TELKOMNIKA, Vol. 11, No. 9, September 2013, pp. 4896~4903
ISSN: 2302-4046

Network Invulnerability Assessment Technology based on the ENI

Yuanni Liu*, Hong Tang, Guofeng Zhao, Yunpeng Xiao, Chuan Xu
The School of Communication and Information Engineering, ChongQing University of Posts and Telecommunications, No. 2, Chongwen Road, Nanan district, 400065, ChongQing, China,
+86-23-62461032
*Corresponding author, e-mail: yuanniliucq@163.com

Abstract

In this paper, we have proposed a network invulnerability assessment technique based on the entropy of node importance (ENI) determined by the node betweenness combined with node degree, which can measure the network invulnerability dynamically. Simulation results show that the ENI network entropy can accurately change its values as the network nodes removed deliberately or randomly from the network, and ENI can estimate the network invulnerability accurately, as well as can reflect the damage degree of the network according to network entropy.

Keywords: *network invulnerability, network entropy, power-law distribution, node betweenness*

1. Introduction

The research on network invulnerability aims to discover the weakness and security risk of the network and to estimate the network ability to resist the attacks, and to improve network invulnerability at last. In order to do this, we have to quantize the network invulnerability, that is, to set up a measure for it. Most of the traditional network invulnerability assessment algorithms were based on the connectivity of a graph, which are complex and inefficient.

The Internet develops fast, with the feature that node degree distribution followed the Power-Law distribution [1-2], which is $P(K) = C * K^{-\lambda}$. Networks followed power-law distribution are scale-free networks, in which most of the nodes own few connections while a few number of the nodes take account to most of the connections. The uneven distribution of the node degree result to the fact that network are fragile to deliberate attacks. In fact, the scale-free feature is a characteristic of homogeneous, which can reflect network invulnerability in some degree. Recently, entropy [3] has received increasing interest in complex system theory as a physical quantity to describe complex system structure, it has been an important researching tool for complex system. Ferrer reobtained optimal network [4] with the method of network optimization. They calculated the entropy value of network degree, and then they found that different kinds of networks had obvious different entropy value. In [5], it proposed the method to study the scale-free of complex network with the concept of network structure entropy.

This paper proposed a network invulnerability assessment technology called ENI (Entropy of Node Importance), the contributions of this paper are:

(1) We defined node importance B_i which combines node degree and node betweenness to compute the network entropy. The network entropy based on node importance B_i can show the network homogeneity change accurately when the network nodes were removed deliberately or randomly than that of the entropy based on node degree importance I_i [3].

(2) The simulation results showed that ENI can estimate the network invulnerability accurately, and can also reflect the damage degree of the network according to network entropy.

The rest of the paper is organized as follows: in section 2, we review the related work; in section 3, we propose our methodology of ENI; section 4 analysis the performance of ENI in both small and large scale networks; and at last; section 5 conclude this paper.

Received April 19, 2013; Revised May 29, 2013; Accepted June 10, 2013

2. Related Work

The invulnerability of a network is defined as the largest removal ratio of node or edge in the network under some constraints of network connectivity. Albert [6] pointed out that “robust yet fragile” is a basic characteristic of complex network, and scale-free network has stronger fault tolerance than stochastic network, but worse anti-attack ability to vertex degree: the network will be paralyzed if only 5% of the nodes were removed. Cohen et, al. [7, 8] transformed the network invulnerability into seepage problem, they studied this problem analytically using the percolation theory, and they proposed a criterion to calculate critical collapse probability f_c, and drew a conclusion that the critical removal ratio of network collapse $f_c = 1-1/(k_0 -1)$. Wang [9] studied the problem about entropy optimization. They found that if the network is more inhomogeneous, it will have stronger invulnerability. So, the problem about invulnerability optimization to random failure is transformed into the problem about degree distribution entropy optimization. They studied the invulnerability to random failure using the model of entropy optimization, and then they found the change law of scale-free network invulnerability with specified minimum degree. When the network scale N is enhanced, it will be stronger. When the scaling exponent K is enhanced, it will be decreased, and if the network average degree $<k>$ is enhanced, it will be stronger. Hou [10] proposed four measures of invulnerability based on network connectivity, but it should take account of more network topology characteristic factors. He [11] improved Albert algorithm during the calculations of the network connectivity after various destructions and the probability of each type of damage occurring in the real world, and the network invulnerability can be measured, but it is difficult to obtain the probability when the network suffers from various attacks and to access this parameter more conveniently and more accurately. Meng [12] presented a mathematically tractable model of node motion to derive a precise relation between mobility and connection stability, and they improved the first order energy consumption model with dynamic clustering firstly and built a incidence matrix to depict the connectivity of the network nodes in a dynamic network model, and simulated the network invulnerability related to time. Yang [13] analyzed the current measure methods of complex network invulnerability and the invulnerability of instant messaging network topology by analytic hierarchy process, and presented the main influencing factors of instant messaging network topology.

