PHYSICAL REVIEW E **72**, 025104(R) (2005)

# Tolerance of scale-free networks against attack-induced cascades

Liang Zhao,[1,2] Kwangho Park,[3] Ying-Cheng Lai,[3] and Nong Ye[4]
[1]*Department of Mathematics and Statistics, Arizona State University, Tempe, Arizona 85287, USA*
[2]*Institute of Mathematics and Computer Science, University of São Paulo, Brazil*
[3]*Department of Electrical Engineering, Arizona State University, Tempe, Arizona 85287, USA*
[4]*Department of Industrial Engineering, Arizona State University, Tempe, Arizona 85287, USA*

(Received 1 February 2005; published 31 August 2005)

Scale-free networks can be disintegrated by attack on a *single* or a very few nodes through the process of cascading failures. By utilizing a prototype cascading model, we previously determined the critical value of the capacity parameter below which the network can become disintegrated due to attack on a single node. A fundamental question in network security, which has not been addressed previously but may be more important and of wider interest, is how to design networks of finite capacity that are safe against cascading breakdown. Here we derive an upper bound for the capacity parameter, above which the network is immune to cascading breakdown. Our theory also yields estimates for the maximally achievable network integrity via controlled removal of a small set of low-degree nodes. The theoretical results are confirmed numerically.

DOI: 10.1103/PhysRevE.72.025104 PACS number(s): 89.75.Hc, 05.10.−a, 89.20.Hh

Security of complex networks in response to random failures or attacks has become a topic of recent interest [1–7]. Complex networks arising in many natural and manmade systems are scale free [8] in that their connectivity (or degree) distributions follow an algebraic law. In contrast to an exponential degree distribution seen in random networks [9], an algebraic degree distribution means that a small set of nodes can have significantly more links than other nodes and they therefore can be regarded as more important. From the standpoint of security, the presence of such a small set of important nodes means that the network can be fragile because attack on one or a few nodes in this group can have a devastating effect. In particular, considering that those nodes typically handle a substantial fraction of loads necessary for the normal operation of the network, an attack to disable one or few of these nodes means that their loads will be redistributed to other nodes. Because the amount of the redistributed loads can typically be large, this can cause other nodes in the network to fail, if their loads exceed their capacities, which in turn causes more loads to be redistributed, and so on. This cascading process can continue until the network becomes disintegrated. Indeed, simulations show, for instance, that for a realistic power-grid network, attack on a single node can disable more than half of the nodes, essentially shutting down the network [6].

In a recent work [7], it was proposed that cascade-induced breakdown of a scale-free network exhibits a phase-transition phenomenon with respect to a parameter $\lambda$ characterizing the network capacity. For small capacity, intentional attack on a single node with relatively large degree can trigger a global cascade to disintegrate the network. For sufficiently large capacity, however, additional loads from the disabled nodes due to attack can be effectively absorbed by the network so that it will remain connected. For a finite, unprotected scale-free network under attack on the most influential node, two critical points of the network capacity parameter are of general interest: $\lambda_c$ and $\lambda_s > \lambda_c$, where $\lambda_c$ is the parameter value below which the network becomes totally disintegrated and $\lambda_s$ denotes the upper bound in the capacity above which the network is immune to global cascades. For $1 < \lambda < \lambda_s$, cascading breakdown of the network is likely but, as we will show later, using a proper protection mechanism can effectively prevent such breakdown. Our recent work [7] presented a method to determine $\lambda_c$. However, from the standpoint of designing safe networks against cascading breakdown, $\lambda_s$ is a more important parameter. The first question we ask here is how to theoretically determine $\lambda_s$ for scale-free networks.

