Information Sciences Letters

Volume 1
Issue 2 *May 2012*

Article 1

2012

Efficient strategies for attack via partial information in scale-free networks

Yilun Shang
Institute for Cyber Security, University of Texas at San Antonio San Antonio, Texas 78249, USA, shylmath@hotmail.com

Information Sciences Letters
An International Journal

Efficient strategies for attack via partial information in scale-free networks

Yilun Shang

Institute for Cyber Security, University of Texas at San Antonio, San Antonio, Texas 78249, USA

Received: Jan. 8, 2012; Revised March 4, 2012; Accepted March 6, 2012
Published online: 1 May 2012

Abstract: In this paper, we propose an attack model based on partial information, which means that one can obtain the information of a part of nodes in the networks. We study the efficient attack strategy (EAS) in random scale-free networks. It is shown that the attack strategy can affect the attack effect remarkably and the EAS can achieve better attack effect than other typical attack strategies. Extensive simulations are performed to validate and illustrate our analytical results. Our results will be of theoretical and practical significance both for protecting infrastructural networks and stopping the spreading of harmful things (like disease) on networks.

Keywords: Attack strategy, partial information, scale-free, complex network.

1. Introduction

The structure and behavior of complex networks have received growing attention in various kinds of studies [1–8]. Of special interest are the power-law random networks in which the fraction of vertices of degree k is proportional to $k^{-\lambda}$ for some scaling exponent $\lambda > 1$. Such networks lack a clear scale and have been called as "scale-free". Scale-free graphs are popular in random network theory and have been proposed as a common way to model the behavior of technological, biological and social networks [4, 9]. For fitting empirical distributions to theoretical models, we refer the reader to the recent review [10].

Due to its broad application, the attack vulnerability of complex networks, namely, how attacks affect the integrity and operation of the networks, has attracted much attention [11–18]. In the pioneer work of Albert *et al*. [11], they study the robustness of networks against two types of attacks: random failure, where nodes are sequentially removed with equal probability, and intentional attack, where hubs (*i.e.*, nodes with large degrees) are preferentially removed. It is shown that scale-free networks having $\lambda \leq 3$ are exceptional robust against the random failure in the sense that almost all nodes have to be removed to disintegrate a scale-free network while are rather fragile to the intentional attack in the sense that the network is destroyed if a small fraction of hubs are removed. Recently, some researchers investigate the effective attack strategy (EAS) for harmful networks such as epidemic spreading networks, cancer networks, and terrorist networks. Lloyd *et al*. [19] study the most effective strategy against an epidemic spreading among computers and people. Quayle *et al*. [20] address various network attack strategies to maximize the preferential perturbation in cancer networks. In most of the existing works concerning attack strategies, it is assumed that we can obtain complete information on the network structure. However, complete information is often not available in real-world networks, especially when the networks are large-scale. Dezsó *et al*. [21] analyze a biased treatment strategy against viruses spreading in scale-free networks based on uncertain information, which means that one can obtain the information of all nodes, but the information may be uncertain. An efficient vaccination strategy is proposed by Holme [22] based on local information, which means that each individual only knows the information of its neighbors. Li *et al*. [23] treat an attack strategy performing on scale-free networks using incomplete information, meaning that one can obtain the information of part of the nodes, not necessarily their neighbors. Our prior work [24] explores a scheme where the information of all nodes can be extracted but is subject to some randomly distributed measurement errors.

* Corresponding author: e-mail: shylmath@hotmail.com

Inspired by the above works, in the current paper, we introduce an attack model for scale-free networks based on information of partial nodes. Unlike [23], we do not fix the attack size, *i.e.*, the number of nodes under attack, but focus on the effect of the attack over the network. We derive various efficient attack strategies (EAS), which vary with the magnitude of attack information in an intricate way. It is found that the attack strategy can affect the attack effect remarkably and the EAS derived can achieve better attack effect than other typical strategies. The theoretical results are confirmed by our simulation study on random scale-free networks.

The rest of the paper is organized as follows. In Section 2, we introduce the attack model. Section 3 and Section 4 are devoted to analytical and simulation studies, respectively. We finally conclude the paper in Section 5.

2. Model and Notations

A complex network is usually modeled by a simple undirected graph $G(V, E)$, where V is the set of nodes, and $E \subseteq V \times V$ is the set of edges. Let $N = |V|$ be the number of nodes, and d_i be the degree of node $v_i \in V$. Denote by m and M the minimum and maximum degrees of G, respectively. Let $p(k) \sim k^{-\lambda}$ $(m \leq k \leq M)$ be degree distribution of the scale-free network in question.

