Robustness of Dynamic Redundancy Nodes in Cascading Failure Networks

XU Ye[1]   CHI Yun[2]

[1] School of information science and engineering, Shenyang Ligong University, Shenyang, Liaoning 100159, China
xuy.mail@gmail.com

[2] Liaoning Academy of Governance, Shenyang, Liaoning 110161, China
chiyun@21cn.com

Received 31 March 2015; Revised 29 April 2015; Accepted 30 April 2015

Abstract. Network cascading failure is studied in this paper. We focus on robustness experiments on small world and scale - free networks. Firstly, based on the optical redistribution principle of collapse node according to its load is founded, and two cascading failure models are set up representing random attacks and target attacks respectively. Then mathematical reasoning of networks load under attacks is studied. Next, simulation experiments are performed to study the effect of network load and redundancy on network robustness. Results show that to an increase of network redundancy and a decrease of network load do help to the enhancement of network robust performance, which is quite consistent with mathematical analyses.

Keywords: complex networks, cascading failure, robustness, attacks, network load, network redundancy

1 Introduction

With the rise of the study of complex networks, people begin to concern the complexity of network structure and its effects on network behavior. A large number of different functions in the real world systems could be described as the networks. For example, human society - a network composed of a variety of social units connected with each other; Internet and computers networks - the one made up by communications units and media such as computers and routers which are connected to the network; the power networks, transport networks and so on [1-2]. These networks are known as "the complex network" because all of them have a high degree of complexity. With the continuous developments of researches of complex networks theory and disciplines [3-9], many scholars have started to focus on some new topics in complex networks such as cascading failure of the network and its robustness analyses by using such new theory and methods, combined with theories from system science and the science of complexity.

Within such fields, random failure and target attacks [10-14] and their effects on network robustness are getting to be the research hotspots. How to find a way to effectively attack the terrorist organization, to control the spread of the disease on network and to protect primary unit such as the Internet hub in the network are all closely related with the topic of the robustness of the network. Albert (2000) [10] and other researchers have discussed about this issue earlier, they made conclusions that scale-free networks are robust to random attacks but fragile to target attacks. Many other researchers made further studies in the fields of the robustness of networks. But most of researches were mainly focused on static networks, i.e., the nodes are removed only in a topological sense and their effects on the present of other nodes are not so much studied. So is the further topic on the effects of network redundancy over networks robustness. However, these are the present features existed in some complex networks examples in real world such as social networks, power networks, Internet and so on. There is a necessity that putting more efforts in such research fields and a topic of research of dynamic redundancy nodes and their effects on network robustness in some typical complex networks such as small-world networks and scale-free networks are taken a try in this paper.

2 Models to Generate Network Topology

There are many types of complex networks examples.

For a better understanding and experiments control of robustness studies in complex networks, we take two typical complex networks models-small-world networks and scale-free networks into consideration and perform some cascading failures experiments on them. First, we give brief introductions on how to construct such networks models.

2.1 Small-world Network

As the transition networks from the regular network to random network, small-world networks have two significant statistical characteristics. The first is having a high clustering coefficient which is similar to the regular network. The second is having a small average path length which is similar to random networks. The networks with topology having the upper properties are usually named as the small-world network [18]. In theoretical analysis level, NW small-world model is simpler than the model of the WS small-world networks model. So NW small-world model is used in this paper. Network generation algorithm [19] is listed as follows:

a) Consider a coupling network with N nearest neighbor nodes, lay the nodes to a ring and let each of the nodes be connected to the *K*/2 neighbor nodes. *K* is even.

b) Select an edge between a pair of nodes with probability p. Only one edge is allowed between any two different nodes and each node cannot have the edge connected to itself.

In NW small world model, p=0 corresponds to the original nearest neighbor coupling network and p=1 corresponds to the global coupling network. NW small world model would be essentially the same as WS small world model when p is small enough and N is large enough.

2.2 BA Scale - Free Network

Generation of scale-free network complies with the principle of preference dependency. When a new node appears in the network, it is more likely connected to an existed node with more links or edges. As time goes on, the generated networks will have some nodes having much more edges than other nodes, which is also known as the famous phenomenon of "Matthew effect". The generation modeling algorithms [19-20] are as follows:

a) Initial state: Set m_0 initial nodes and links between all nodes.

b) Growth: Add a new node with *m* links, $m<=m_0$.

c) Priority connection: The relations between the connection probability Π of a node to an existed node *i* and the degree K_i of node *i* is:

$$\Pi_i = \frac{k_i}{\sum_j k_j} . \tag{1}$$

After *t* steps of generation, the networks would evolve into one with $N=t+m_0$ nodes and *mt* edge.