A closely related issue that may be of significant interest concerns practical strategies to prevent catastrophic cascades caused by attacks. A simple and intuitive method is to lower the average loads present in the network. This can be achieved by removing a small set of nodes that contribute to the loads in the network but they themselves otherwise process little load [10]. Removal of these nodes and all links connected to them will not affect the functioning of the network but will help enhance the load tolerance for each remaining node. When an intentional attack occurs to disable one or a few influential nodes in the network, the load to some remaining node will increase but, because of the extra capacity gained through control, failure is less likely, thereby helping prevent the spread of the failure or cascading. It was demonstrated for scale-free networks that cascades can be prevented or their sizes can be reduced significantly by intentionally removing a carefully selected small fraction of nodes [10]. The criteria to select these nodes are that they should have small loads but their links should carry a large excess of loads. To be more specific, let $\rho$ be the fraction of intentionally removed nodes. As $\rho$ is increased from zero, the network becomes more robust against global cascades (to be quantified below). However, this trend cannot continue indefinitely, for the network will become disintegrated (even without any attack) if $\rho$ is too large. There exists then a critical value $\rho_c$ for which the network's ability to sustain attack-induced cascading breakdown reaches maximum. This interesting phenomenon was recently discovered by Motter [10]. With the potential utility of this phenomenon in network design, it is useful to be able to determine the critical value $\rho_c$ theoretically. This is the second question to be addressed in this paper.

In this paper, we present a theoretical analysis and numerical support to address the above two questions. By focusing on the load distribution and its scaling, we are able to show that the intentional removal of a small set of low-degree nodes is equivalent to increasing the value of capacity parameter $\lambda$, which makes the network more robust against global cascades. Interestingly, we find that, after proper rescaling using factors that involve both parameters $\lambda$ and $\rho$, the degree of the network integrity as a function of $\lambda$ follows a universal relation, regardless of the value of $\rho$, insofar as it is small. Our theory yields simple formulas that can be used to numerically determine $\lambda_s$ and $\rho_c$. Considering the great importance of attack-induced global cascades in complex networks, our work can be of wide interest as it represents a step toward a systematic understanding of the security issue in complex networks.

We consider a prototype model based on load dynamics for cascading in complex networks as proposed in Ref. [6]. The load (or betweenness) at a node $i$ is defined as the total number of shortest paths passing through this node [11,12]. The capacity of a node is the maximum load that the node can handle, which is assumed to be proportional to its initial load [6]: $C_i=\lambda L_0(i)$, where the constant $\lambda \geqslant 1$ is the capacity parameter. Removal of nodes in general changes the loads on other nodes. For a particular node, if the load on it increases and becomes larger than its capacity, the node fails. Any failure leads to a redistribution of loads over the network and, as a result, subsequent failures can occur. The failures can stop without largely affecting the network connectivity but can also propagate and shut down a considerable fraction of the whole network. Cascading failures can be conveniently quantified by the relative size of the largest connected component $G=N'/N$, where $N$ and $N'$ are the numbers of nodes in the largest connected component before and after the cascade, respectively. The integrity of the network is maintained if $G\approx 1$, while breakdown at a global scale occurs if $G\approx 0$.

To clearly distinguish various network states, we use the following notation. The original scale-free network is denoted by $\mathcal{W}^0$. The corresponding network with intentional removal in the absence of attack is $\mathcal{W}^R$, and the unprotected network after an attack on the most connected node is $\mathcal{W}^A$. Finally, the network state under the attack and with protection is denoted by $\mathcal{W}^F$. For a scale-free network, its load distribution obeys algebraic scaling with the degree variable $k$ [7,12,13]: $L(k)=bk^{\eta}$, where $\eta$ and $b$ are positive constants. After removing a small fraction of low-degree nodes, the average connectivity of the network changes little. Moreover, the degree distribution remains algebraic with approximately the same scaling exponent, which can be seen, as follows. On average, the load reduction due to the removal of a low-degree node is proportional to its original load. Let $L(k_1)$ and $L(k_2)$ be the average loads of the original network $\mathcal{W}^0$ on nodes of degree $k_1$ and $k_2$, respectively. After the removal, the average loads of the network $\mathcal{W}^R$ are $L'(k_1')=L(k_1)-c_1L(k_1)$ and $L'(k_2')=L(k_2)-c_2L(k_2)$, respectively, where $k_1'$ and $k_2'$ are the new degrees. Since $c_1\approx c_2$, we have $L'(k_1')/L'(k_2')\approx L(k_1)/L(k_2)$. Thus, the algebraic scaling exponent of $\mathcal{W}^R$ assumes approximately the same value as in the original network $\mathcal{W}^0$: $\eta' \approx \eta$. The network remains scale-free, and the load distribution of $\mathcal{W}^R$ can be written as $L'(k)=b'k^{\eta'}\approx b'k^{\eta}$. This property has been confirmed by our numerical simulations (to be shown below).