Let $\hat{V} \subseteq V$ be the *white area* in which one can obtain the attack information and $\tilde{V} = V \backslash \hat{V}$ the *black area* in which one can not obtain the attack information. We remark that “white area of a map” colloquially means an “unchartered territory”, however, we believe the use of words *white* and *black* is visual herein and helps to understand. To characterize the magnitude of attack information quantitatively, we assume that $\hat{V}$ and $\tilde{V}$ have the same degree distribution as V. The ratio $\alpha = |\hat{V}|/N \in [0, 1]$ can then be seen as a measure of magnitude of attack information. For simplicity we use the degree sequence $\{d_i\}_{i=1}^N$ as the attack information and choose the relative size of the largest component $S \in [0, 1]$ [11] as the performance measure of a network. We define the increment $\varDelta S$ of the relative size of the largest component after attack as the attack effect [23].

We take $\varOmega \subseteq V$ as the attack targets. Thus, $n_w = |\varOmega \cap \hat{V}|$ is the number of attacked nodes in the white area, while $n_b = |\varOmega \cap \tilde{V}| = |\varOmega| - n_w$ is the number of attacked nodes in the black area. Since we can obtain the attack information d_i in the white area, we will attack the n_w nodes in the descending order of d_i in the white area. Nevertheless, we can only attack the n_b nodes in the black area randomly due to the absence of attack information. We take $f_w = n_w/|\hat{V}|$ as the white attack proportion and $f_b = n_b/|\tilde{V}|$ as the black attack proportion. Our aim is to determine the optimal white (or black) attack proportion f_w^* (or f_b^*) that maximizes the attack effect $\varDelta S$ for any given black (or white) attack proportion f_b (or f_w). It is clear that $\alpha = 0$ corresponds to the random failure and $\alpha = 1$ corresponds to the intentional attack. Therefore, our attack model, like [24], interpolates the two extreme scenarios studied in [11].

3. Analytical Study

In this section, we will exploit the generating function formalism [4,25] to analytically derive the optimal attack proportions f_w^* and f_b^*.

Let $q(k)$ be the probability distribution that a node is not attacked given that it has degree k. Denote by $\tilde{K}$ the maximum degree of the remain nodes in the white area after the attack. Then we can express $q(k)$ as

$$q(k) = \begin{cases} 1 - (1-\alpha)f_b, & k \leq \tilde{K} \\ 1 - \alpha - (1-\alpha)f_b, & k > \tilde{K} \end{cases} \tag{1}$$

Let K be the maximum degree of nodes in the white area before attack. Sort all $N\alpha$ nodes in the white area in the decreasing order of degree, and let $r(k)$ be the rank of a node with degree k in the white area. We obtain

$$r(k) = N\alpha \int_k^K p(t)\mathrm{d}t \tag{2}$$

Since $r(\tilde{K}) = N\alpha f_w$, we have

$$r(\tilde{K}) = N\alpha \int_{\tilde{K}}^K p(t)\mathrm{d}t = N\alpha f_w \tag{3}$$

We can obtain $\tilde{K}$ by solving (3). For scale-free networks with power-law distribution $p(k) = ck^{-\lambda}$ $(m \leq k \leq M)$, where $c \approx (\lambda - 1)m^{\lambda-1}$ and $M \approx mN^{1/(\lambda-1)}$ by extreme value theory [4], we calculate $\tilde{K}$ as

$$\tilde{K}(\alpha, f_w, f_b) = m\left(f_w + \frac{1}{N}\right)^{\frac{1}{1-\lambda}} \approx m f_w^{\frac{1}{1-\lambda}} \tag{4}$$

The generating function for $p(k)$ is given by $G_0(x) = \sum_{k=m}^{M} p(k)x^k$. The excess degree distribution, that is, the distribution of the degree of the nodes that we arrive at by choosing a random edge and following it to one of its ends, is another important quantity [26]. The normalized distribution $R(k)$ of the remaining degree is then given by $R(k) = (k+1)p(k+1)/\langle k\rangle$, where $\langle k\rangle$ is the average degree of the graph G. Hence, the corresponding generating function is

$$G_1(x) = \sum_{k=m}^{M} R(k-1)x^{k-1} = G_0'(x)/\langle k\rangle \tag{5}$$

Let $w_0(k) = p(k)q(k)$ be the probability that a randomly chosen node has degree k and is not attacked. Let $w_1(k) = R(k)q(k+1)$ be the probability that a node at the end of a randomly chosen edge has remaining degree k and is not attacked. Thus, the generating functions of $w_0(k)$ and $w_1(k)$ are seen to be given by

$$F_0(x) = \sum_{k=m}^{M} w_0(k)x^k = \sum_{k=m}^{M} p(k)q(k)x^k \tag{6}$$

and

$$F_1(x) = \sum_{k=m-1}^{M-1} w_1(k)x^k = \sum_{k=m}^{M} \frac{kp(k)}{\langle k\rangle} q(k)x^{k-1} = \frac{F_0'(x)}{\langle k\rangle} \tag{7}$$

respectively.

