is a crucial property associated robust of network. We found that after rewired network follow the algorithm the degree of big hub will be decrease, then the result from attack will be alleviated. On the other hand, the average path length of the network only has a neglectable difference between the rewired and original network.

Acknowledgment

We thank R. Albert, A.-L. Barabsi, Chaoming Song, Lan Luo and Hongrong Cheng. We would like to acknowledge China Scholarship Council (CSC).

References

1. Albert, R., Jeong, H., Barabsi, A.-L.: Diameter of the world wide web. Nature 401, 130–131 (1999)
2. Watts, D.J., Strogatz, S.H.: Collective dynamics of 'small-world' networks. Nature 393, 440–442 (1998)
3. Barabsi, A.-L., Albert, R.: Emergence of scaling in random networks. Science 286, 509–512 (1999)
4. Albert, R., Jeong, H., Barabsi, A.-L.: Error and attack tolerance of complex networks. Nature 406, 482 (2000)
5. Albert, R., Barabsi, A.-L.: Statistical mechanics of complex networks. Reviews of Modern Physics 74, 47–97 (2002)
6. Callaway, D.S., Newman, M.E.J., Strogatz, S.H., Watts, D.J.: Network Robustness and Fragility Percolation on Random Graphs. Phys. Rev. Lett. 85, 5468 (2000)
7. Xiao, S., Xiao, G., Cheng, T.H.: Tolerance of Intentional Attacks in Complex Communications Networks. IEEE Communications Magazine 46(1), 146–152 (2008)
8. Liu, J., Xiao, G., Lu, K., Chlamtac, I.: An Evaluation of Distributed Parallel Reservations in Wavelength-Routed Networks. IEEE Journal on Selected Areas in Communications - Supplement on Optical Communications and Networking 25(9), 27–39 (2007)
9. Achlioptas, D., Clauset, A., Kempe, D., Moore, C.: On the bias of traceroute sampling. In: Proc. ACM STOC 2005 (Feburary 2005)
10. Valente, A.X.C.N., Sarker, A., Stone, H.A.: 2-Peak and 3-Peak optimal complex networks. Phy. Review Letter 92, 118702 (2004)
11. Li, Y., Xiao, G., Ghafouri-Shiraz, H.: On Traffic Allocations in Optical Packet Switches. IEEE Journal on Selected Areas in Communications - Supplement on Optical Communications and Networking 25(9), 108–117 (2007)
12. Cohen, R., Erez, K., Ben-Avraham, D., Havlin, S.: Breakdown of the Internet under intentional attack. Phy. Review Letter 86(16), 3682–3685 (2001)
13. Alderson, D., Wilinger, W.: A contrasting look at self-organization in the Internet and next-generation communication networks. IEEE Commu. Mag. 43(7), 94–100 (2005); Li, L., Alderson, D., Willinger, W., Doyle, J.: A first-principles approach to understanding the Internet's router-level topology. In: Proc. ACM SIGCOMM 2004, pp. 3–14 (2004)
14. May, P., Ehrlich, H.-C., Steinke, T.: ZIB structure prediction pipeline: Composing a complex biological workflow through web services. In: Nagel, W.E., Walter, W.V., Lehner, W. (eds.) Euro-Par 2006. LNCS, vol. 4128, pp. 1148–1158. Springer, Heidelberg (2006)