International Journal of Security and Its Applications
Vol. 10, No. 1 (2016), pp.277-286
http://dx.doi.org/10.14257/ijsia.2016.10.1.26

Robustness and Security of Router-level Internet and Complex Networks Examples under Hybrid Networks Attacks

Xu Ye, Shen Yang, Wang Zhuo

School of information science and engineering, Shenyang Ligong University
Shenyang, Liaoning 100159, China
{xuy.mail, shenyang, wangzhuo}@163.com

Abstract

For a better predicting and analyses of robustness and security properties of some networks examples such as scale-free networks, small-world networks and real-world router-level Internet, models with different topologies and variable loads of the corresponding networks were founded firstly. Then, experiments of hybrid attacks ranging from complete random attacks where attack parameter tao=1 to complete targeted attacks where tao=0 were simulated. Results showed clearly that scale-free networks were robust to random failures and quite fragile to target attacks and the progression of networks fragility seems to have power-law distribution with workload parameter. For the NW small-world networks, attacks types are not so much sensitive to the robustness of the networks. What's found here would be useful for design and implement of some real-world networks.

Keywords: *scale-free networks; small-world networks; robustness; hybrid attacks; variable loads*

1. Introduction

With the rapid development of the study in complex networks, people begin to find interactions between the complexity of network topology and its effects on network behavior. Many scholars have started to study such new topics in complex networks, and study of cascading failure [1] of network are becoming flourishing.

A large number of different functions in the real world systems could be described as 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. Some of urgent needs in real-life networks such as 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 highly studied recently and something was found that all such issues were closely correlated with the topic of the robustness of the network. Therefore, random failure and target attacks[10-14] and their effects on network robustness are getting to be new research interests.

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 under single kind of attacks, *i.e.*, the networks were attaced in random or target way, the effects of hybrid attacks on present network nodes are not so much studied. There is a necessity that putting more efforts in such research fields in some typical complex networks such as small-world networks and scale-free networks, and studies to these topics are performed

ISSN: 1738-9976 IJSIA

in this paper.

2. Topological Properties of Complex Networks Examples

2.1. 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. The growth of BA scale-free networks is shown[3-5] in Figure 1.

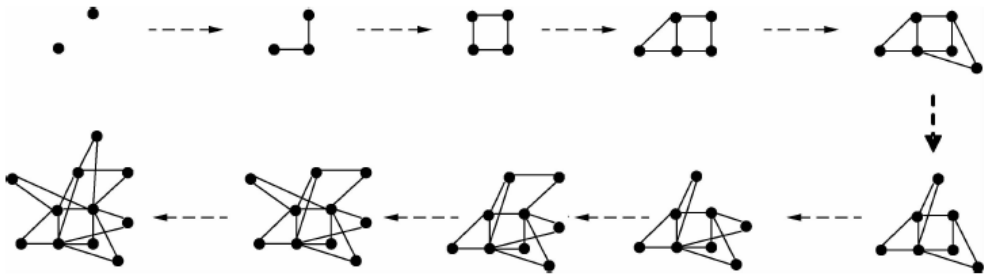


Figure 1. Growth of Scale-Free Networks

2.2. NW Small World networks

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:

1) In a network, the distance between two nodes i and j d_{ij} is defined as the number of edges connecting the two nodes in the shortest path. The maximum distance between any two nodes in a network is called the network diameter [14], recorded as $D, D = \max_{i,j} d_{ij}$.

Average path length l of a network is defined as the average of the distances between any two nodes:

$$L = \frac{1}{\frac{1}{2}N(N+1)} \sum_{i \geq j} d_{ij} \quad (2)$$

Where N is the number of nodes in the network. The average path length of the network is also known as the characteristic path length.

2) 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.

3) 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.

2.3. Router-Level Internet Topology

Measuring Internet is to accurately capture the quantitative measurement data of the Internet and their activities. Generally, main parameters of network measurement include RTT, path data, bandwidth and delay, congestion, the bottleneck, the target site accessibility, throughput, and bandwidth utilization, packet loss rate, response time of servers and network devices, the largest network traffic, and QoS *etc*.