3 Mathematical Analyses

3.1 Theoretical Analysis of Network Load

Cascading failure is a phenomenon having a lot in common with the other network propagation behaviors. Our research is focused on global dynamic properties of a network when a node is removed or failed. The global dynamic property means that one failed node would cause failure propagations in the networks. On the initial, each node is having a workload less than its safety threshold (capacity). We call this network to be in a stable state. Then we remove a node *i* (or put this node *i* into failure state), the workload of node *i* would be assigned to its neighbor nodes according to the coupling relationship among the nodes. The load redistribution could trigger in a certain probability the failures of the other nodes. This failure propagation procedure would not stop until all the affected nodes have their network load to be under their safety threshold, in which case the network reaches its equilibrium. Or sometimes the equilibrium would never be reached, and in this chain reaction, the failure propagation would result in failures of a considerable number of nodes or even collapse of the entire network, i.e., Internet congestion and blackout of power networks.

For networks in real world load, there is relations between the a node's workload and its degree in network topology:

1) The greater the degree of a node has in the network, the higher load it would have. For any initial node *j* in the network, the relations between its load and its degree are:

$$L_j = bK^{\alpha+\beta} . \tag{2}$$

where b, α, β are adjustable parameters, and b is multiplier factor defaulting to be 1. α is index coefficient indicating a node has more load capacities with greater degree. Studies found that the network system reaches most powerful when α=1. β is a attenuation function. It indicates that the relations between the node's load capacity and its degree is not fully proportional. Usually we set $\beta = 1/(1+e^{(-g\frac{K}{sum(K_j)})})$.

2) A failure node j would redistribute its load on to its neighbor nodes i on a probability of:

$$\prod_j = \frac{\beta k_j^\partial}{\sum_{n\in\Gamma_i} \beta k_n^\partial}. \tag{3}$$

where k is a set comprising all the neighbors of node i.

3) Then, when node i fails, its neighbor node j would receive additional load ΔL_{ji}:

$$\Delta L_{ji} = L_i \frac{k_j^\partial}{\sum_{n\in\Gamma_i} k_n^\partial}. \tag{4}$$

Take the factors into account that the processing load capacity of a node is bound by corresponding cost, so we give that a node's load is defined as its betweenness centrality (BC) which indicates the number of the shortest paths passing through this node in the network. Define node j's capacity C_j (maximum load) to be proportional to the initial load L_j:

$$C_j = (1+\alpha)L_j, j=1,\ 2,\ \cdots N \tag{5}$$

where constant α>=0 is a tolerance factor. The network runs in a free flow state under regular circumstances and when one node fails in the network, or if its load – the sum of the received load and its initial load, is greater than its capacity, i.e., $L_j + L_{ji} > C_j$, the node will fail. It could be considered that the failure node separated itself from the maximal connected subgraph of the networks, and the redistribution of the failure node's load would cause a failure propagation in the networks.

3.2 Formal Specification of a Network Cascading Failure

A ratio of the maximal connected subgraph over the networks G is used to measure he degree of collapse indicating how much the network has failed. And G is:

$$G = N'/N. \tag{6}$$

where N' is the size of the maximal connected subgraph after cascading failure propagations, and N is the size of the initial network.

4 Simulations

4.1 Generation of Network Model

A NW small-world networks and a BA scale-free networks are generated according to above algorithms, respectively. Set N is the size of the corresponding networks, m_0 is size of the initial networks, m is increase of links when a new node is generated.

In the simulation, parameters are set as:

1) Small-world networks: N=50，m=4;

2) Scale-free networks: N=50，m=3，m_0=3.

The generated two kinds of networks are illustrated in Fig. 1.

4.2 Robustness Analyses

For a better view of robustness properties of the two networks, random and target attacks on the nodes are mainly studied and experiments are simulated. Experimental parameters are set as:

