Collapse by Cascading Failures in Hybrid Attacked Regional Internet

Ye Xu[1] and Zhuo Wang

College of Information Science and Engineering,
Shenyang Ligong University, Shenyang China
xuy.mail@gmail.com

Abstract

To study the cascading failures and robustness of Internet, measuring topology of regional Internet with monitors is performed first. The mathematical transformation of measured results into matrix is introduced to set up a simulation platform for further experiments. By setting up various simulation parameters, we found that Internet is to some extent having the performances of highly resistance to random attacks and easily collapse while under intentional attacks. And in hybrid attack situations, Internet is also quite fragile no matter what ratio of intentional attacks over the random ones is. Besides, we find that networks with high loads would easily result in more damaged networks even under the same attacks.

Keywords: *Internet; cascading failures; random attacks; targeted attacks*

1. Introduction

Recently, plenty of research interests are found in studies of the resilience of scale-free network to random attacks or to targeted attacks on the highest degree nodes. It's found in most researches that scale-free networks are robust to random attacks but vulnerable to intentional attacks. Since a large percent of real-life networks have special features blending that of scale-free networks, i.e., biological networks, social relation networks, traffic networks and particularly Internet, it is necessary and essential for us to know the optimal guideline to re-design or alter the networks to a certain extent into one that are optimally robust against both types of attacks.

2. Preceding Studied Properties

2.1. Measuring Regional Internet

2.1.1. Measuring methods: 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 [1].

Static methods based on the BGP route table and the dynamic methods based on the active probing are the main ways to measure the router-level Internet topology [2]. And the static methods are gradually replaced by the dynamic ones due to their lack of the redundant routers measures [2].

[1] Our work is supported by the Liaoning Provincial Natural Science Foundation (201003676) and the Shenyang Natural Science Foundation (F10-205-1-26)

CAIDA, as one of dynamic measuring methods, could implement multi-monitor-measuring and consequently yield better measuring results [4] and [5], and was used in this paper.

2.1.2. Measuring results: Testing samples in this paper were generated from the measuring monitors dispersely located in the continents on the earth, and more than twenty of the monitors were employed. With the measured data, we first gather them together to form a complete testing sample. Then, for a better view and analysis, we made several incomplete testing samples, and they are sample(1) comprising data from only one monitors (arin monitor), and sample(2) from two monitors (arin, b-root), till sample(20) from twenty monitors.

Then we eventually get 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], and this is why we select as many as twenty-one monitors.

However, there is still no good approach to completely solve the problem of sampling bias except trying to include more sampling nodes at present, so we could not prove how much sampling bias is solved by using the twenty-one-monitor sample and. The key point is, the more monitors we use, the less the sampling bias would be. So the complete sample (the twenty-one monitor sample) is the primary testing sample in this paper, and the others are used for comparisons.

All testing samples belong to the router-level Internet samples.

2.2. Robustness researches in scale-free networks

Studies in [3, 6, 7, 8] found that properties of Internet topology are quite consistent to those of Scale-free networks. The mentioned properties are found in studies of frequency-degree power-law distribution, degree-rank power-law and CCDF(d)-degree power-law distribution. Spectra distributions studies in [3, 4, 5] also found similar nature of network topology between two given samples which gives great potential possibilities that robustness of regional Internet is supposed to be quite close to that of the scale-free networks since it is highly agreed in the relative research fields that networks' robustness are closely related to its topology.

In the scale-free networks, the degree distribution P(k), i.e., the probability of a node have k connections to other nodes, typically decreases as a power of k. In random attacks, it's found that the attack has little effect on the network since the randomly removed chosen node would have a low degree when a fraction p of the nodes and their connections of the scale-free network are removed randomly [7, 9, 10].

Removal in intentional way, however, is found to have great influences on the networks. Removal of a highly connected node in intentional attacks could produce a large effect, since such a node may hold significant fractions of the network together by providing connections between many other nodes and the integrity of the network topology would be sharply destroyed by removal of these nodes.

Numerical simulations suggest that scale-free network has clear nature to be highly robust to random attacks but extremely sensitive to intentional ones. We have reasonable ground to believe that regional Internet is supposed to have similar properties in robustness studies against attacks.