The measured results were generated from the router-level Internet measuring monitors dispersely located in the continents on the earth, and more than twenty of the monitors were employed. We eventually have twenty-one testing samples together with the complete testing sample. To main reason to generate these twenty-one samples is to avoid the sampling bias [2][5] in the large extent. Though the problem of sampling bias is not the main topic of the paper, we still made our efforts to reduce the effect of the sampling bias by increasing sampling nodes [2][5]. The final Internet samples were composed of measured results from as many as twenty-one monitors.

3. Robustness Analysis of Complex Networks Examples

3.1. Identification Parameters of Robustness

Robustness is used to represent the ability to maintain its functions or properties when the system is disturbed especially from outside interference or damage. In complex networks it reflects the ability of a network structure to resist the destructions.

The robustness of the complex networks can be expressed through the network behavior under the attacks. Attacks are divided into two broad categories: one is complete random attack that is to randomly remove a few of the nodes in the networks; the other is target attacks that are to attack peticular nodes in the networks, especially those nodes with highest degree. Compared with random attacks, target attacks could destroy high-degree-nodes in networks and usually result in greater harms. Most of the scale-free network has good robustness against random attacks, but for target attacks, especially for high-degree-node attacks, they show fragility.

We start several robustness experiments on the complex networks examples against random attack and target attack respectively. Some of the parameters in simulation experiments are：

τ is scale for the attack, its value lies in interval [0,1], when τ=1 it means a complete random attack, and when τ=0 it is called complete target attack;

ω is network load, its value lies in range [0,1], when ω=1 it indicates that the network is under full load, when ω=0 it means that the network is zero loaded;

θ is network redundancy, its value lies in range [0,1], and the higher θ is, the more

redundancy the network is, whearas the costs of network construction and maintenance increase at the same time.

In this paper, we set G to evaluate the degree of network collapse:

$$G = \frac{N'}{N} \tag{9}$$

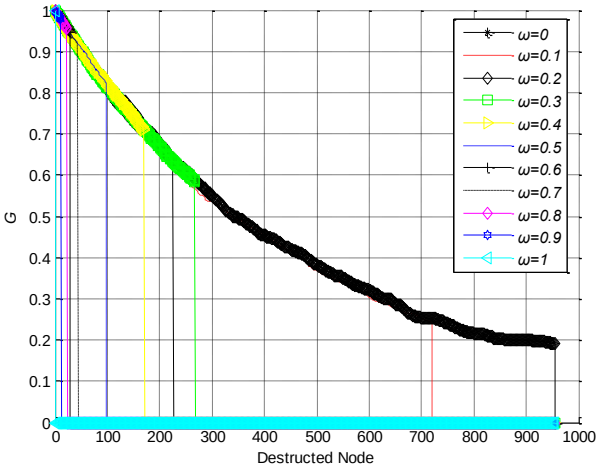
where N is the number of nodes in the network simulation experiments, N' is the number of nodes of the maximum connected subgraph after the end of cascading failure in the network, G is the parameter indicating connectivity of largest connected subgraph .

3.2. Analysis of Networks Examples

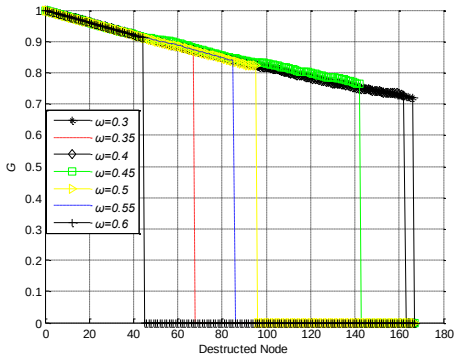
3.2.1. Attacks on BA Scale-Free Networks: In order to study the effect of network load over the robustness of BA Scale-free networks, an experiment on a 1000-node topology under random attacks and target attack are performed respectively.

