International Journal of Pure and Applied Mathematics

Volume 39 No. 1 2007, 101-106

ENHANCE ROBUSTNESS OF SCALE-FREE NETWORKS

Qiang Guo[1], Jian-Guo Liu[2 §], Da-Tian Niu[3]

[1,3]School of Science
Dalian Nationalities University
Dalian, 116600, P.R. CHINA

[2]Institute of System Engineering
Dalian University of Technology
Dalian, 116024, P.R. CHINA
e-mail: liujg004@yahoo.com.cn

Abstract: In this paper, we investigate the network design guideline which can enhance the robustness of the network to both random failures and intentional attacks maximum while keeping the average connectivity $\langle k \rangle$ per node constant. We find that the strategy that protect the highest degree nodes is not effective. When 3% highest nodes are protected, the robustness only enhances about 0.001.

AMS Subject Classification: 65Y05, 65Y10, 49J35, 90C25, 90C30, 68W10, 68W25

Key Words: scale-free network, optimal programme, power-law distribution, random failure, intentional attacks

1. Introduction

Recently there have been much interests in determining network configurations which are robust against various types of attacks [1, 7, 6, 8]. Many social, biological and communication systems can be properly described as scale-free networks with nodes representing individuals or organizations and edges mimicking the interactions among them [7, 6, 8]. Since scale-free networks are robust to random failures but vulnerable to intentional attacks, it is important for us to know the optimal network guideline to design scale-free networks which are

Received: April 29, 2007

[§]Correspondence author

optimally robust against both types of attacks. Although many papers have designed the optimal network topology, such as the two-peak and three-peak optimal complex network [10], but we can not convert its topology to the theoretical optimization directly disobeying its evolutionary principle. On the contrary, we should study the optimal scale-free network guideline to enhance the existed scale-free network robustness. Inspired by this simple idea, we studied the strategy that can enhance robustness of scale-free networks effectively.

Studies of scale-free networks robustness have been considered only the case in which there was only one type of attack in a given network, that is, the network was subject to either random attacks or targeted attacks but not subject to different types of attack simultaneously [2, 10]. In scale-free networks, the degree distribution $P(k) \sim k^{-\gamma}$ is the probability of a node have k connections to other nodes, typically decreases as a power of k. When a fraction p of the nodes and their connections of scale-free networks are randomly removed, the probability that the chosen nodes have a low degree is very high, so its removal has little effect on the network. But the removal of a highly connected node could produce a large effect since such nodes may hold significant fractions of the network together by providing connections between many other nodes. Cohen et al [3] presented a criterion to calculate the percolation critical threshold of randomly connected networks. They found that for $\gamma \leq 3$ the transition never takes place, unless the network is finite. Cohen et al [4] studied the tolerance of breakdown of random networks to intentional attacks. They found that scale-free networks with $\gamma \leq 3$ are sensitive to intentional attack. Paul et al [9] studied the network design guideline which maximize the robustness of networks to both random failures and intentional attacks while keeping the average number of links per node of the network constant. Liu et al [5] found that when $\langle k \rangle = 3$ the robustness of the scale-free networks reach its maximum value if the minimal connectivity $m = 1$, but when $\langle k \rangle$ is larger than four, the networks will become more robust to random failures and targeted attacks as the minimal connectivity m gets larger. Wang et al [11] presented the entropy optimization method of scale-free networks robustness to random failures and give the most optimal robustness scale-free networks to random failures.

But these work did not tell us how to enhance the existing network robustness in detail. This inspired us the question: what is the effective strategy to improve scale-free networks robustness. In this paper, a strategies is given to enhance scale-free networks robustness. Since the highest degree nodes are more important to the network robustness, the strategy is to protect the nodes with degree higher than k_c without any new edges are added.

This paper is organized as follows. In Sections 2 and 3, the optimization method to calculate the thresholds to random failures and intentional attacks are given respectively. In Section 4, the strategy that protect the highest degree nodes are given. Finally, the conclusion and discussion are given.

