http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (9): 1868-1872, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.1868.1872
© 2013 Asian Network for Scientific Information

Entropy Optimization of Scale-free Networks Robustness to Targeted Attack

Zhang Feiyun
College of Electrical and Information Engineering, Xuchang University, Xuchang, 461000, China

Abstract: Many networks are characterized by highly heterogeneous distributions of links which are called scale-free networks, with the degree distributions following $p(k)\sim ck^{-\alpha}$. Entropy of the degree distribution has been proved an average measure for the network heterogeneity so can be useful for optimizing scale-free network robustness to random failure. In this work we improve the theory of the effectiveness of entropy of the degree distribution on measuring scale-free networks robustness to targeted attack, by introducing the edges related parameter of pd which means the ratio threshold of the lost edges to all the edges in the topology at which the scale-free networks will break down. Our work has proved that the entropy of the degree distribution is really an effective measurement for network robustness to not only random failure but also targeted attack.

Key words: Scale-free networks, information theory, entropy, targeted attack

INTRODUCTIONS

Many networks can be characterized as scale-free networks whose degree distributions following $p(k)\sim ck^{-\alpha}$, with $\alpha\in(2, 3)$ (Albert *et al*., 1999; Newman, 2003), these networks including information networks, technological networks, social networks and biological networks.

To investigate the vulnerability of scale-free networks, Albert *et al*. (1999) presented two failure modes, i.e., random failure and targeted attack and they found that the scale-free network performs robust to random failure but is vulnerable to targeted attack (Albert *et al*., 2000). Cohen *et al*. (2000, 2001) formulated the scale-free network vulnerability as the percolation of generalized random networks using percolation theory. Through the thorough analysis of the robustness of scale-free networks under random failure and targeted attack, Cohen *et al*. (2000) pointed out that there exists a threshold p and when a fraction $p>p_c$, the network will be broken to disconnected island parts, where p is the ratio of the number of nodes removed to the total number of the nodes in the whole network.

The heterogeneous distribution on links is an essential character of a scale-free network and impacts on the network robustness directly. The more heterogeneous of a network is, the better robustness the network will be. Therefore, other than using percolation theory to analysis and optimize network robustness, the heterogeneity measured by entropy is also used to analyze scale-free network vulnerability and optimization network robustness (Wang *et al*., 2006). The work by Wang *et al*. (2006) has proved that the entropy of the degree distribution is effective to measure robustness for scale-free network to random failures. However, the parameter threshold p_c indicating the ratio of removed nodes, can not prove the correlation of the entropy of degree distribution to targeted attack, so can not prove the effectiveness of the entropy in measuring the robustness of scale-free networks to targeted attack. Wu and others proposed many different methods to enhance network robustness against intentional attack (Wu *et al*., 2007; Zhao and Xu, 2009; Xiao *et al*., 2010; Xiao and Xiao, 2011) etc. Though these methods appear to be effective in detail, they can't reveal the essential relationship among p_c, heterogeneous and scale-free networks robustness.

In this study, we improve the work of Wang *et al*. (2006) to investigate the effectiveness of the entropy in measuring robustness of scale-free network to targeted attack. After examining the relationship between the entropy and the network threshold p_c being defined in (Cohen *et al*., 2000), we define and introduce a parameter p_d, to indicate the threshold of the ratio of the number of lost edges to that of all edges in the whole network, i.e., at the threshold p_d, the network began to break down to disconnected island parts and no longer is an integrated network topology. Using p_d, our work has proved that the entropy of the degree distribution has a positive effect on p_d, so that the entropy can be used to measure the network robustness to targeted attack.

To sum up, our work has proved that the entropy of the degree distribution is an effective measurement to evaluate network robustness to both random failures and targeted attack.

THE ENTROPY OF DEGREE DISTRIBUTION FOR TARGETED ATTACK

As demonstrated by Albert *et al.* (1999), the degree distribution of scale-free network follows power law, i.e., $p(k)\sim ck^{-\alpha}$, k = m, m+1,...,K, m is the minimal network degree (e.g., for Internet, m = 1), K is the maximal network degree. The entropy of the degree distribution is defined by Wang *et al.* (2006) as follow:

$$H = -\sum_{k=1}^{N-1} p(k)\log p(k) \quad (1)$$

N is the total number of vertices.