(1) Random attacks

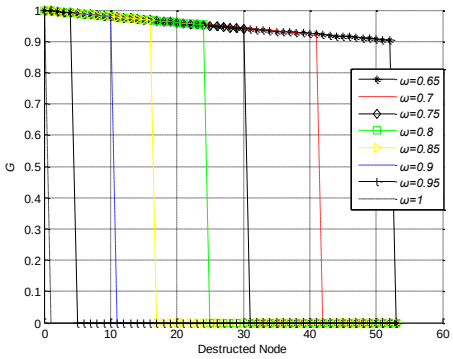
We set τ=1 (random attack), ω=[0, 1], θ=0 (network redundancy is zero). Experiments results are shown in Figure 2.



(a) Result of random attacks with ω=[0,1]



(b) Result with ω=[0.3,0.6]



(c) Result with ω=[0.6,1]

Figure 2. Random Attacks on the BA Scale-Free Networks with Network Load Changes

Figure 2(a) gives us an overview of experiments results with ω ranges from 0 to 1. And Figure 2(b) and 2(c) gives us a better view of results while ω ranges between [0.3, 0.6] and [0.6, 1] respectively.

From Figure 2(a) we can see that: BA scale-free networks seem to be robust against random attacks since it does not collapse till more than 90% nodes were destroyed when ω is set to be a very low value, *i.e.* 0. And when network load ω=0.1, random attacks damage around 25% nodes in the networks to make network collapse with G reaches 50%. When the percent of the damaged nodes reaches 72%, the collapse degree G reaches under 10% indicating the network is completely collapsed.

For a better view of it, we move to Figure 2(b) and 2(c). Here we find that with the growth of network load ω, we see that only less than 17% of destroyed nodes would result in a networks breakdown with ω=0.3. Then with ω grows from 0.3 to 0.6 in Figure 2(b), the threshold of a percent of destroyed nodes for networks collapse is found to be 14%, 10%, 8% and so on. Move to Figure 2(c), we see the same properties that fewer nodes destoyed would lead to same collapse in the networks. Figure 3 gives the ratio of destroyed nodes over how much networks would breakdown with different network loads.

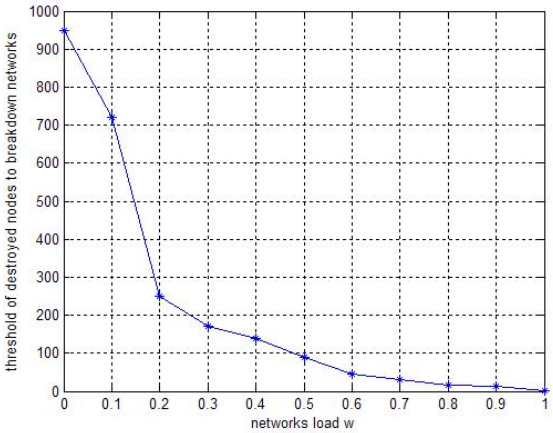


Figure 3. Ratio of Destroyed Nodes in Collapse Scale-Free Networks with Different Network Loads

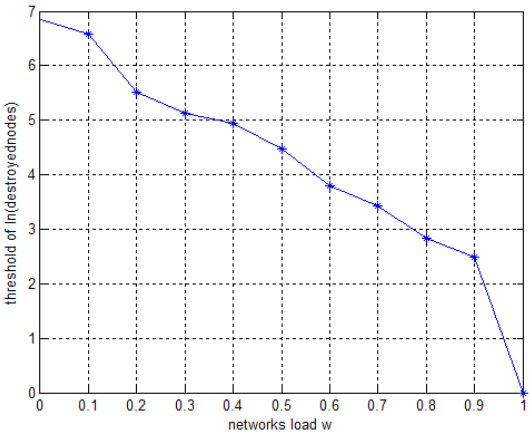


Figure 4. Semi-Log View of the Ratio of Destroyed Nodes in Collapse Scale-Free Networks with Different Network Loads

From Figure 3, it's found that the ratio of required destroyed nodes decrease sharply with increase of workloads. We give a further view in a semi-log coordinate in Figure 4 and a close straight line is resulted. By this, it's roughly concluded due to straight line in semi-log coordinate that there is a kind of power-law properties between the ratio of destroyed nodes and the workloads to breakdown scale-free networks. That is to say, the requirement amount of destroyed nodes for collapse BA scale-free networks would sharply decrease when workloads get larger and larger. Conclusions could be made that scale-free networks are quite robust against random attacks, however, it turns out to be very fragile when workloads is getting heavier.