As derived in [4,25], the generating function for the distribution of the size of component by following a randomly chosen edge is $H_1(x) = 1 - F_1(1) + xF_1(H_1(x))$. Similarly, the probability distribution for the size of component to which a randomly chosen node belongs is generated by $H_0(x)$, where $H_0(x) = 1 - F_0(1) + xF_0(H_1(x))$. Let the relative size of the largest component after the attack be S_a. Hence, we can write S_a as

$$S_a = F_0(1) - F_0(u) \tag{8}$$

where u is the smallest non-negative solution of the equation $u = 1 - F_1(1) + F_1(u)$. Assume that the network is connected before the attack and then we obtain the attack effect $\Delta S = 1 - S_a$ as a function of attack proportions f_w and f_b. Consequently, we can obtain the optimal white (and black) attack proportion f_w^* (and f_b^*) that maximizes the attack effect, ΔS.

4. Simulation Results

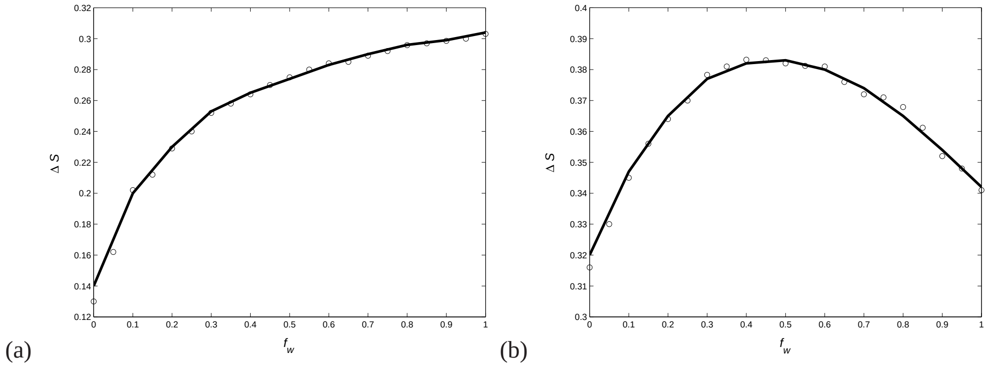
To validate our above model and results, we perform extensive simulations in random scale-free networks. We generate random scale-free networks with degree distribution $p(k) = ck^{-\lambda}$ using the method of configuration model described in [27]. The parameters of this model used here are the number of nodes $N = 2000$, the exponent $\lambda = 2.5$ and the minimum degree allowed $m = 2$. In this model, the degrees of the nodes are determined initially from the desired distribution and then connections are assigned at random.

In Figure 1, we show the numerical results for the attack effect ΔS. We find that the white attack proportion f_w and the black attack proportion f_b affect ΔS remarkably. For instance, if one can obtain the attack information of 60% nodes and intend to attack 60% of nodes in black area, *i.e.*, $\alpha = 0.4$ and $f_b = 0.6$, the attack effect ΔS achieves its maximum when $f_w \approx 0.4$, namely, attacking $n_w = f_w N\alpha = 320$ nodes in the white area and attacking $n_b = f_b N(1-\alpha) = 720$ nodes in the black area.

Next, we consider two typical attack strategies as comparison.

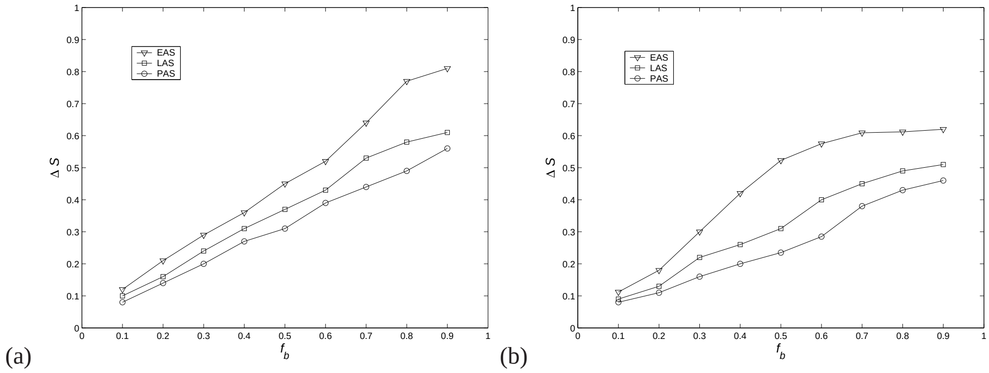
(i)Linear attack strategy (LAS): $f_w = c_1 f_b$ or $f_b = c_1 f_w$ for some $c_1 \in [0,1]$.
(ii)Power attack strategy (PAS): $f_w = f_b^{c_2}$ or $f_b = f_w^{c_2}$ for some $c_2 \in (0,\infty)$.