We can now determine the relation between the load distributions before and after the protection by removing a fraction of $\rho$ low-degree nodes, in the absence of any attack. For convenience, all nodes in the network are labeled by integers from 1 to $N$, while the removed nodes are labeled by $(1-\rho)N+1$ to $N$. The total load in $\mathcal{W}^0$ can be written as $S=\Sigma_{i=1}^{(1-\rho)N}L_i+\Sigma_{i=N(1-\rho)+1}^{N}L_i\equiv S_0+S_1$, where $S_0$ is the sum of loads of the remaining nodes before the removal and $S_1$ is the total load of the nodes to be removed. Because the nodes to be removed have relatively low degrees, we have $S_0 \gg S_1$ and, hence, $S\approx S_0=\Sigma_{i=1}^{N(1-\rho)}L_i$. After the removal, the total load of the network $\mathcal{W}^R$ is $S'=\Sigma_{i=1}^{N(1-\rho)}L_i'\approx\Sigma_{i=1}^{N(1-\rho)}\sigma L_i$, where $0<\sigma<1$ is a shifting constant. Since $S=N(N-1)D\approx N^2D$, $S'=N(1-\rho)[N(1-\rho)-1]D'\approx(1-\rho)^2N^2D'$ and $D\approx D'$, where $D$ and $D'$ are the diameters of $\mathcal{W}^0$ and $\mathcal{W}^R$, respectively, we have $\sigma\approx(1-\rho)^2\approx 1-2\rho$. Thus, on average, the load of node $i$ after the removal becomes $L_i-2\rho L_i$. The load tolerance (total number of extra shortest paths passing through node $i$ without causing failure of node $i$) before and after intentional removal, is $(\lambda-1)L_i$ and $(\lambda-1+2\rho)L_i$, respectively. It means that, after the removal, the node will not fail unless the load increment due to an attack exceeds $(\lambda-1+2\rho)L_i$. Controlled removal of a fraction of $\rho$ low-degree nodes is thus equivalent to increasing the parameter $\lambda$ to $\lambda+2\rho$ in the original network. We have

$$\bar{\lambda}\approx\lambda+2\rho. \tag{1}$$

We now examine the effect on $G^F$ ($G$ in $\mathcal{W}^F$) by removing the most connected node and a $\rho$ fraction of low-degree nodes. In general, $G^F$ depends on both $\lambda$ and $\rho$, so we write $G^F(\lambda,\rho)$. Without the controlled removal (in $\mathcal{W}^A$), $G^F$ depends on $\lambda$ only and we write $G^F(\lambda,0)\equiv G^A(\lambda)$. As $\rho$ is increased from zero (in $\mathcal{W}^F$), the equivalent enhancement of the network capacity can result in an increase in $G$. This effect is important for small $\rho$ values. However, for larger values of $\rho$, because of the protection offered by the controlled removal, cascading failures tend to affect only a small set of nodes so that the probability for an intentional attack to trigger a global cascading process is small. The effect on $G^F$ is then simply a linear decrease with $\rho$. This line of thinking suggests

$$G^F(\lambda,\rho)\approx G^A(\lambda+2\rho)(1-\rho). \tag{2}$$

The interesting observation is that the rescaled quantity $G^F(\lambda,\rho)/(1-\rho)$ vs $\bar{\lambda}\equiv\lambda+2\rho$ should be independent of $\rho$.

Equation (2) can be used to estimate $\lambda_s$ of network state $\mathcal{W}^A$. To accomplish this it is helpful to examine the physical meaning of $\lambda_s$. By definition, $\lambda_s$ is the critical capacity parameter value above which the network is resilient to global cascades even for $\rho=0$, i.e., without any protection. For $\lambda\lesssim\lambda_s$, in the event of attack, it is necessary to intentionally