With the formula (1) of H and continuous approximation, the approximate entropy of the degree distribution can be expressed as formula (2). For more detail derivation, please refer to by Wang *et al.* (2006):

$$H(\alpha,m,N) = \left(\log\left(\frac{\alpha-1}{m}\right)+\frac{\alpha}{1-\alpha}\right)\left(\frac{1}{N}-1\right)-\frac{\alpha}{\alpha-1}\frac{\log N}{N} \quad (2)$$

Essentially, H is the approximate entropy of the degree distribution in scale-free network α is the scaling exponent. Figure 1 shows the relationship between α and H, for different values of N when m = 1. For a given N, the entropy of the scale-free network degree distribution decreases with α increasing. With the increase of scaling exponent α, the network heterogeneity will decrease, so that H will also decrease. As an extreme example, when $\alpha\to\infty$:

$$(k) = \begin{cases} 1 (k = m) \\ 0 (k \neq m) \end{cases}$$

so that the degree distribution is lowest with the entropy being zero. On the contrary, when $\alpha\to\infty$, p(m) = p(m+1) = ··· = p(K), network heterogeneity reaches the largest, the entropy H is the largest. For a given α, the larger N is, the more complex the scale-free network is and thus the larger H is.

As mentioned above, p_c is an important indicator to measure networks robustness, i.e., the larger the p_c, the more robust the network (Cohen *et al.*, 2000). In the random failure scenario, p_c behaves a positive effect on the entropy H (Wang *et al.*, 2006).

In the random failure scenario, the failure on nodes and edges of a network occur randomly, nevertheless, the targeted attackers usually destroy the most important network nodes with high connection degree. Such differences should be carefully considered in proving of the entropy on targeted attack.

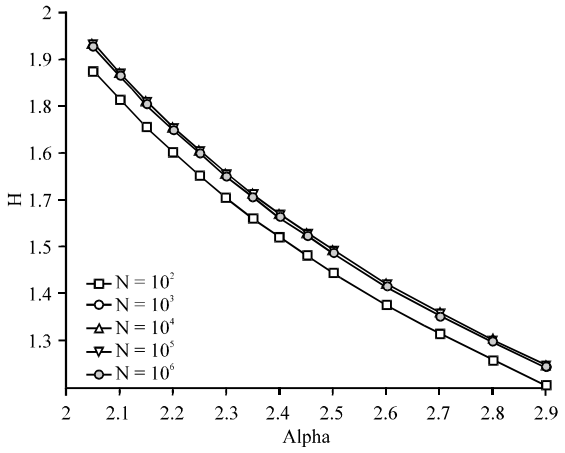

Fig. 1: Relationship between α and H for different N with m = 1

Under the targeted attack scenario, according to the percolation theory, we can figure out the standard formula of p_c is (Cohen *et al.*, 2001):

$$1-\tilde{p} = \frac{1}{\kappa_0-1} \quad (3)$$

$$\kappa_0 = \left(\frac{2-\alpha}{3-\alpha}\right)\frac{\tilde{K}^{3-\alpha}-m^{3-\alpha}}{\tilde{K}^{2-\alpha}-m^{2-\alpha}} \quad (4)$$

$$\tilde{p} = \sum_{k=\tilde{K}}^{K}\frac{kp(k)}{\langle k_0\rangle} \quad (5)$$

$$p_c = \sum_{k=\tilde{K}}^{K} p(k) \quad (6)$$

where, $\tilde{p}$ is the probability of an edge randomly being selected associating the removed nodes.

$\tilde{K}$ in the targeted attack scenario, is equivalent to the maximum degree in the random failure scenario.

K is the maximal network degree in the targeted attack scenario.

p_c is the percentage of removed points in the targeted attack scenario when the network crashes.

Therefore, in the targeted attack scenario, the relationship between p_c and α, as well as that between p_c and the entropy H can be illustrated in Fig. 2 and 3 respectively, for a set of N(m = 1).

Figure 3 indicates that in the targeted attack, as the entropy H increases, p_c increases and then decreases, that is, p_c is no longer proportional to the entropy H as do in

random failure, so that the entropy H can not be used to measure network robustness. Another indicator other p_c is required to evaluate the entropy H on network robustness for targeted attack.

From Fig. 2, we can find that the smaller α is, the larger the max degrees are, i.e., the larger number of edges the max degree node will be connected to. In other words, more edges are occupied by just a small number of hub nodes with a small α, so that once these hub nodes are removed by targeted attacker, a large quantities of network edges will be lost and the network is more be crashed. Therefore, the lost edges can also be used as an effective measurement to evaluate the robustness of networks to targeted attack.

Therefore, we define the edges parameter p_d to be the threshold ratio of the removal edges to all the edges in the network topology at which the scale-free networks will break down, so that we can discuss the relationship between p_d and H for targeted attack.