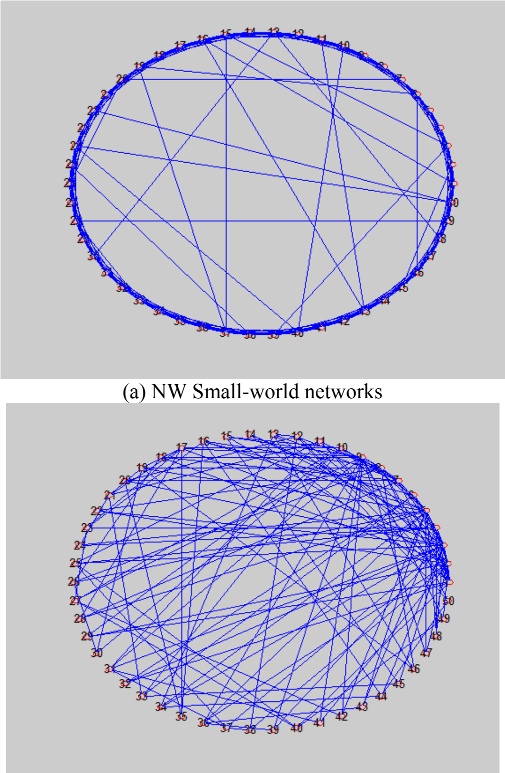
τ is attack index with value range [0 1]; τ=1 indicates a complete random attack and τ=0 is a fully target attack which is the kind of attack implemented directly on the nodes with the largest degree.

ω is network load index with value range [0 1]; ω=1 indicates the network is at full capacity and ω=0 indicates the network is at empty load.

θ is network redundancy index with value range [0 1]; the higher *θ* is, the higher the level of redundancy the network has. The network costs of generation and maintenance, however, would largely increase with the growth of parameter network redundancy index *θ* at the same time.

With the parameters set as above, we perform three kinds of experiments as follows:

(1) Set *ω*=0.5, *θ*=0, and set *τ*=0 and *τ*=1 to simulate target attacks and random attacks respectively. The experiment results are illustrated in Fig. 2 in which the red curve is for the NW small-world network and the blue curves for BA scale-free networks.



(a) NW Small-world networks

(b) BA Scale-free networks

Fig. 1. Topology of two generated networks

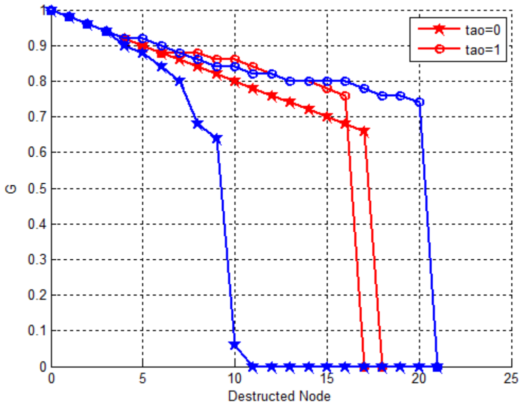


Fig. 2. Results of NW small-world network and BA scale-free networks under random and target attacks when set *ω*=0.5, *θ*=0.

It is obvious from Fig. 2 that, a) For NW small-world networks, the difference of robustness against two attacks is rather minor under the same conditions. Compared with NW small-world networks, BA scale-free networks is quite different against two attacks. It expresses a better robustness against random attacks but an extreme vulnerability under target attacks. b) The rate of the red curve in the figure declines slowly and obviously stays on the right side of the blue one when τ=0. So the robustness of NW small-world networks is stronger than BA scale-free networks against target attacks. However, BA scale-free networks are better than NW small-world networks in robustness against random attacks.

Conclusions could be made from above: degree of BA scale-free networks complies with a power-law distribution resulting an uneven distribution of nodes in networks leading to the results of vulnerability to target attacks and robustness against random attacks. Small-world networks, however, have a similarly uniform distribution of nodes' degree, and do not show a clear characteristics such as BA networks under different attacks.

(2) Set τ=0, θ=0 and τ=1, θ=0 to research networks' abilities against two attacks in a state of no redundancy. The experiment results are illustrated in Fig. 3 and Fig.4 in which the red curve is for the NW small-world network and the blue curves for BA scale-free networks.

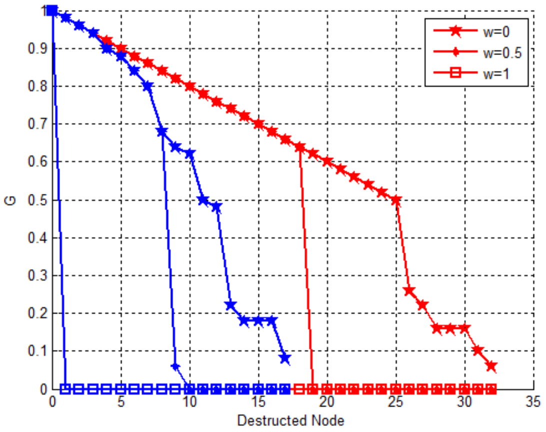


Fig. 3. Results of NW small-world network and BA scale-free networks under target attacks when set ω=[0, 0.5, 1] and θ=0.