We present the attack effect under the EAS along with the attack effects under the LAS and PAS in Figure 2 and Figure 3. We draw the following observations. First, the attack effect ΔS is increasing with the attack proportions f_w and f_b, which agrees with our intuition. Second, there is a clear variation of ΔS with distinct differences between the three attack strategies, implying ΔS may be used to measure the attack effect stably even for relatively small sized networks. Third, the EAS can achieve better attack effect than the two typical attack strategies as desired.



(a) (b)

Figure 1 The attack effect ΔS as the function of the white attack proportion f_w for different magnitude of attack information α and black attack proportion f_b in random scale-free networks with degree distribution $p(k) = ck^{-\lambda}$, where $N = 2000$, $\lambda = 2.5$ and $m = 2$. The results are the average of 50 independent simulation runs. (a) $\alpha = 0.2$, $f_b = 0.2$ and (b) $\alpha = 0.4$, $f_b = 0.4$.



(a) (b)

Figure 2 The attack effect ΔS under the efficient attack strategy (EAS), linear attack strategy (LAS) and power attack strategy (PAS) as the function of the black attack proportion f_b for different magnitude of attack information α in random scale-free networks with degree distribution $p(k) = ck^{-\lambda}$, where $N = 2000$, $\lambda = 2.5$ and $m = 2$. (a) $\alpha = 0.3$, $f_w = 0.8f_b$ and (b) $\alpha = 0.7$, $f_w = f_b^2$.

5. Conclusion

To conclude, we have proposed an attack model based on partial information and addressed the efficient attack strategy in random scale-free networks both analytically and numerically. We have shown that the attack strategy can affect the attack effect remarkably and the EAS, including the optimal white attack proportion f_w^* and optimal black attack proportion f_b^*, can achieve better attack effect than other typical strategies. Our results are of great theoretical and practical significance to attack and defense issues in complex networks. Needless to say, there are still some problems remain open. For example, does the network topology has a significant impact on the efficient strategies? How can we characterize this affect qualitatively? What other kinds of measurement of information such as centrality can be used instead of degree? We will treat some of these problems in the future research.

Acknowledgements

The author would like to thank two anonymous referees for their valuable comments that have helped to improve the paper.

References

[1] R. Albert, A.-L. Barabási, Statistical mechanics of complex networks. *Rev. Mod. Phys.*, 74(2002) 47–97

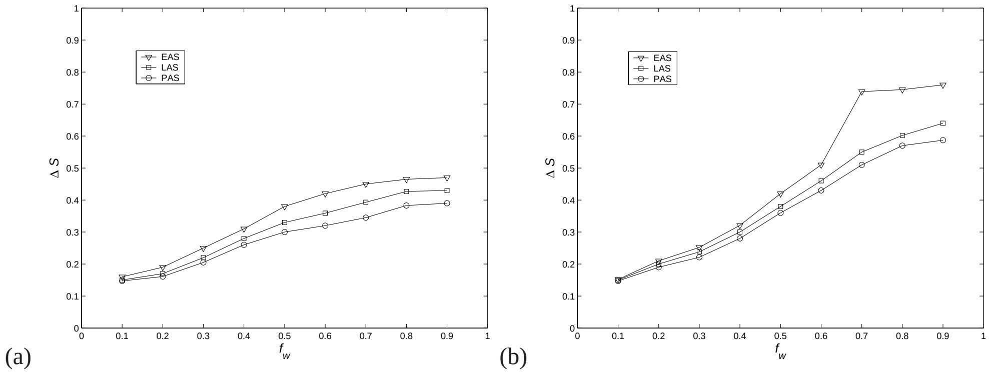


Figure 3 The attack effect ΔS under the efficient attack strategy (EAS), linear attack strategy (LAS) and power attack strategy (PAS) as the function of the white attack proportion f_w for different magnitude of attack information α in random scale-free networks with degree distribution $p(k) = ck^{-\lambda}$, where $N = 2000$, $\lambda = 2.5$ and $m = 2$. (a) $\alpha = 0.3$, $f_b = 0.8f_w$ and (b) $\alpha = 0.7$, $f_b = f_w^2$.