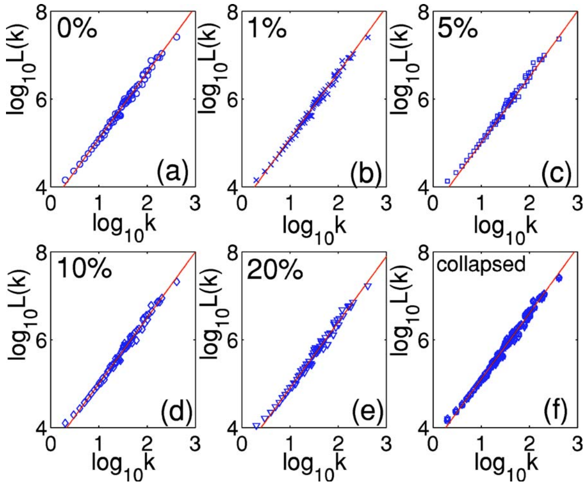

FIG. 1. (Color online) (a) Algebraic scaling of the load distribution $L(k)$ for a scale-free network of $N=10000$ nodes, $\gamma=3$, and $\langle k\rangle=4$. (b)–(e) Load distributions after removing 1%, 5%, 10%, and 20% of the lowest-degree nodes. (f) Rescaled plots of all curves in (a)–(e). The algebraic scaling exponent is $\eta\approx 1.5$.

remove a small fraction of nodes to protect the network. That is, in this case for fixed λ the relative size $G^F(\lambda,\rho)$ should increase with $\rho$, insofar as it is small. We then have $\partial G^F/\partial\rho|_{\lambda\lesssim\lambda_s,\rho=0}\gtrsim 0$. However, for $\lambda\gtrsim\lambda_s$, the network is secure against cascading breakdown and, hence, removing a small fraction of nodes would simply reduce $G^F(\lambda,\rho)$ by a proportional amount. We have $\partial G^F/\partial\rho|_{\lambda\gtrsim\lambda_s,\rho=0}\lesssim 0$. We see that $\lambda_s$ is the critical value of the capacity parameter for which an infinitesimal increment of $\rho$ does not change $G$: $\partial G^F/\partial\rho|_{\lambda=\lambda_s,\rho=0}=0$. Utilizing this fact and performing Taylor expansion of both sides of Eq. (2) to first order in $\rho$, we obtain

$$\left.\frac{dG^A}{d\lambda}\right|_{\lambda=\lambda_s}\approx\frac{G^A(\lambda_s)}{2}. \qquad (3)$$

Equation (3) means that $\lambda_s$ is the point when the slope of $G^A$ decreases to be equal to half of $G^A$. Thus, $\lambda_s$ can be estimated implicitly.

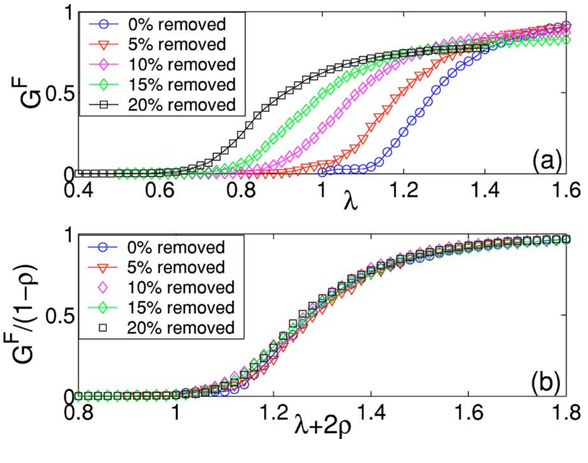

FIG. 2. (Color online) For a scale-free network with $N=3000$, (a) $G^F(\lambda,\rho)$ vs λ for five different values of $\rho$ and (b) properly rescaled plots that exhibit a universal relation.

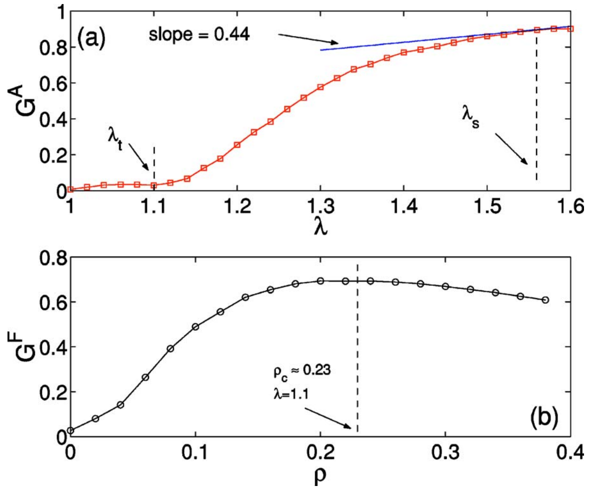

FIG. 3. (Color online) For the scale-free network in Fig. 2(a), (a) $G^A(\lambda)$ vs λ, to which Eq. (3) can be applied for estimating $\lambda_s$. (b) $G^F(\lambda,\rho)$ vs $\rho$ for $\lambda=1.1$, which gives $\rho_c\approx 0.23$. In both panels, the data points were the result of averaging over 30 network realizations.