Wu [14] analyzed the inhomogeneity of scale-free network topology structure with network structure entropy. By introducing degree-rank function, it analytically put forward the scale-free network structure entropy. Research shows that the scale-free network structure entropy will take minimum value when scaling exponent equal to about 1.7 with specified network scale minimum degree. When scaling exponent is over 1.7, the scale-free network structure entropy will monotonically increasing with the scaling exponent. Wu also proposed two new measurements [3] of complex network invulnerability; they are fault-tolerability and anti-attack degree. They are comprehensive exponents without taking the dispersion of degree value into account. But Wu can't break the framework of Albert, in other words, they only studied the invulnerability with different attack pattern to different degree distribution network. Wu proposed the network entropy [3, 14] to measure the scale-free feature of the network, it pointed out that the entropy is a measure of the system ‘ordered’, and if the links are built randomly, with almost equal importance of the nodes, then the network is “disordered”; on the other hand, if it is a scale-free network, with a few high degree key nodes and a lot of low degree hub-nodes, that is to say ,the node degrees are greatly different, then the network is “ordered”. Network entropy is in this way to measure this kind of “order”.

In [3], the network entropy was defined as:

$$E = -\sum_{i=1}^{N} I_i \ln I_i \tag{1}$$

Where I_i is the importance of node i, which is defined as follows:

$$I_i = k_i / \sum_{i=1}^{N} k_i \tag{2}$$

Where *N* is the network size, k_i is the degree of node *i*, and *i* means the percentage of degree *i* taken account to the total degree of the nodes in the network., with the supposition that K_i >0.

The network entropy in [3] can depict the network scale-free feature properly in some degree, but in actual network, degree is not the only measurement of the node importance. In this paper we proposed a new network entropy based on node importance B_i, which will be introduce in section 3.

3. Network Entropy based on ENI

3.1. Network Entropy based on Node Degree Importance

In [3], though node degree can determine the importance of a node in some extent, the importance of two nodes with same degree may be considerably different. For example, in Figure 1, node 5 and node 6 each has the same degree of 4, but when removed from the network separately, the influence to the network is greatly different: the removal of node 5 will result to nodes 1, 2, 3 and 4 be apart from the network, while the removal of node 6 will make the network be divided into 4 separate parts in consequence. The reason is that transmission in the network are basically along the shortest path, and the more number of the shortest paths through a node, the more important of the node in the network.

Concerned to the fact that the transmission in a network along shortest path tree, in order to depict the node importance, [15] proposed node betweenness, which is defined as (3).

$$B_i = \sum_{j,k \in N} \frac{n_{jk}(i)}{n_{jk}} \qquad (3)$$

Where n_{jk} is the number of the shortest paths between node *j* and *k*, and $n_{jk}(i)$ is the number of the shortest paths between node *j* and *k* that through node *i*. The node betweenness is the ratio of the shortest paths through node *i* and the total number of the shortest paths which shows the importance of a node in the network. The node betweenness is more efficient than node degree to estimate the importance of a node.