3. Robustness Evaluations to Attacks

3.1. Definitions of Simulation Environments

First we transform the measured data into a matrix ***M***, as is well known, ***M*** is a symmetrical matrix with elements equal to 1 where there is a connection between the nodes identified by the row and column of the matrix. And the matrix element equals to 0 where there is no links between the corresponding two nodes[11-13]. Then, we get ***M***:

$$M = \begin{bmatrix} 1 & r_1 & .. & r_n \\ r_1 & 1 & .. & .. \\ .. & .. & 1 & .. \\ r_n & .. & .. & 1 \end{bmatrix} r_i \in \{1,0\}. \tag{1}$$

We control attacks types by variable of attack degree *t*.

$$t \in [0,1]. \tag{2}$$

Setting attack degree *t*=1 means a complete random attack occurs, whereas *t*=0 is for that of a complete intentional attack, interpreted as attacking the nodes with the largest degrees intentionally in this context. Hybrid attacks will occur when t equals to value between [0, 1], and we could give controls how much random attacks weigh on the overall attacks by assigning different values to *t*.

We control the network load by variable of network load ratio *w*.

$$w \in [0,1). \tag{3}$$

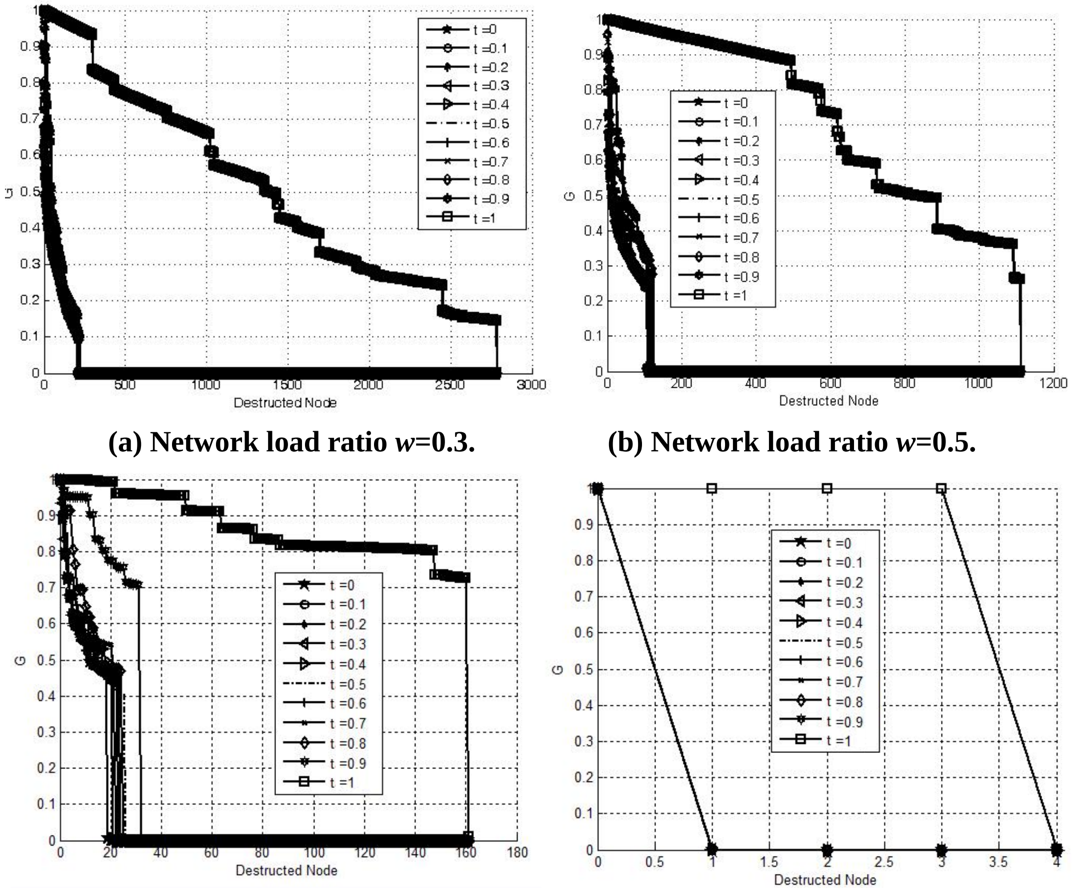
Setting network load ratio *w*=0 means the network is empty loaded, and there is no network flow on the current situation. When *w* is approaching to but not reaching 1, meaning the network load is getting heavier, more network flow is ongoing in the targeted network. Network load ratio *w* will never reaches 1 in this study, due to reasons that a fully loaded network is yet considered to be a collapsed one, there is no need to testify its robustness character.