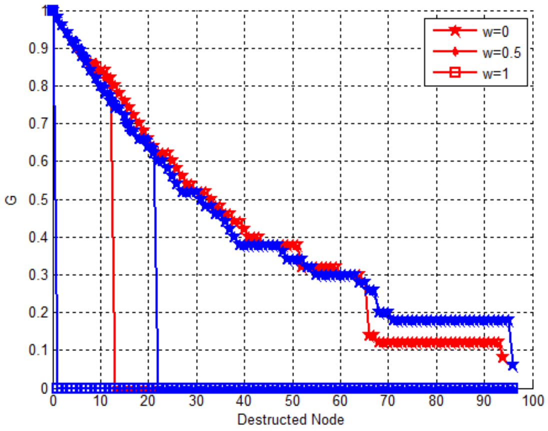


Fig. 4. Results of NW small-world network and BA scale-free networks under random attacks when set ω=[0, 0.5, 1] and θ=0.

From the figures we see that the larger the network load is, the faster both curves decline showing that both networks would collapse faster with larger workloads.

a) Scale-free networks

Further observe the figures of the scale-free networks (the blue curves) we find that the networks collapse less than 20% when random attacks killing about 20% of the total nodes in the network at ω=0. And in target attacks, however, when nearly 20% of the network nodes fail, the network collapse index G reaches around 50%. At ω=0.5, the network to totally collapse when random attacks destroy about 35% nodes. Target attacks would cause a complete collapse with only destroy around 10% nodes.

At ω=1, only a random failure of 0.1% of the total nodes would result in a crash of the network completely. And a complete collapse of networks only needs failures of less than 0.02% nodes under target attacks.

b) Small-world networks

Similar to the analyses of scale-free networks, it's obvious that networks are easy to collapse when being under a high load. A minor increase of attacks would result in a complete crash from robustness state.

The both networks, however, show a strong robustness against random attacks no matter how much the workloads are, showing that the robustness properties of both networks are not much influenced by parameter workload. The network load index only plays a role of a "catalyst" in failure propagations in the networks.

(3) Set τ=0, ω=0.5 and τ=1, ω=0.5 to research networks with the same load but different redundancy under random and target attacks. The experiment results are illustrated in Fig. 5 and Fig. 6 in which the red curve is for the NW small-world network and the blue curves for BA scale-free networks.

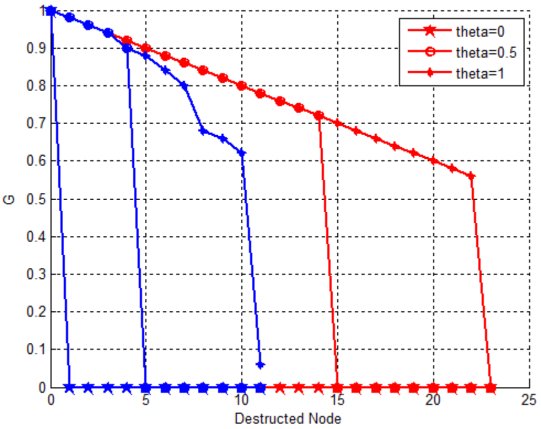


Fig. 5. Robustness results of NW small-world network and BA scale-free networks under target attacks when set *θ*=[0, 0.5, 1].

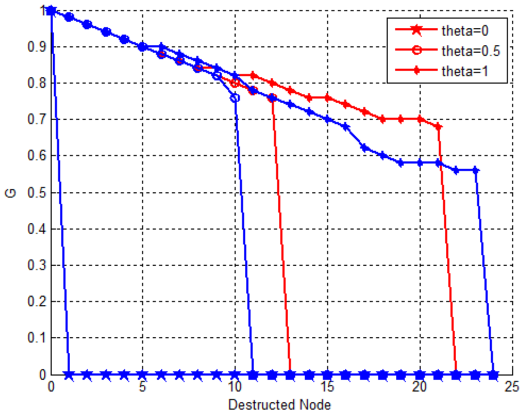


Fig. 6. Results of NW small-world network and BA scale-free networks under random attacks when set θ=[0, 0.5, 1].