2. Breakdown for Random Failures

The percolation phase transition in scale-free random networks have been studied by Cohen [3]. The critical threshold to random failures p_c can be expressed as

$$p_c = 1 - \frac{1}{\kappa_0 - 1}, \tag{1}$$

where $\kappa_0 \equiv \langle k_0^2 \rangle / \langle k_0 \rangle$ is calculated from the original connectivity distribution. A wide range of networks have power-law degree distribution: $P(k) = ck^{-\alpha}, \ \ k = m, m+1, \ldots, K$, where $k = m$ is the minimal connectivity and $k = K$ is an effective connectivity cutoff presented in finite networks. Liu et al have presented the optimization robustness of scale-free network to random failures. The idea is maximize the threshold for random removal with the condition that the average degree $\langle k \rangle$ per node is constant. They have got the following conclusion.

— If the average connectivity $\langle k \rangle$ per node and the exponent α of the scale-free network is constant, the robustness of the network will decrease when the network size becomes larger.

— If the network size N is constant, the robustness of the network increases when the average connectivity $\langle k \rangle$ becomes larger.

— To the random failures, we have to take several times cost to increase the robustness of the scale-free network one percent.

3. Breakdown under Intentional Attacks

The intentional attacks to scale-free networks can be considered as the process that a fraction p of the sites with the highest connectivity are removed, and the links emanating from the sites are removed as well. This would make the cutoff connectivity K of the network reduce to some new value, $\widetilde{K} < K$. Because the upper cutoff K before intentional attacks can be estimated from $\sum_{k=K}^{\infty} P(k) = \frac{1}{N}$, the new cutoff $\widetilde{K}$, after the attacks, can be estimated by

$$\widetilde{p} = (\widetilde{K}/m)^{2-\alpha}[1 - (\frac{K}{\widetilde{K}})^{2-\alpha}]. \tag{2}$$

Replacing p_c and K in $1-p_c^{\rm rand} = \frac{1}{\kappa_0 - 1}$ with (2) and $\widetilde{K}$, this yields the equation:

$$1 - \widetilde{p} = \frac{1}{\widetilde{\kappa} - 1}, \tag{3}$$

where $\widetilde{\kappa} = \frac{2-\alpha}{3-\alpha} \frac{\widetilde{K}^{(3-\alpha)} - m^{(3-\alpha)}}{\widetilde{K}^{(2-\alpha)} - m^{(2-\alpha)}}$. Equation (3) can be solved numerically to obtain $\widetilde{K}(m, \alpha, K)$ and $p_c(m, \alpha)$. The numerically results are as follows: (1) scale-free networks are very fragile when the minimum connectivity m equals to 1. If intentionally remove about five percent nodes which have the highest connectivity of scale-free networks, the networks would collapse. (2) The robustness of the networks would increases dramatically when the minimum connectivity m increases.

4. Strategy of Highest Degree Nodes are Protected against Intentional Attacks

When scale-free networks have random failures and intentional attacks simultaneously, our strategy is to enhance the robustness of scale-free networks is to protect the highest degree nodes without any new edges added. The threshold of the strategy can be demonstrated as

$$p_c^{\rm total} = p_c^{\rm rand} + p_c^{\rm target}, \tag{4}$$

where $p_c^{\rm rand}$ presents the threshold to random failures and $p_c^{\rm target}$ presents the threshold to intentional attacks after the highest degree nodes protected. Suppose that the nodes with degree higher than k_c are protected, then there are $f_c = \sum_{k \geq k_c}^{K} ck^{-\gamma}$ percent of nodes are protected. Replacing K in (3) with k_c, one can get the threshold to the intentional attacks after highest degree nodes protected. The $p_c^{\rm rand}$ can be obtained from (1). The total critical percolation thresholds have been demonstrated in Figure 1.

From Figure 1, one can get the following conclusions:

(1) When $N = 10^6$, if there are 2% highest nodes are protected to intentional attacks, the total thresholds of $\langle k \rangle = 3, 4, 5$ enhance about 0.038%, 0.0565% and 0.0847%, respectively. Although the total thresholds increase with the average degree, the growth are very small which almost can be neglected.