Finally we set *N* as the number of the overall nodes in the target networks, and *N*' is the node size of the largest connected graph after removing fractions *p* of the original nodes by hybrid attacks. Then we set *G*=*N*/*N*' is the relative ratio of the largest connected graph over the original network, which is used to evaluate the collapse level of the network.

3.2. Simulation of Network Under Hybrid Attacks

First experiment of hybrid attacks against the targeted networks is performed. In the experiments, we set *N*=4000, meaning that there are 4000 nodes in the networks.

We set *t* equal to [0, 0.1, 0.2, .., 1], representing hybrid attacks from completely intentional attacks (*t*=0) to totally random attacks (*t*=1). When *t* belongs to [0.1, 0.2, .., 0.9], a hybrid attacks with different mix ratio of random attack over targeted attacks in the networks are constructed, trying to simulate the realistic attacks in the real world. Besides, we set *w* equal to [0, 0.1, 0.2, .., 1], representing various workload of the networks. The reason to construct networks with different load under hybrid attacks is that we are trying to simulate the real world attacks on Internet, as well as to get profound explanations of the relationship between the network robustness and the load of the same networks. In the following experiments, we choose three or four representative results to be presented in the paper. And some of the experiments are as follows.



(a) Network load ratio *w*=0.3.

(b) Network load ratio *w*=0.5.

(c) Network load ratio *w*=0.8.

(d) Network load ratio *w*=0.95.

Figure 1. Collapse of the Networks with Different Network Load under Hybrid Attacks

From the above figures, we find that Internet shows highly robustness against completely random attacks and is rather fragile to intentional attacks. This is quite consistent to what was found in studies of scale-free networks. The reason is that both Internet and scale-free networks have obvious power-law distributions properties, i.e., some nodes in the networks have large quantity of connections to others whereas the most nodes have relatively very few links shown as having low degrees. The target attacks over the high degree node certainly will result in large extent collapse of whole networks.

What surprises us most, however, is that Internet is also quite fragile to hybrid attacks no matter what ratio of intentional attacks over the random ones (almost in the level of that of completely intentional attacks). Which means although there might be minor target attacks, the effect over the networks robustness is quite notable.

3.3. Evaluations of the Network Robustness under Hybrid Attacks

We then give further explanations on the experiments results.

3.3.1. Under random attacks: As what is found in Figure 1(a)-(d), Internet is quite robust against random attacks. However, the robustness deceases along with the increment of network load ratio *w*.

When *w*=0.3, as is shown in Figure 1(a), according to the line with *t*=1, we find that only to randomly destroy nearly 37.5% percent of all *N*(*N*=4000 as is shown above) nodes, the networks would collapse to level of 50%, meaning only half of the networks still function normally where the other 50% is totally damaged. And when the destroyed nodes reach 75%, the networks is considered to be totally collapsed due to collapse level *G* reaches to more than 90%.

When it comes to a network with *w*=0.5 as is shown if Figure 1(b), we find that only to destroy nearly 18% percent of all *N* nodes, the networks would collapse to level of 50%. And when the destroyed nodes reach 30%, the networks is considered to be totally collapsed and the collapse level *G* reaches to more than 90%.

When *w*=0.8 as is shown if Figure 1(c), we find that only to destroy nearly 4% percent of all *N* nodes, the networks would collapse to level of 90%. And in Figure 1(d) with *w*=0.95, the destroyed nodes needed for collapse level *G*=0.9 is only 0.1%.

Although Internet is proved to be quite resistant to random attacks, it is obvious that the robustness of Internet would decrease sharply when network load ratio *w* is growing larger. Especially the networks under conditions when *w*>0.8, a minor random attacks would lead to a total collapse of the networks directly.

3.3.2. Under targeted attacks: As what is found in Figure 1(a)-(d), Internet is quite fragile to intentional attacks. And the robustness also deceases along with the increment of network load ratio *w*.

When *w*=0.3, as is shown in Figure 1(a), according to the line with *t*=0, we find that only to intentionally destroy nearly 2.5% percent of all *N*(*N*=4000 as is shown above) nodes, the networks would collapse to level of 50%. And when the destroyed nodes reach 5.75%, the networks is considered to be totally collapsed due to collapse level *G* reaches to more than 90%.