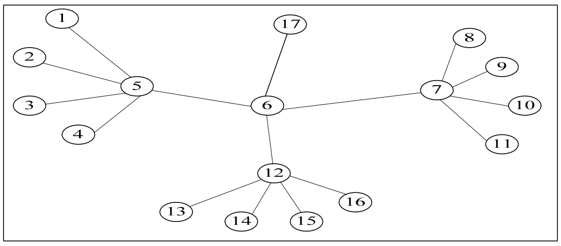


Figure 1. Network Topology

But the betweenness proposed in [15] only make sense in a connected network, the node betweenness will be incomputable when the shortest paths decreased as the increment of the connected components because of the network is unconnected. Extremely, when the network is divided into *N* isolated nodes, it is difficult to compute the node betweenness using Equation 3. In this paper, we define node importance in (4).

$$B_i = \frac{2(\sum_{j,k \in N} n_{jk}(i) + d_i + 1)}{N(N+1)} \qquad (4)$$

In our definition, the importance of node *i* is a ratio between the number of shortest paths through node *i* added (d_i+1) and $(N(N+1))/2$. Where (d_i+1) is the degree of node *i* (include the link to itself), and $n_{jk}(i)$ is the shortest paths through node *i*. $(N(N+1))/2$ is the number of the shortest paths in a completely connected network. In this way, we can estimate the node importance as the network topology changed by the removal of some nodes or edges.

By our means, if a node is isolated, the node importance is $2/(N(N+1))$, and the node importance computability is assured, and if a node importance is equal to $2/(N(N+1))$, then the node is an isolated node, which can be judged easily.

The importance in our method combines node betweenness and node degree to determine node importance. In this way, we can find out the isolated node in the network easily, and the network heterogeneous will be showed clearly.

3.2. Network Entropy in ENI Technology

In our ENI technology, we will first compute the node importance B_i according to Equation 4, and then the network entropy is shown as (5).

$$E = -\sum_{i=1}^{N} B_i \ln B_i \quad (5)$$

By analysing the network entropy, the even network, with all of node linked to all the other nodes in the network, in which all the nodes have the same shortest path number of N, then B_i=2/(N+1), and

$$E_{\max} = -\sum_{i=1}^{N} \frac{2}{N+1} \ln \frac{2}{N+1} \quad (6)$$

The network entropy is largest. While the star network is the most heterogeneous, for the sake of simplicity, we assume all the other nodes linked to the first node, then:

$$B_i = \begin{cases} 2/N, i = 1 \\ 2/N^2, 2 \le i \le N \end{cases} \quad (7)$$

The entropy of the star network is:

$$E_{\min} = -\left(\frac{2}{N} \ln \frac{2}{N} + \frac{2(N-1)}{N^2} \ln \frac{2}{N^2}\right) \quad (8)$$

4. Simulation Analysis

In this section, first we will illustrate how our technology works through the analysis of how the network entropy is changed compared to the entropy in [3] as the node was removed both randomly and deliberately in small network, and then we will analysis the performance of ENI in large scale network.

4.1. Entropy in Small Scale Network

The topology of small scale network is as shown in Figure 2.

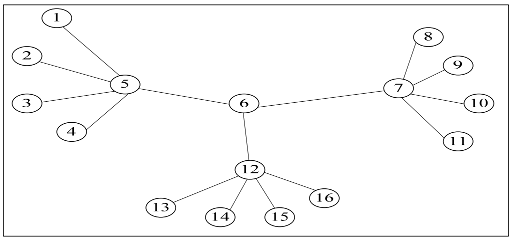


Figure 2. The Topology of Small Scale Network

According to Figure 2 the correspondent K_i, B_i, I_i are computed, as shown in Table 1 Consequently, the initial entropy based on node degree importance (E_{11}) and in ENI (E_{12}) are:

$$E_{11} = -\sum_{i=1}^{16} I_i \ln I_i = 2.487$$

$$E_{21} = -\sum_{i=1}^{16} B_i \ln B_i = 1.9$$

4.1.1. Analysis of Network Entropy under Random Node Removal

We randomly chose node 6 to be removed, and the topology will be as shown in Figure 3.