(2) Target attacks

The experiments of target attacks on BA scale-free networks are performed and the results are shown in Figure 5.

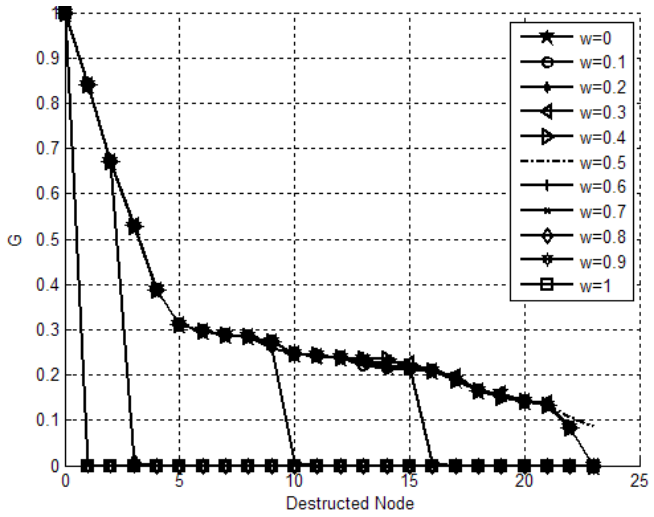


Figure 5. Target Attacks on the BA Scale-free Networks with the Network Load Changes

As expected, we see from the figure that BA scale-free networks are completely fragile to target attacks. No matter what network load value is, only a minor damage to nodes in networks would lead to a cascading failure and results in an overall collapse in BA scale-free networks.

3.2.2. Attacks on NW Small-World Networks: (1) Generation of NW small-world networks

According to the NW small-world network model, we set a network with average degree K=4, probability p=0.2 and size N=500. The generated result is illustrated in Figure 6.

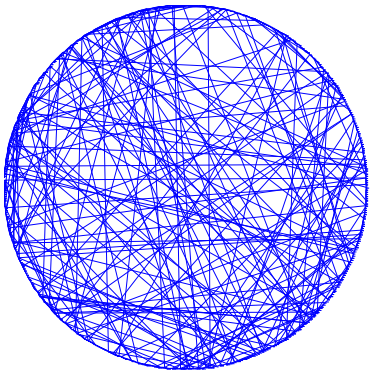
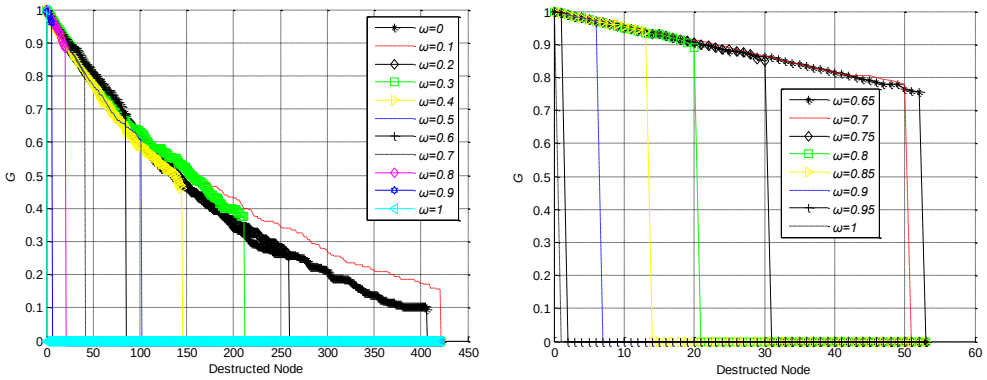


Figure 6. Example of NW Small-World Networks with N=500, K=4 and p=0.2

Random attacks and target attacks are simulated on this NW small-world networks.