Having determined $\lambda_s$ of $\mathcal{W}^A$ from Eq. (3), we can obtain the value of $\rho_c$ of $\mathcal{W}^F$ for which $G(\lambda,\rho)$ reaches maximum for fixed value of λ. Let $\lambda_0$ denote the initial value of the network capacity. Controlled removal of a $\rho_c$ fraction of low-degree nodes is equivalent to increasing $\lambda_0$ to $\lambda_s$ with $\rho=0$. This gives $\lambda_s\approx\lambda_0+2\rho_c$ or

$$\rho_c\approx(\lambda_s-\lambda_0)/2. \qquad (4)$$

We now present numerical support for our theoretical results Eqs. (3) and (4). We generate scale-free networks with degree exponent $\gamma=3$ and average connectivity $\langle k\rangle=4$ by using the standard Barabási-Albert model [8]. The shortest paths and the load distribution $L(k)$ are computed by using the algorithm due to Newman [11]. Figure 1(a) shows the algebraic scaling of the load distribution of the network without any removal of nodes. Approximately the same scaling behavior is observed when some small fractions of nodes with the lowest degrees are removed (without attack), as shown in Figs. 1(b)–1(e) for $\rho=1\%$, 5%, 10%, and 20%, respectively. That the intentional removal of a small set of nodes does not change the algebraic load distribution can be seen more clearly in Fig. 1(f), where all plots in Figs. 1(a)–1(e), rescaled by some proper constants, apparently collapse into a single curve. In particular, the algebraic scaling exponent $\eta$ remains approximately the same, regardless of the value of $\rho$.

Figure 2(a) shows $G^F(\lambda,\rho)$ vs λ for different values of $\rho$, where an attack on the node with the largest degree is assumed. We see that the curves shift toward the left as $\rho$ is increased from zero, indicating that the network is more robust against cascading breakdown. This clearly illustrates the protective role played by selectively removing a small set of low-degree nodes. Figure 2(b) shows that the relation between the rescaled quantities $G^F(\lambda,\rho)/(1-\rho)$ and $\lambda+2\rho$ is independent of the value of $\rho$, as predicted. In the original network $\mathcal{W}^0$, the capacity of each node is defined as

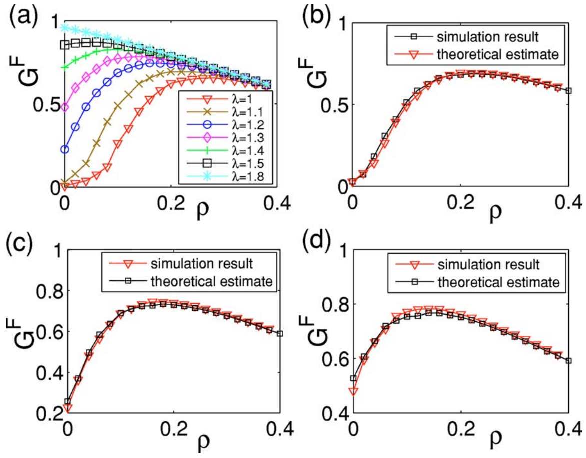

FIG. 4. (Color online) For the scale-free network in Fig. 2, (a) $G^F$ as a function of $\rho$ for different values of $\lambda$ and (b)–(d) the same curve for $\lambda = 1.1$, 1.2, and 1.3 obtained through two approaches: Eq. (2) and direct numerical simulation.

