Research on The Static Robust and Vulnerability of Internet on The Level of Isp

Fu Yun
Postgraduate College, The Academy of Equipment Command & Technology
Beijing, China

Zhao Hongli,Yang Haitao
The Academy of Equipment Command & Technology,
Beijing, China

***Abstract*—A metric called S -resilience is comed up with aimed at the fact that the existed metics which evaluate the robust and vulnerability have disadvantages. Evaluate the measured ISP network of Internet with S -resilience, compared the performances to the same scale random graphs and scale-free networks. The result is that the metric is feasible in charactering the performances, which is available to evaluate the ability that networks own on condition of failure and attacks. The simulation shows that the ISP networks are robust in event of failure as well as vulnerable under the attacks. they both have critical values under the two troubles.**

Keywords- Robust; vulnerability; failure; Attack

I. INTRODUCTION

The network robust belongs to the research field of importance of network complexity.More and more researchers pay much attention to the question. Callawany and Cohen applied percolation theory to analysis the nework robust[1-3], Valente reduced that the degree at best have three values in case of the failure and the attack[4]; Bollobás and Riordan analyzed the robust and the vulnerability of the scale-free network by random graph theory[5]. Holme studied the delete strategy based on the betweenness centrality[6]. In a typical network robust analysis problem, the focus is the possibility of maintaining the structure when the random failure and the intended attack happened. The study of robust is mostly considered the ability of normal working of network when the network undergone the failure and attack.

Despite the rewarding discuss on the effective elements of the network structure robust is implemented in aspects academic analysis and attack strategies. The node number and the average path length of greatest left component are commonly used to evaluate the robust. There is lack of a compositive metric and the research field is mostly focus on the scale-free network.

The static robust of network is the ability to maintain its function as the loss of nodes or edges not affects other nodes and edges, which is defined in order to distinguish the continuing dynamic robust. The dynamic robust is the ability to maintain its function as the loss of nodes or edges affects other nodes and edges, such as, other nodes invalid because of overload or virus.

The paper first put forward S-resilience of network metric looser than the tenacity owing to the idea of tenacity, secondly, compared the static robust of the two ISP networks using the new metric with the same scale network-random graph and the scale-free network.. There are four kinds of methods that invalided the nodes and the relative edges, failure, degree-based, betweenness-based, efficiency-based, the simulation shows that the certain networks all exist a critical value.

II. THE INDEX DEFINITION OF ROBUST

A. Tenacity[7]

$T(G)=\min\left\{\frac{|S|+\tau(G-S)}{\omega(G-S)}: S\subseteq V(G)\right\}$, S is a subset of node set, $G-S$ denotes the graph removed S set form the graph G . $\tau(G-S)$ denotes the nodes of the greatest component, $\omega(G-S)$ expresses the number of $G-S$. $|S|$ expresses the number of nodes or edges.

Tenacity takes the cost damaged the network and the connected branches and the greatest component into account. Tenacity gives consideration both the damaged and the left aspects at the same time, which can more profoundly depict the vulnerability of network on a whole view, it is a preferable metric.

B. Efficiency[8]

Efficiency : $E=\frac{1}{n(n-1)}\sum_{i\neq j}\frac{1}{l_{ij}}$, that is the summary of the inverse of the average shortest path length between any two nodes, which shows the easiness level of average communication.

C. S-resilience of network

Tenacity considers both the “cost” and the “fruit”, the ‘cost’ is the size of S and the greatest left component, as the great left component means that “attacker” is not too successful ,the ‘fruit’ is the left branches.(Much amount of left branches makes difficult to rebuild network).Although this idea is available to character the connection of network., the definitive range of the projective relationship of tenacity is node set, the value range is a value. when the scale of network is small, the tenacity can be calculated by the searching method through the permutation and combination of each node. For example, a network contains 5 nodes, the calculation is $C_5^1+C_5^2+C_5^3+C_5^4+C_5^5=31$, when the number of nodes adds, the amount of calculation is huge.

Published by Atlantis Press, Paris, France.

The definition is unpractical while the scale of network is great.

The paper defines the resilience when the node set S is disable, which can evaluate the effect in which the certain attack result.

Definition 1: S -resilience is that $R_S = \frac{\tau(G-S)}{n} \cdot \frac{|S|+\tau(G-S)}{l(G-S)}$, $G-S$ denotes the graph removed S set form the graph G . $\tau(G-S)$ denotes the nodes of the greatest component, $l(G-S)$ expresses the average shortest path of the greatest component of $G-S$. $|S|$ expresses the number of nodes.

S -resilience considers not only the "cost" but also the "fruit", which is the same as tenacity, but the "fruit" is the average shortest path of the greatest component, not the number of the branches after attack. It is broken out the restriction of the minimum, looser than tenacity, which not just decrease the amount of the calculation but more of pertinence in the way of attack. It can decide which is more effective when the number of nodes of disable is equal. To the erector of the network, they can rebuild the network with protecting or rapairing the relative nodes in terms of the change of the resilience, which may be the efficient method to regain the function of the network. It is called resilience as for the efficiency of repairing.