(2) Random attacks

We set τ=1 (random attack), ω=[0, 1], θ=0 (network redundancy is zero) to simulate random attacks experiments. Experiments results are shown in Figure 7.



(a) Result of Random Attacks with ω=[0,1]

(b) Result of Random Attacks with ω=[0.6,1]

Figure 7. Random Attacks on the NW Small-World Networks with Network Load Changes

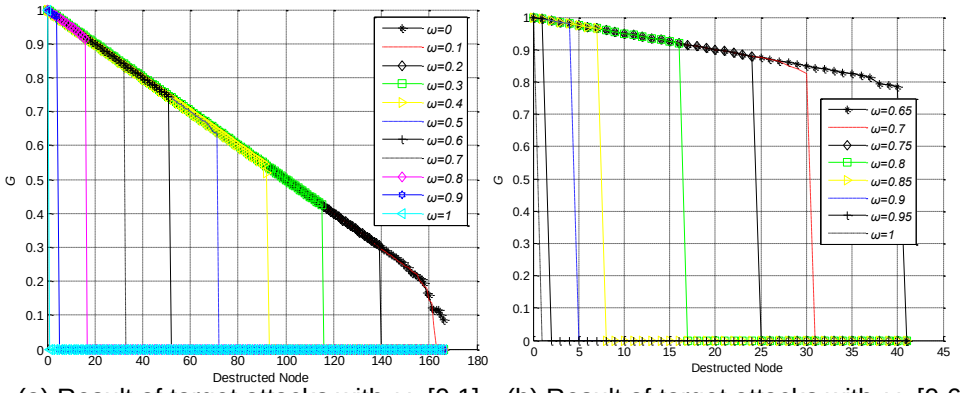
Figure 7(a) gives us an overview of experiments results with ω ranges from 0 to 1. And Figure 7(b) gives us a better view of results while ω ranges between [0.6, 1].

From Figure 7(a) we can see that: NW small-world networks seem to be robust against random attacks since it does not collapse till 420 and 430 nodes of 500-node-size networks die, which means the networks collapse parameter G reaches below 0.1 only after more than 85% of nodes in the networks are destroyed.

However, the networks get fragile when the workload is getting larger. We find in Figure 7(b) that only a destroy of 55 out of 500 nodes would lead to a quick breakdown in the small-world networks with ω=0.65. For simulations with ω>0.65 in this figure, quicker collapse is resulted with fewer nodes die.

(3) Target attacks

We set τ=0 (target attack), ω=[0, 1], θ=0 (network redundancy is zero) to simulate target attacks experiments. Experiments results are shown in Figure 7.



(a) Result of target attacks with ω=[0,1] (b) Result of target attacks with ω=[0.6,1]

Figure 8. Target Attacks on the NW Small-World Networks with Network Load Changes

Figure 8(a) gives us an overview of experiments results with ω ranges from 0 to 1. And Figure 8(b) gives us a better view of results while ω ranges between [0.6, 1].

From Figure 8(a) we can see that: NW small-world networks seem not to be so much sensitive to target attacks as that of BA scale-free networks. When the networks are working in light workload with ω is set to be 0, 0.1, it would not breakdown until more than 34% nodes die. With Figure 8(b), we see clearly that the networks become less

robust quickly with the increase of workloads. Only a breakdown of very few nodes would result in a collapse of networks when workload ω>0.8.

Here we find that NW small-world networks are not so much sensitive to attack types. And when the workloads are getting larger, the networks would also lead to collapse very quickly under both random and target attacks.

From the above experiments we see that target attacks would lead the NW small-world networks to a quicker breakdown in target attacks than that in random attacks. And the difference, however, is not significant. The reason to this conclusion might lie in that uniform distribution of nodes in NW small-world networks.