(2) When $\langle k \rangle = 3$, if there are 2% highest nodes are protected to intentional attacks, the total thresholds of scale-free network with network size $N = 10^3, 10^4, 10^6$ enhance about 0.04%, 0.0196% and 0.0287%, respectively.

The above two conclusions imply that the strategy that protect the highest degree nodes is not effective.

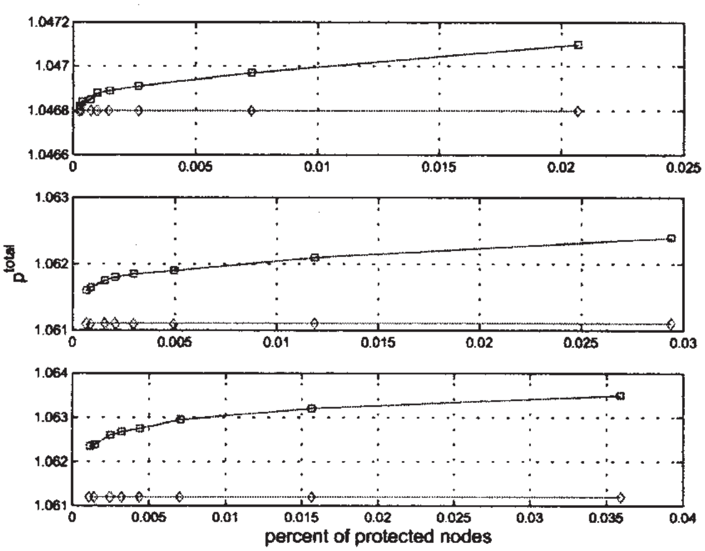

Figure 1: Total critical percolation thresholds for scale-free networks with size $N = 10^6$ to different average degree.

5. Discussion and Summary

In this paper, we presented a strategies to enhance the robustness of scale-free networks to random failures and intentional attacks. The numerical results indicate that the strategy that protect 2% highest degree nodes can enhance the networks robustness very little.

Although the theoretical optimal networks to both random and targeted attacks have been designed, it is very important that some large size networks, such as Internet, are self-organizing system and evolves with time according to their evolutionary principle dictated by the interplay between cooperation and competition. To the exist growing scale-free networks, we cannot convert its topology into the theoretical optimization directly disobeying its evolutionary principle. But we can improve the network robustness in detail. Further work should emphasis on the most effective strategy to enhance robustness of scale-free networks.

References

[1] R. Albert, A.-L. Barabási, *Rev. Mod. Phys.*, **74** (2002), 47.

[2] R. Albert, H. Jeong, A.L. Barabási, *Nature*, **406** (2000), 6794.

[3] R. Cohen, K, Erez, D. Ben-Avraham, S. Havlin, *Phys. Rev. Lett.*, **85** (2000), 4626.

[4] R. Cohen, K, Erez, D. Ben-Avraham, S. Havlin, *Phys. Rev. Lett.*, **86** (2001), 3682.

[5] J.G. Liu, Z.T. Wang, Y.Z. Dang, *Mod. Phys. Lett. B*, **19** (16) (2005), 785.

[6] J.F.F. Mendes, S.N. Dorogovtsev, A.F. Ioffe, *Evolution of Networks: From Biological Nets to the Internet and the WWW*, Oxford University Press, Oxford (2003).

[7] M.E.J. Newmann, *SIAM Rev.*, **45** (2003), 167.

[8] R. Pastor-Satorras, A. Vespignani, *Evolution and Structure of the Internet: A Statistical Physics Approach*, Cambridge University Press, Cambridge (2004).

[9] G. Paul, T. Tanizawa, S. Havlin, H.E. Stanley, *Eur. Phys. J.B*, **38** (2004), 187.

[10] A. Valente, A. Sarker, H.A. Stone, *Phys. Rev. Lett.*, **92** (2004), 118702.

[11] B. Wang, H.W. Tang, C.H. Guo, Z.L. Xiu, d-mat/0506725, *Physica A*, To Appear.