III. THE NETWORK MODEL AND THE WAY OF DISABLE

A. The way of disable

Divide the ways of the node disable to two, failure that random choose a part of nodes and the edges connected to these nodes and the intended attack that choose the given nodes and the edges connected to these nodes, the given nodes on which based betweenness, degree, vulnerability. The functional index metrics are efficiency and the S -resilience the paper defined.

1)Degree

Degree is the attribution that simple but important of a single node. The definition of degree is the number of nodes connected to the node.

2)Betweenness

The betweenness is the ratio of the shortest path through which passing the node. Analogously, there is the definition edge betweenness also.

3)Vulnerability

The vulnerability of node is : $V_i = 1 - E_i / E$, E_i is the network efficiency after removing the node i .

B. Network model

The network model of the paper simulating both come from the measuring item Rocketfuel, which is called N3257 and N4755 as the numbers of the measuring area. The characters of the two networks are in the table 1.

The same scale random and scale-free networks which have the same number edges and nodes as N3257 and N4755 are built in order to compare the network static robust with the varies networks.

TABLE I. THE CHARACTERS OF N3257 AND N4755

Number	Numbers of nodes	Numbers of edges	The average shortest path	Average degrees	Clustering coefficient
N3257	411	653	5.5273	3.1776	0.0078
N4755	41	68	2.9805	3.3171	0.0829

IV. SIMULATION AND ANALYSIS

The diagrams show us changing curved shapes, which demonstrate that as the rate f of removed nodes and edges taking up original nodes and edges enlarges.

A. The simulation and analysis of N3257

From the diagram 1, the network efficiency and resilience are both decreased slowly under the failure, not until the ratio reachs 0.7,does the efficiency and resilience reaches zero. While in the intended attack(based on degree and betweenness), the efficiency and resilience reaches zero at the time the removes nodes ratio less than 0.1. Diagram 2 shows, as for the same scale random graph, the speed of change is faster than N3257 under the failure, although the performance at last reaches zero under the intended, the speed is much gradual, when compared with the N3257, the removed nodes must have arrived at about 0.3 provided that the network is fall apart., three times of N3257. All curves in diagram 3 have the same currents with the diagram 1, which confirms that N3257 is more tend to scale-free network. Diagram 4 shows that the attack bases on degree is more efficient than the attack bases on vulnerability.

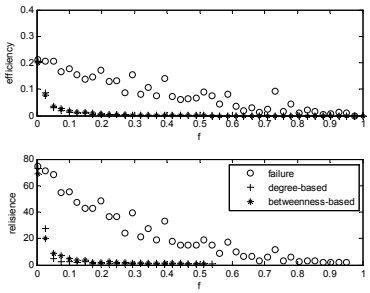

Figure 1. Change curves of N3257 on efficiency and resilience

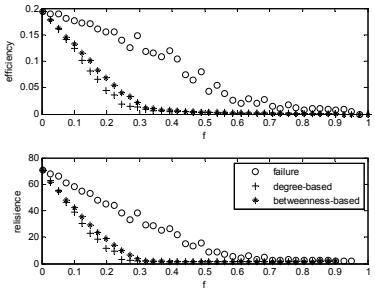

Figure 2. Change curves of same scale random graph on efficiency and resilience

N3257 have been fall apart when f close to 0.1, we believe 0.1 is the critical value, the network no longer has any communication. N3257 is robust when failure, but is vulnerable when undergoing intended attacks.

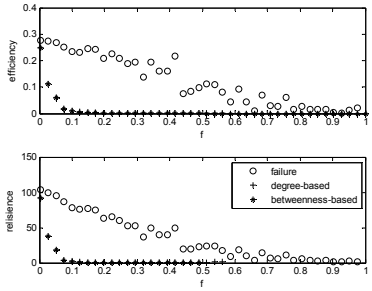

Figure 3. Change curves of same scale scale-free network on efficiency and resilience

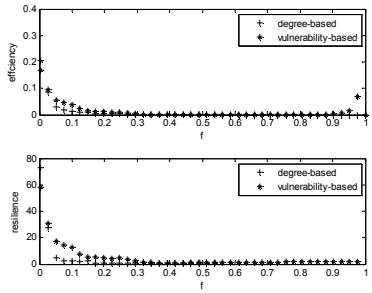

Figure 4. Change curves of N3257 degree-based and vulnerability-based attacks on efficiency and resilience

B. The simulation and analysis of N4755

Diagram 5 shows that the characters are not as stable as N3257 when failure, but ascend or descend, mostly, performs decreased. While under the intended attack, N4755 is vulnerable as well, the critical value is about 0.2, the cricital value of the same scale random graph is about 0.6, same times with the N3257. In the same scale scale-free network , the critical value is about 0.4, it is because that the degree distribution of scale-free takes on laws distribution ,as the scale of network small, the laws rule cannot appear. We can see form the diagram 8, the changes the efficency and the resilience under degree-based attack and vulnerability-bases attack are general identical, have no more difference ,that is related to the small scale of N4755.

