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 $p(k)\sim k^{-\alpha}$. 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 $p_d$ 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 $p(k)\sim k^{-\alpha}$, 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 of 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 $p$, 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., $p(k) - k^{-\alpha}$, $k = m, m+1, \ldots, K$, $m$ 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:

$$H = \sum_{k=m}^{\infty} p(k) \log p(k)$$

(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):

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

(2)

Essentially, $H$ is the approximate entropy of the degree distribution in scale-free network $\alpha$ is the scaling exponent. Figure 1 shows the relationship between $\alpha$ 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 $\alpha$ increasing. With the increase of scaling exponent $\alpha$, the network heterogeneity will decrease, so that $H$ will also decrease. As an extreme example, when $\alpha \to \infty$:

$$p(k) = \frac{\delta}{\delta (k - m)}$$

so that the degree distribution is lowest with the entropy being zero. On the contrary, when $\alpha \to \infty$, $p(m) = p(m+1) = \ldots = p(K)$, network heterogeneity reaches the largest, the entropy $H$ is the largest. For a given $\alpha$, 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 the entropy on targeted attack.

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

$$\hat{p} = \frac{1}{\kappa' k^\alpha}$$

(3)

$$\kappa' = \frac{2 - \alpha}{3 - \alpha} \frac{K^{1/m - \alpha}}{3 - \alpha}$$

(4)

$$p_c = \frac{\hat{p}}{\sum_{k} p(k)}$$

(5)

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

$K$ 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 $\alpha$, 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 $p_e$ is required to evaluate the entropy $H$ on network robustness for targeted attack.

From Fig. 2, we can find that the smaller $\alpha$ 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 $\alpha$, 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 $p_e$ 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 $p_e$ and $H$ for targeted attack.

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

$$\bar{p} = \sum_{k>2} \frac{k p(k)}{\langle k \rangle}$$  \hspace{1cm} (7)

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

$$p_e = \sum_{k>2} \frac{k p(k)}{\langle k \rangle}$$ \hspace{1cm} (8)

Formula (7) and (8) are factually the same, i.e., $\bar{p} = p_e$

So we can the percolation theory to get the following equations:

$$1-p_e = \frac{1}{\kappa_{e-1}}$$ \hspace{1cm} (9)

$$\kappa_{e} = \sum_{m=2}^{\infty} \frac{m^{\alpha-3}}{\langle k \rangle}$$ \hspace{1cm} (10)

$$p_e = \sum_{k>2} \frac{k p(k)}{\langle k \rangle}$$ \hspace{1cm} (11)

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