$C_i = \lambda L_i(0)$. If $\lambda < 1$, the network will break down immediately because the capacities of all nodes are less than their respective loads. Thus, $\lambda < 1$ is not a physically meaningful setting. However, with controlled removal, the new load of each remaining node decreases such that it would be still smaller than its capacity even if the capacity parameter $\lambda$ is less than 1, i.e., cascading breakdown may not happen for $\lambda < 1$. It is in this sense that we can study the behavior of the network state $\mathcal{W}^F$ even for $\lambda < 1$, as shown in Fig. 2.

Figure 3(a) illustrates the estimation of $\lambda_s$ from the relation $G^A(\lambda)$ by using Eq. (3) for the scale-free network in Fig. 2. We obtain $\lambda_s \approx 1.56$. Assuming (arbitrarily) that the initial capacity of the network is $\lambda_0 = 1.1$, we obtain from Eq. (4) $\rho_c \approx 0.23$, the fraction of removed nodes that can give the maximum degree of protection against cascading breakdown. Figure 3(b) shows, for $\lambda = 1.1$, $G^F(\lambda, \rho)$ vs $\rho$, which gives $\rho_c \approx 0.23$, in good agreement with the predicted value.

To provide further support for our theoretical analysis, we plot in Fig. 4(a) the ratio $G$ versus $\rho$ for a set of different values of $\lambda$. We see that if $\lambda \geqslant 1.5 \approx \lambda_s$, the network is already safe against cascading breakdown. In such cases the protective scheme by selective node removal simply causes an approximately linear decrease in $G^F$. Figure 4(b) shows, for $\lambda = 1.1$, the curves $G^F(\lambda, \rho)$ obtained from our theory Eq. (2) and from direct numerical simulation, which agree with each other reasonably well.

In summary, we have addressed quantitatively what it takes for a scale-free network to be robust against global cascading breakdown as caused by an attack on a single node. By analyzing the dynamics of load redistribution resulted from selectively removing a small set of low-degree nodes, we obtained a criterion which allows the minimum value of the capacity parameter for cascade-free scale-free networks and the optimal fraction of intentionally removed nodes to be determined. Cascading breakdown of complex networks can be catastrophic in a modern society. Our work represents a step toward understanding the dynamical mechanism of cascades and devising protective schemes in this important area of network security.

This work was supported by NSF under Grant No. ITR-0312131 and by AFOSR under Grant No. F49620-01-1-0317.

[1] R. Albert, H. Jeong, and A.-L. Barabási, Nature (London) **406**, 378 (2002).

[2] R. Cohen, K. Erez, D. b-Avraham, and S. Havlin, Phys. Rev. Lett. **85**, 4626 (2000); **86**, 3682 (2001).

[3] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys. Rev. Lett. **85**, 5468 (2000).

[4] S. N. Dorogovtsev and J. F. F. Mendes, Phys. Rev. Lett. **87**, 219801 (2001).

[5] P. Holme and B. J. Kim, Phys. Rev. E **65**, 066109 (2002); P. Holme, *ibid.* **66**, 036119 (2002).

[6] A. E. Motter and Y.-C. Lai, Phys. Rev. E **66**, 065102(R) (2002).

[7] L. Zhao, K. Park, and Y.-C. Lai, Phys. Rev. E **70**, 035101(R) (2004); E. J. Lee, K.-I. Goh, B. Kahng, and D. Kim, e-print cond-mat/0410684.

[8] A.-L. Barabási and R. Albert, Science **286**, 509 (1999); A.-L. Barabási, R. Albert, and H. Jeong, Physica A **272**, 173 (1999).

[9] P. Erdös and A. Rényi, Publ. Math., Inst. Hautes Etud. Sci. **5**, 17 (1960).

[10] A. E. Motter, Phys. Rev. Lett. **93**, 098701 (2004).

[11] M. E. J. Newman, Phys. Rev. E **64**, 016132 (2001); Proc. Natl. Acad. Sci. U.S.A. **98**, 404 (2001).

[12] K.-I. Goh, B. Kahng, and D. Kim, Phys. Rev. Lett. **87**, 278701 (2001); M. Barthélemy, *ibid.* **91**, 189803 (2003); K.-I. Goh, C.-M. Ghim, B. Kahng, and D. Kim, *ibid.* **91**, 189804 (2003).

[13] K. Park, Y.-C. Lai, and N. Ye, Phys. Rev. E **70**, 026109 (2004).