Table 1. Different Values of Node in Small Scale Network

i	1	2	3	4	8	9	10	11	13	14	15	16	5	7	12	6
K_i	1												5			3
B_i	2/17												15/34			91/136
I_i	1/30												1/6			0.1

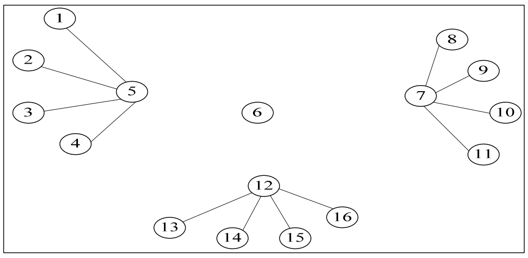


Figure 3. Network Topology after Node 6 is Removed

The correspondent entropies of the network are:

$$E_{12} = -\sum_{i=1}^{15} I_i \ln I_i = 2.485$$

$$E_{22} = -\sum_{i=1}^{16} B_i \ln B_i = 0.4973$$

Compared E_{12} to E_{11}, the network entropy is changed weakly after the removal of node 6 from network, in which the variance ratio is only 0.08%, while the variance ratio in ENI is up to 73.8%. In fact, the removal in the actually network will result to the network be divided into four connected components, and the communication capability will be decreased significantly. From the above analysis, the network entropy based on degree importance is less sensitive to network topology changed than that of the ENI.

4.1.2. Analysis of Network Entropy under Deliberate Node Removal

Under the deliberate attack, we first chose the node with highest degree to remove. In Figure 2 node 5, 7, 12 each has the same highest degree of 5, and each of the node is equivalent to network topology. The network topology will be Figure 4 after we removed node 5. In this condition, the network entropies correspondent to node degree importance and ENI respectively are:

$$E_{13} = -\sum_{i=1}^{11} I_i \ln I_i = 2.122$$

$$E_{23} = -\sum_{i=1}^{16} B_i \ln B_i = 1.1444$$

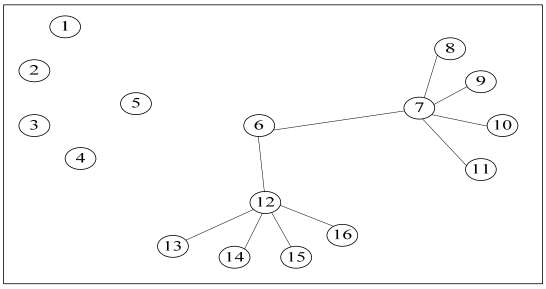


Figure 4. Network Topology after Node 5 is Removed

Compared E_{13} to E_{23}, both entropies based on degree importance and ENI are reduced after the removal of node 5, while the descender in ENI is 39.7%, larger than the descender based on node degree importance entropy which is 14.7%. Compared the removal of node 5 to node 6, the network communication capability based on the node 6 removal is obviously decreased significantly than that of the removal based on node 5, as well as the network homogeneity. As a result, the network entropy descender should be larger in the network entropy based on the removal of node 6 than that of node 5, and ENI is consistent to this case, while the entropy based on node importance is inconsistent to the removal of node 6 compared to node 5.