When it comes to a network with *w*=0.5 as is shown if Figure 1(b), we find that only to destroy nearly 2% percent of all *N* nodes, the networks would collapse to level of 50%. And when the destroyed nodes reach 2.5%, the networks is considered to be totally collapsed and the collapse level *G* reaches to more than 90%.

When *w*=0.8 as is shown if Figure 1(c), we find that only to destroy nearly 0.5% percent of all *N* nodes, the networks would collapse to level of 90%. And in Figure 1(d) with *w*=0.95, the destroyed nodes needed for collapse level *G*=0.9 is only 0.025%.

It is obvious that the robustness of Internet would decrease sharply when network load ratio *w* grows larger, even under intentional attacks. Especially the networks under conditions when *w*>0.8, a minor intentional or hybrid attacks would lead to a total collapse of the networks directly. The relationship between network load and robustness of networks is consistent to what we find in real world.

4. Conclusions

As is shown in the experiments, robustness of Internet is to some extent consistent to that of scale-free networks by the performances of highly resistance to random attacks and great fragilities to intentional attacks. However, when we perform further experiments on Internet by removal of nodes in way of hybrid attacks, we found that, which quite surprise us, Internet is also quite fragile to hybrid attacks no matter what ratio of intentional attacks over the random ones is (almost in the level of that of completely intentional attacks). Which means although there might be minor target attacks, the effect over the networks robustness is quite notable.

Finally, the relationship between network load and robustness of networks is studied, and we find that networks with high loads would easily result in more damaged networks even under the same attacks.

References

[1] M. Faloutsos, P. Faloutsos and C. Faloutsos, "On power-law relationships of the Internet topology", ACM SIGCOMM Computer Communication Review, 29(4):251-262 **(1999)**.

[2] Y. Jiang, B. X. Fang and M. Z. Hu, "An Example of Analyzing the Characteristics of a Large Scale ISP Topology Measured from Multiple Vantage Points", Journal of Software, 16(5):846-856 **(2005)**.

[3] G. Siganos, M. Faloutsos, P. Faloutsos and C. Faloutsos, "Power laws and the AS-level Internet topology", IEEE/ACM Trans. on Networking, 11(4):514-524 **(2003)**.

[4] N. Spring, R. Mahajan and D. Wetherall, "Measuring ISP topologies with rocketfuel", ACM SIGCOMM Computer Communication Review, 32(4):133-145 **(2002)**.

[5] B. M. Waxman, "Routing of multipoint connections", IEEE Journal on Selected Areas in Communications, 6(9):1617~1622 **(1988)**.

[6] D. Centola, "Failure in Complex Social Networks", Journal of Mathematical Sociology. 33(1):64-68 **(2009)**.

[7] J. Wang, Y.-H. Liu, Y. Jiao and H.-Y. Hu, "Cascading dynamics in congested complex networks", Euro. Phys. J. B. 67, 95–100 **(2009)**.

[8] P. Li, B.-H.Wang, H. Sun, P. Gao and T. Zhou, "A limited resource model of fault-tolerant capability against cascading failure of complex network", Euro. Phys. J. B. 62, 101–104 **(2008)**.

[9] X. H. Xiao, G. W. Ye, B. Wang and M. F. He, "Cultural dissemination in a complex network", Physica A. 388(5):775-779 **(2009)**.

[10] J. W. Wang and L. L. Rong, "Attack vulnerability of scale-free networks due to cascading failures", Physica A. 387:6671–6678 **(2008)**.

[11] J. W. Wang and L. L. Rong, "A model for cascading failures in scale-free networks with a breakdown probability", Physica A. 388: 1289-1298 **(2009)**.

[12] Z. J. Bao, Y. J. Cao and G. Z. Wang, et. al., "Analysis of cascading failure in electric grid based on power flow entropy", Physics Letters A. 373: 3032-3040 **(2009)**.

[13] J. Ash and D. Newth, "Optimizing complex networks for resilience against cascading failure", Physica A. 380: 673-683 **(2007)**.

Authors

Ye Xu

Ph.D, associate professor. His current research interests include large-scale networks and complex dynamic systems.

Zhuo Wang

Associate professor. His current research interests include complex networks and data mining systems.