From the figures we find that for both networks under both attacks with fixed workloads, the crash curves shifts clearly to right showing that they both show a great performance of robustness when network redundancy increases. Continue to increase *θ* till it reaches 1, the networks would get into an extreme state – fully-connected networks, and would have the best robustness performances although the maintenance cost of networks increases sharply. Furthermore, network load also influences badly the networks robustness no matter how much the redundancy the network has, which means that robustness of the network will also receive substantial inhibition when the network is overloaded.

5 Conclusions and Works Next

BA scale-free networks and NW small-world networks model and their robustness against attacks are studied in this paper. Network load index and network redundancy index would give much effect on network robustness.

The experiments performed in this paper are focused mainly on the failures and failures propagations of nodes, those of edges in networks are not involved yet. How to assign weights to links so as to improve the overall ability of network robustness against attacks and failure propagations is a quite important and significant issue. On the one hand, there is still a lack of general way to give definitions to the weights of edges in the networks. On the other hand, even after the assignments of the weights and there is still lack of studies of how the weights would affect the nature, topology, efficiency and robustness of networks. Therefore, the further studies on these issues are of great significance and these would be our next work.

Acknowledgment

This work was supported in part by a grant from the National Natural Science Foundation of China (No. 61373159), the Shenyang Natural Science Foundation (F13-316-1-22) and the Open foundation of Key lab of Information Networking and Confrontation of Shenyang Ligong University (No. 4771004kfs18).

References

[1] R. Albert, A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of Modern Physics*, Vol. 74, 47, 2002.

[2] M.E.J. Newman, "The structure and function of complex networks," *SIAM Review*, Vol. 45, No. 2, pp. 167-256, 2003.

[3] V. N. Gudivada, "Information Retrieval on the World Wide Web," *IEEE Internet Computing*, Vol. 1, No. 5, pp. 58-68, 1997.

[4] D. J. Wats, S. H. Strogatz, "Collective dynamics of small-world networks," *Nature*, Vol. 393, pp. 440-442, 1998.

[5] D. J. Wats, P.S. Dodds, and M.E.J. Newman, "Identity and search in social networks," *Science*, Vol. 296, pp. 1302-1305, 2002.

[6] S. H. Strogatz, "Exploring complex networks," *Nature*, Vol. 410, pp. 268-276, 2001.

[7] C. Li, K. Philip, "Complex networks generated by the Penna bit-string model: emergence of small-world and assortative mixing," *Physical Review E*, Vol. 72, 045102, 2005.

[8] S. Milgram, "The small-world problem," *Psychology Today*, Vol. 2, pp. 60-67, 1967.

[9] A. Barabasi, R. Albert, "Emergence of scaling in random networks," *Science*, Vol. 286, No. 5439, pp. 509-512, 1999.

[10] R. Albert, H. Jeong, A.L. Barabsi, "Attack and error tolerance in complex networks," *Nature*, Vol. 406, pp. 87-482, 2000.

[11] J. Carlson, J. Doyle, "Highly optimized tolerance: Robustness and power laws in complex systems," *Physical Review Letters*, Vol. 84, pp.2529-32, 2000.

[12] A. Broder, R. Kumar, F. Maghoul et al., "Graph structure in the web," *Computer Networks*, Vol. 33, No. 1-6, pp. 309-320, 2000.

[13] A.X.C.N. Valente, A. Sarkar, H. A. Stone, "Two peak and three peak optimal complex networks," *Physical Review Letters*, Vol. 92, 118702, 2004.

[14] B. Bollobas and O. Riordan, "Robustness and vulnerability of scale free random graphs," *Internet Mathematics*, Vol. 1, No. 2, pp. 215-225, 2003.

[15] R. Pastor-Satorras, A. Vazquez, A. Vespignani, “Dynamical and correlation properties of the Internet," *Physical Review Letters*, Vol. 87, No. 25, 258701, 2001.

[16] W. Willinger, et al., "Scaling phenomena in the Internet: Critically examining criticality," *Proceedings of the National Academy of Sciences*, Vol. 99, pp. 2573-2580, 2002.

[17] K.I. Goh, B. Kahng, D. Kim, "Fluctuation-driven dynamics of the Internet topology," *Physical Review Letters*, Vol. 88, 108701, 2002.

[18] D.J. Watts, S.H. Strogatz, "Collective dynamics of ‘small-world’ networks," *Nature*, Vol. 393, No. 6684, pp. 440-442, 1998.

[19] X. Wang, X. Li, G. Chen, *The Complex Network Theory and Its Applications*, Beijing, China: Tsinghua University Press, 2006.

[20] Y. Xu, *Internet Topology Modeling Based on Large - Scale Models*, Beijing, China: Publishing House of Electronics Industry, 2011.