In study Cohen *et al.* (2001), $\tilde{p}$ is defined as: the probability that a connection belongs to a deleted node, i.e.:

$$\tilde{p} = \sum_{k=\tilde{K}}^{K} \frac{kp(k)}{\langle k_0 \rangle} \tag{7}$$

According to the definition of p_d, in the scenario of targeted attacks, we can formulate p_d as following:

$$p_d = \frac{\sum_{k=\tilde{K}}^{K} kp(k)}{\sum_{k=m}^{K} kp(k)} \tag{8}$$

Formula (7) and (8) are factually the same, i.e., $\tilde{p} = p_d$. So we can the percolation theory to get the following equations:

$$1\text{-}p_d = \frac{1}{\kappa_0\text{-}1} \tag{9}$$

$$\kappa_0 = \left(\frac{2\text{-}\alpha}{3\text{-}\alpha}\right)\frac{\tilde{K}^{3-\alpha}\text{-}m^{3-\alpha}}{\tilde{K}^{2-\alpha}\text{-}m^{2-\alpha}} \tag{10}$$

$$p_d = \sum_{k=\tilde{K}}^{K} \frac{kp(k)}{\langle k_0 \rangle} \tag{11}$$

Thus we can derive the relationship between p_d and α for m = 1, as shown in Fig. 4. We can find that p_d will increase with the increasing of α. In addition, using equation (1), we can get the relationship between the entropy H and p_d, as shown in Fig. 5, in which, at m = 1, the change of p_d is consistent with that of H. In other words, when m = 1, the greater the entropy of the degree