3.2.3. Attacks on Router-Level Internet: (1) Random attacks

Experiments on a one-thousand-node router-level Internet topology is set up here with parameters set as τ=1 (random attack), ω=[0, 1], θ=0 (network redundancy is zero). Experiments results are shown in Figure 9.

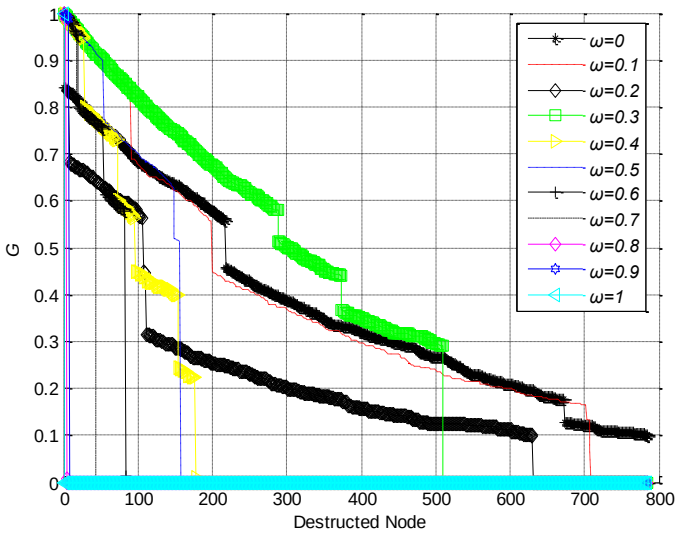
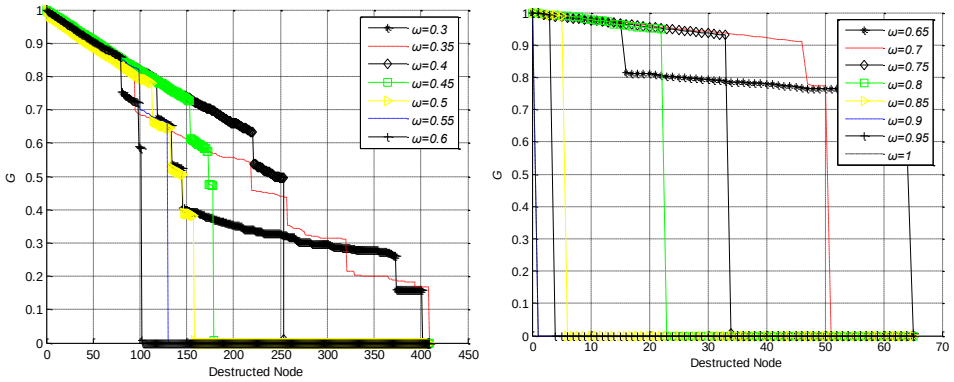


Figure 9. Random Attacks on the Router-Level Internet with Network Load Changes

From Figure 9 we can see that Internet seems to be robust against random attacks since it does not collapse till more than 70% percent of nodes die at a low workload. Compared to that of BA scale-free networks in Figure 2(a), we see that Internet is closely similar to but a little less than scale-free networks in robustness against random attacks. When workloads get higher, the networks' robustness decrease sharply, as the other two networks do.

(2) Target attacks

We set τ=0 (target attack), ω=[0, 1], θ=0 (network redundancy is zero) to simulate target attacks on router-level Internet topology and results are illustrated in Figure 10.



(a) Result of Target Attacks with ω=[0.3,0.6] (b) Result of Target Attacks with ω=[0.6,1]

Figure 10. Target Attacks on the Router-Level Internet with Network Load Changes

It's found from Figure 10(a) that Internet robutness against target attacks is very low though the networks work in a low workloads. With increase of workloads, Internet is getting more fragile against target attacks.

3.2.4. Comparisons Among the Complex Networks Examples: With experiments results from random attacks on BA scale-free networks, NW samll-world networks and router-level Internet, it's seen that all three networks are kind of robust ones when workloads are low. The worksloads have a high impact on all three networks and the sacle-free networks, however, is most influenced since there is power-law decrease in it's roubutness with workloads increase. In this view, Internet ranks two and NW samll-world is the last.