[2] C. L. Apicella, F. W. Marlowe, J. H. Fowler, N. A. Christakis, Social networks and cooperation in hunter-gatherers. *Nature*, 481(2012) 497–501

[3] S. N. Dorogovtsev, A. V. Goltsev, J. F. F. Mendes, Critical phenomena in complex networks. *Rev. Mod. Phys.*, 80(2008) 1275–1335

[4] L. Li, D. Alderson, J. C. Doyle, W. Willinger, Towards a theory of scale-free graphs: definitions, properties, and implications. *Internet Math.*, 2(2005) 431–523

[5] I. Farkas, I. Derényi, H. Jeong, Z. Néda, A. N. Oltvai, E. Ravasz, A. Schubert, A.-L. Barabási, T. Vicsek, Networks in life: scaling properties and eigenvalue spectra. *Physica A*, 314(2002) 25–34

[6] Y. Shang, A note on the 2-connectivity in one-dimensional ad hoc networks. *Sci. China Inf. Sci.*, 54(2011) 123–128

[7] L. Gu, X. D. Zhang, Q. Zhou, Consensus and synchronization problems on small world networks. *J. Math. Phys.*, 51(2010) 082701

[8] D. J. Watts, S. H. Strogatz, Collective dynamics of "small world" networks. *Nature*, 393(1998) 440–442

[9] S. N. Dorogovtsev, J. F. F. Mendes, *Evolution of Networks: From Biological Nets to the Internet and World Wide Web*. Oxford University Press, New York, 2003

[10] A. Clauset, C. R. Shalizi, M. E. J. Newman, Power-law distributions in empirical data. *SIAM Review*, 51(2009) 661–703

[11] R. Albert, H. Jeong, A.-L. Barabási, Error and attack tolerance of complex networks. *Nature* 406(2000) 378–382

[12] B. Bollobás, O. Riordan, Robustness and vulnerability of scale-free random graphs. *Internet Math.*, 1(2003) 1–35

[13] P. Holme, B. J. Kim, C. N. Yoon, S. K. Han, Vertex overload breakdown in evolving networks. *Phys. Rev. E*, 65(2002) 066109

[14] Y. Shang, Perturbation results for the Estrada index in weighted networks. *J. Phys. A: Math. Theor.*, 44(2011) 075003

[15] Y. Shang, W. Luo, S. Xu, L-hop percolation on networks with arbitrary degree distributions and its applications. *Phys. Rev. E*, 84(2011) 031113

[16] T. Tanizawa, G. Paul, R. Cohen, S. Havlin, H. E. Stanley, Optimization of network robustness to waves of targeted and random attacks. *Phys. Rev. E*, 71(2005) 047101

[17] J. Wu, Y. Tan, H. Deng, D. Zhu, Y. Chi, Relationship between degree-rank distributions and degree distributions of complex networks. *Physica A*, 383(2007) 745–752

[18] J. Wu, H. Deng, Y. Tan, D. Zhu, Vulnerability of complex networks under intentional attack with incomplete information. *J. Phys. A: Math. Theor.*, 40(2007) 2665–2671

[19] A. L. Lloyd, R. M. May, How viruses spread among computers and people. *Science*, 292(2001) 1316–1317

[20] A. P. Quayle, A. S. Siddiqui, S. J. M. Jones, Preferential perturbation and network topology. *Physica A*, 371(2006) 823–840

[21] Z. Dezsó, A.-L. Barabási, Halting viruses in scale-free networks. *Phys. Rev. E*, 65(2002) 055103

[22] P. Holme, Efficient local strategies for vaccination and network attack. *Europhys. Lett.*, 68(2004) 908–914

[23] J. Li, J. Wu, Y. Li, H. Deng, Y. Tan, Optimal attack strategy in random scale-free networks based on incomplete information. *Chin. Phys. Lett.*, 28(2011) 068902

[24] Y. Shang, Robustness of scale-free networks under attack with tunable grey information. *EPL*, 95(2011) 28005

[25] M. E. J. Newman, S. H. Strogatz, D. J. Watts, Random graphs with arbitrary degree distributions and their applications. *Phys. Rev. E*, 64(2001) 026118

[26] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, D. J. Watts, Network robustness and fragility: percolation on random graphs. *Phys. Rev. Lett.*, 85(2000) 5468–5471

[27] M. Molloy, B. Reed, A critical point for random graphs with a given degree sequence. *Ramdom Struct. Algor.*, 6(1995) 161–180