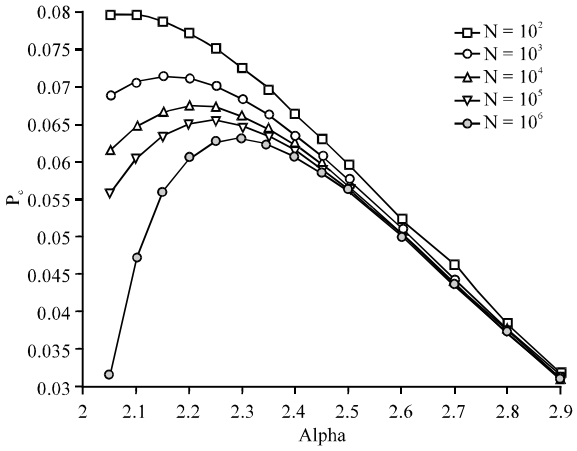

Fig. 2: Relationship between p_c and α for different N with m = 1

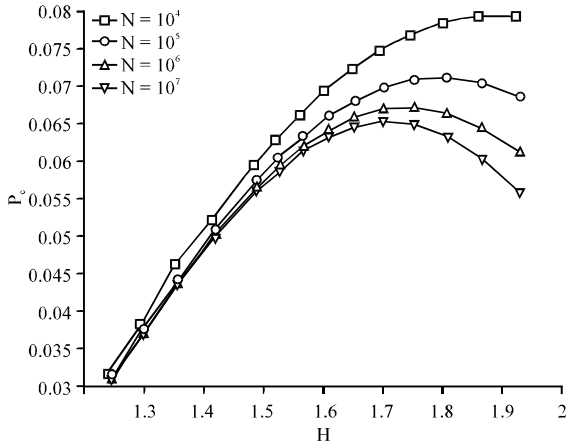

Fig. 3: Relationship between p_c and H for different N with m = 1

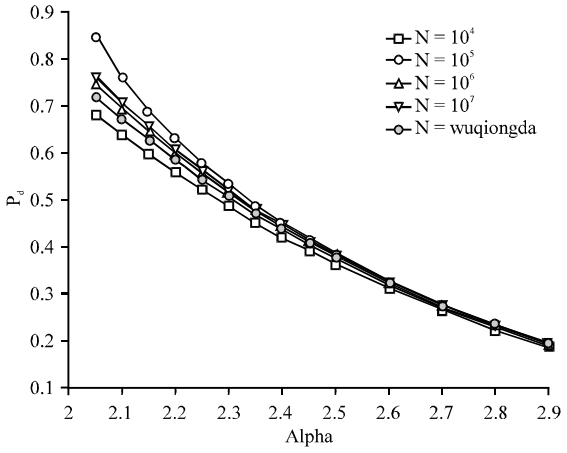

Fig. 4: Relationship between p_d and α for different N with m = 1

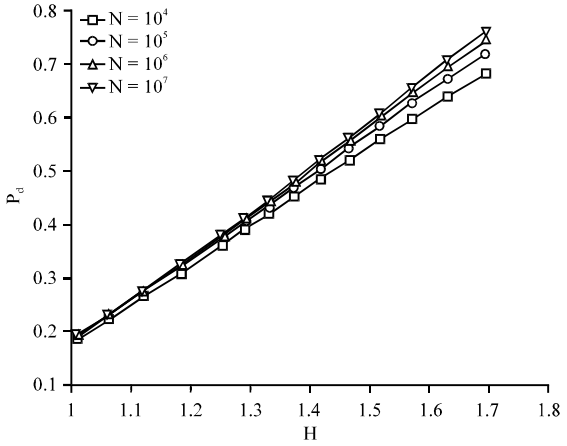

Fig. 5: Relationship between p_d and H for different N with m = 1

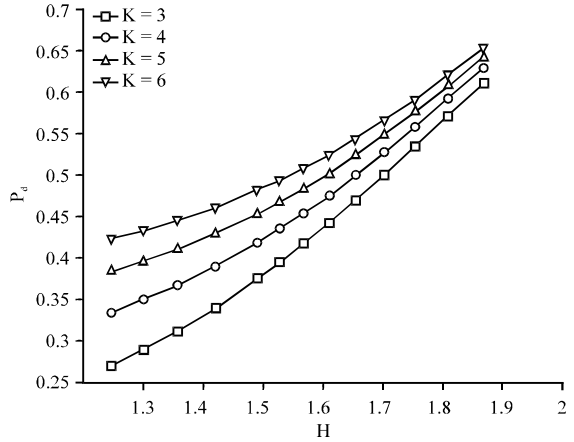

Fig. 6: Relationship between p_d and H for different average connectivity (k). For all curves, $\alpha \in (2, 3)$, $N = 5\times10^4$

distribution is, the larger number of edges need to be removed to collapse the network.

To demonstrate the relationship between p_d and H in detail, we show the results of the parameter threshold p_d and H for different average connectivity (k) in Fig. 6, when $\alpha \in (2, 3)$, $N = 5\times10^4$. The average connectivity (k) is obtained with continuous approximation:

$$\langle k \rangle = \int_m^K k \cdot p(k)dk = \int_m^K k \cdot ck^{-\alpha}dk = \frac{c}{2-\alpha}\left(K^{2-\alpha}-m^{2-\alpha}\right) \quad (12)$$

As shown in Fig. 6, with the increase of (k), the p_d will also increase which means the enhancing on the network robustness. Given a constant (k), p_d is proportional to H which indicates that on targeted attack, the bigger p_d is, the greater the entropy of the network is and the more edges need to be removed to collapse the network and thus the stronger the network robustness will be.

CONCLUSION

The heterogeneity of network links relates to network robustness to both random failures and targeted attacks. The entropy of degree distribution has been proved to be an effective parameter to measure the heterogeneity of link distribution, so to measure network robustness to random failure. In this work, we proved that the entropy of degree distribution also performs its effectiveness on measuring network robustness to targeted attack, via introducing the parameter p_d as the ratio of removed edges. Therefore, the entropy of degree distribution will contribute to understanding in deep robustness of scale-free networks so to achieve the optimal design of scale-free networks which are our future investigations.

ACKNOWLEDGMENTS

This study was supported by the Science Research Project of Henan Education Department (Grant No. 12A510021), Science and technology R&D program of Xuchang Science and technology bureau (Grant No. 1101060).

REFERENCES

Albert, R., H. Jeong and A.L. Barabasi, 1999. Internet: Diameter of the world-wide web. Nature, 401: 130-131.

Albert, R., H. Jeong and A.L. Barabasi, 2000. Error and attack tolerance of complex networks. Nature, 406: 378-381.

Cohen, R., K. Erez, D. Ben-Avraham and S. Havlin, 2000. Resilience of the internet to random breakdowns. Phys. Rev. Lett., 85: 4626-4628.

Cohen, R., K. Erez, D. Ben-Avraham and S. Havlin, 2001. Breakdown of the internet under intentional attack. Phys. Rev. Lett., 86: 3682-3685.

Newman, M.E.J., 2003. The structure and function of complex networks. Soc. Indust. Applied Mathe. Rev., 45: 167-256.

Wang, B., H. Tang, C. Guo and Z. Xiu, 2006. Entropy optimization of scale-free networks robustness to random failures. Phys. A: Stat. Mech. Appl., 363: 591-596.

Wu, J., H.Z. Deng, Y.J. Tan, Y. Li and D.Z. Zhu, 2007. Attack vulnerability of complex networks based on local information. Modern Phys. Lett. B, 21: 1007-1014.

Xiao, S., G.X. Xiao and T.H. Cheng, 2010. Tolerance of local information-based intentional attacks in complex networks. J. Phys. A, Vol. 43.

Xiao, S. and G.X. Xiao, 2011. On imperfect node protection in complex communication networks. J. Phys. A, Vol. 44.

Zhao, J.C. and K. Xu, 2009. Enhancing the robustness of scale-free networks. J. Phys. A, Vol. 42.