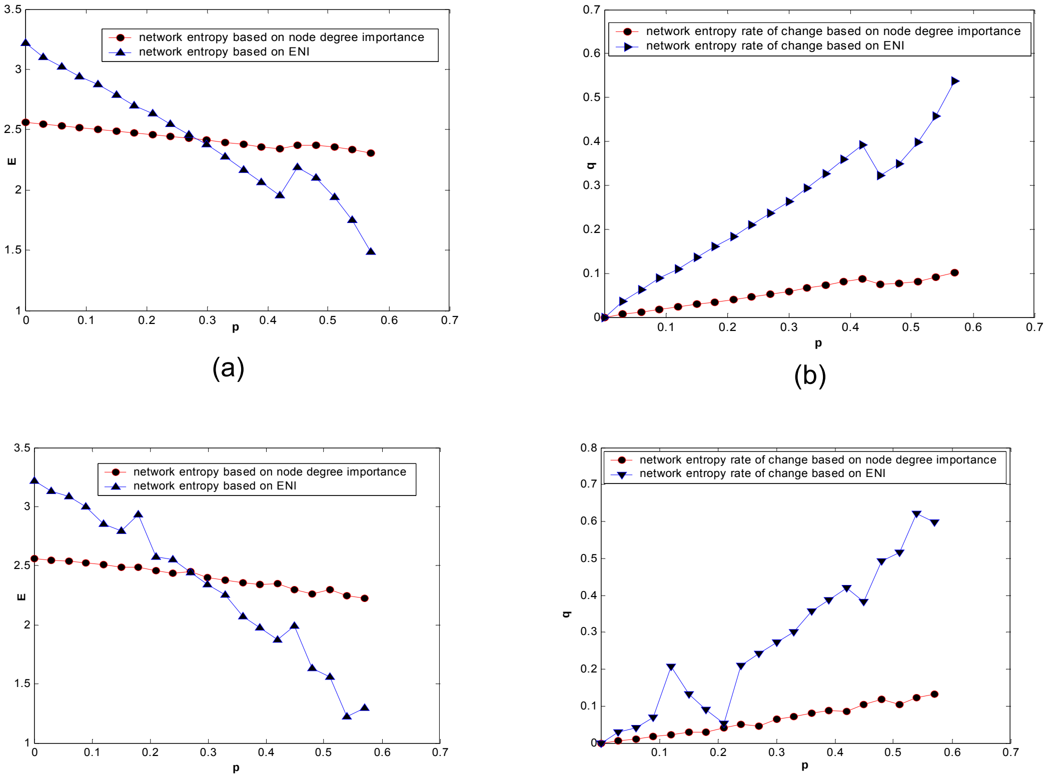
In a word, ENI is more accurate to evaluate network homogeneity and can dynamically reflect the network damage degree.

4.2. Simulation Results in Large Scale Network

In this section, we will find out how the two types of network entropies will be affected under both deliberate and random node removal in large scale network. The simulation environment is Matlab 6.5, our scale free network topology, i.e., graph with an algebraic distribution of degree $p(k) \sim k^{-\lambda}$, with $\lambda = 3$ [1], is generated artificially according to the BA model [2]. In both cases we have constructed networks with *N*=500, and *M*=1494. We will observe the entropy to explore how the network will be influenced as a function of p, which is the percentage of removed nodes in the network.

Figure 5 shows the results of network entropies and the network entropy variations as a function of p respectively. Figure 5(a) shows different network entropies as a function of p under deliberate removal of the nodes, and both of the entropies are decreased as p is increased, while the entropy based on node degree importance is changed in a small range from 2.3038 to 2.5332, and the entropy in ENI is altered in the range from 1.4894 to 3.0224. Figure 5(b) shows in deliberate removal, the entropy variance ratios increased as p is increased, from which, we can also find out that the network entropies of ENI changed evidently greater than that of node degree importance.

Figure 5(c) shows different network entropies as a function of p under random removal of the nodes, in one hand, the curve of the entropy of ENI fluttered, which showed the fact that the network entropy of ENI is changed randomly, while the entropy of node degree importance is decreased almost slightly; on the other hand, as the nodes were randomly removed from the network, both of the entropies are decreased as p is increased, while the entropy based on node degree importance is changed in a small range from 2.2254 to 2.5637, and the entropy in ENI is altered in the range from 1.221 to 3.2222. Figure 5(d) shows in random removal, the entropies variance ratio as *p* is increased. In Figure 5(d), network entropy of ENI is changed randomly, which is a great evident of the network topologies changed randomly as the nodes were removed randomly from the network. From the curve of the network entropy of node degree importance variance ratio in Figure 5(d), we can hardly draw the conclusion as that of ENI.



(a) (b)

(c) (d)

Figure 5. The Variance of Network Entropies in Large Scale Network

From the simulation in both small and large scale network, we can draw the conclusion that the entropy in ENI is more dynamical and is consistent to the change of network homogeneity, which can exhibit the network invulnerability efficiently.