For the target attacks experiments, we see BA scale-free networks and Interent are quite fragile unders such attacks. BA scale-free networks seems to be worse in roubstness than Internet, and NW samll-world is best in robustness against target attacks.

4. Conclusions

In this paper, some of complex networks examples were discussed and robustness experiments on these networks under hybrid attacks were performed. The experiments results showed that that scale-free networks and Internet were robust to random failures and quite fragile to target attacks. For the NW small-world networks, attacks types are not so much sensitive to target attacks on the networks. As for random attacks, all three networks have relative robustness when workloads are low. All three networks become fragile when workloads are getting higher.

On the workloads issue, some studies show that there is a way to decrease the negative effects of the heavy workloads by increasing networks redundancy, and this would be our future works.

Acknowledgement

This work is financially supported by 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. Dai, L. Cao, “Internet-an open complex giant systems”,Science in China, vo.33, no.4, pp. 289-296.
[2] M. Faloutsos, P. Faloutsos, “On power-law relationship of the Internet topology”,ACM SIGCOMM Com puter Communication Review, vol. 29, no.4, **(1999)**, pp.251-262.
[3] Y. Jiang, B.X Fang, M.Z Hu, “An Example of Analyzing the Characteristics of a Large Scale ISP Topolo gy Measured from Multiple Vantage Points[J]”, Journal of Software, vol.16, no. 5, **(2005)**, pp. 846-856
[4] Y. Zhang, H. Zhang, B. Fang, “Summary of Internet topology modeling”, Journal of Software, vol.15, no.8, **(2004)**, pp.1220-1226.
[5] BM Waxma, “Routing of multipoint connections[J]”, IEEE Journal on Selected Areas in Communications, vol. 6, no. 9, **(1988)**, pp. 1617-1622.
[6] G. Zhang, G. Zhang, “Association study of Internet network”, Journal of Software, vol. 17, no.3, **(200 6)**, pp. 490-497.
[7] B-M Waxman, “Routing of multipoint connections”, IEEE Journal of Selected Areas in Communication, vol.6, no. 9, **(1988)**, pp. 1617-1622.
[8] M. Doar, “A better model for generating test networks”, Proceedings of IEEE Global Internet, London, **(1996)**, pp. 86-93.
[9] K. Calvert, M. Doar , E. Zegura, “Modeling Internet topology”, IEEE Communication *Magazine* vol. 35, no. 6, **(1997)**, pp. 160-163.
[10] A. Medina, A. Lakhina, I. Matta, J. Byers, “BRITE: an approach to universal topology generation”, Proceedings of MASCOTS, Washington, **(2001)**, pp. 346-353.
[11] Y. Xu, “topology modeling based on large-area model”, Publishing House of electronics industry, Beijing, **(2011)**.
[12] X. Wang, X. Li, GC, “Complex Network Theory and Its Application”, Tsinghua University press,Beijing, **(2006).**
[13] R.Cohen, K,Erez, D,ben-Avraham, S.Havlin. Resiliense of the Internet to Random Breakdowns.Phy.Rev.Lett.85,4626, **(2000)**.
[14] A E Motter, “Cascade Control and Defense in Complex Network.Phys”, Rev.Lett, vol. 93, no. 9, **(2004)**,098701.
[15] V.Latora,A and M, Marchiori, “Efficient Behavior of Small-World Network”, Phys.Rev.Lett,**(2003)**,87.198701
[16] A E Motter, T. Nishikawa, Y C Lai, “Cascade-based attacks on complex networks”.Phys.Rev.E,**(2002)**,66:065102

Authors

Xu Ye. (1976-), received his ph.D degree in major of computer application technology in 2006 from Noreastern University, China. He is now working as a full professor in Shenyang Ligong University, China. And his research interests now include Complex Networks and Intelligent Systems.