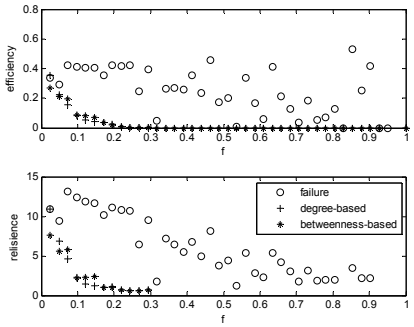

Figure 5. Change curves of N4755 on efficiency and resilience

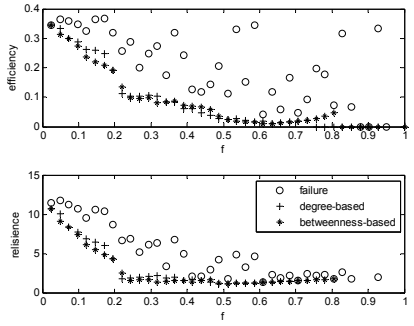

Figure 6. Change curves of same scale random graph on efficiency and resilience

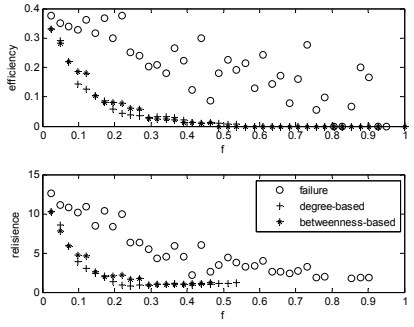

Figure 7. hange curves of same scale scale-free network on efficiency and resilience

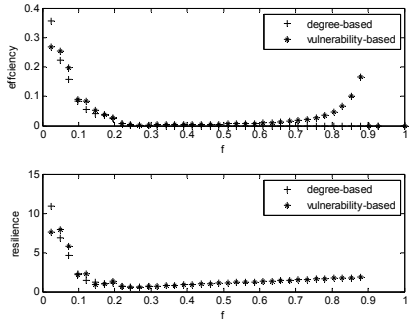

Figure 8. Change curves of same scale scale-free network on efficiency and resilience

In the simulation , the efficiency and the resilience changed almost consistently, that shows the resilience is a feasible metric in depicting the performance of network, but it considers more elements than the efficiency, more practical on the communication ability that the left greatest component to which is more paid attention by the erector and attacker of networks. The two networks both have robust on the condition of failure, as far as the attacks is concerned, the network is vulnerable, the critical value is 1/3 times as the same scale random graph. The change patterns are mostly according to the change that the same scale-free networks, which tests the thesis that the ISP networks are belong to the scale-free networks, but the performance is more close to the performance on which scale-free network take as the scale of the network is becoming greater and greater.

V. CONCLUSION

We put forward a metric called S -resilience based on the idea of the "cost" and the "fruit", furthermore, evaluate the robust and the vulnerability on the two measured ISP network. The result is that the S -resilience is effective in evaluating network characters which contains more elements affect the performance on condition of failure and attack. The simulation shows that the ISP networks are robust in the event of failure, while in the event of attacks, they are vulnerable. The critical values are 1/3 times of the same scale random graph.

REFERENCES

[1] Newman M E J. Assortative mixing in networks [J]. Physical Review Letters, 89, 208701, 2002.

[2] P.Erdös, A.Renyi. On the evolution of random graphs. Publications Mathematicae Inst.Hungar.Acad.Sci,1960,17-61.

[3] P.Erdös, .Renyi.On the strength of connectedness of a random graphs.Acta.Math.Acad.Sci.Hungar,1961,12:261-267.

[4] L.A.Adamic, B.A.Huberman, Power-law distribution of the world wide web, Science,2000,287(5461)2115.

[5] H.Jeong, .Tombor, .Albert, .Oltvai, .Barabási.The large-scale organization of metabolic networks.Nature406,2000,651-654.

[6] Shi Dinghua,Network－the new path to explore complexity. The transaction of system engineering. 2005,20(2):115-120.

[7] Cozzens M,Moazzami D,Stueckle S.The Tenacity of a Graph.Seventh International Conference on the Theory and Applications of Graphs,Wiley,New York,1995,1111-1122.

[8] V.Goldshtein, G.A.Koganov, and G.I.Surdutovich. Vulnerability and hierarchy of complex networks. Cond-mat/0409298,2004.

Published by Atlantis Press, Paris, France.