5. Conclusion

Recently, great efforts were devoted into the research of network invulnerability assessment, and most of them are based on the network connectivity, with high computation complexity. Most of the actual complex network are followed the scale-free characteristic with power-law node degree distribution, which is a performance of the network heterogeneity. The heterogeneity is that most of the nodes have a few of connections, but a few of the nodes own a great number of connections. The more heterogeneous of a network, the more invulnerable it is. The heterogeneity of the network can be represented by network entropy. In this paper, we proposed a network entropy named ENI to assessment network invulnerability, which combined node degree and node betweenness to determine the node importance. The simulation in both small and large scale networks showed the results that our ENI is efficient to estimate network heterogeneity and is dynamically consistent with it when the network topologies are changed. Obviously, the ENI is efficient to assessment the network invulnerability. In the future, we will implement our ENI technology to estimate network invulnerability, and propose effective protective measures.

Acknowledgements

This work was supported by the CQUPT Dr. Start-up Fund Research(A2011-48), Natural ScienceFoundation of CQUPT(A2012-83),National Program on Key Basic Project(973 program: 2012CB315803), National Natural Science Foundation of China(641040044, 60873079), the Natural Science Foundation of ChongQing(CSTC2009BA2089).

References

[1] Faloutsos M, Faloutsos P, Falouts SC. On power-law relationships of the Internet topology. *ACM SigCOMM Computer Communication Review*. 1999; 251- 262.

[2] Barabasi AL, Reka Albert, Hawoong Jeong. Scale-free characteristics of random networks: the topology of the world wide web. Physica A: *Statistical Mechanics and its Applications*. 2000; 69- 77.

[3] Jun Wu, Yue-Jin Tan. Study on measure of complex network invulnerability. *Journal of Systems Engineering*. 2005; 128-131.

[4] R Ferrer, RV Solé. Statistical Mechanics of Complex Networks. *Springer-verlag.* Berlin Heidelbeng. USA. 2003.

[5] Yue-jin Tan, Jun Wu. Network Structure Entropy and Its Application to Scale-free Networks. Systems Engineering-Theory & Practice. 2004; 1-3.

[6] R Albert, H Jeong, AL Barabási. Error and attack tolerance of complex networks. *Nature*. 2004; 388-394.

[7] Gerald Paul, Sameet Sreenivasan, H Eugene Stanley. Resilience of the Internet to random breakdowns. Physical Review Letters. 2005; 4626-4628.

[8] Dorogovtsev SN, Mendes JF. Comment on Breakdown of the Internet under intentional attack. *Phys. Rev.Lett.* 2001; 3682- 3685.

[9] Wang Bing, Huan-wen Tang, Chong-hui Guo. Entropy Optimization of Scale-free Networks Robustness to Random Failures. *Physical A: Statistical Mechanics and its Application*. 2006; 591-596.

[10] Lvlin Hou, Gang Liu, Songyang Lao. *Measures of network topology invulnerability*. International Conference on Applied Robotics for the Power Industry. 2012; 1038-1040.

[11] Shaojun He, Jin Cao, He Wei. *A measure method for network Invulnerability Based on Improved Albert Algorithm*. International Conference on Instrumentation, Measurement, Computer, Communication and Control. 2011; 812-815.

[12] Liming Meng, Kai Zhou, Jingyu Hua. *Connection Stability AnalyzeBased on Dynamic Clustering Algorithm for Mobile Ad hoc Network*. WRI International Conference on Communications and Mobile Computing. 2009; 97-100.

[13] Songtao Yang, Zongli Zhang. Entropy weight method for Evaluation of Invulnerability in Instant Messaging Network. International Conference on Internet Computing for Science and Engineering. 2009; 239-243.

[14] Jun Wu, Yue-Jin Tan, Hong-zhong Deng. Heterogeneity of Scale-free Network Topology. Systems Engineering-Theory & Practice. 2007; 101-105.

[15] Freeman LC. Centrality in Social Networks Conceptual Clarification. *Social Networks*. 1979; 215-239.