PRAMANA
— journal of
physics

Vol. 64, No. 4
April 2005
pp. 483–502

Complex networks: Dynamics and security

YING-CHENG LAI[1], ADILSON MOTTER[2], TAKASHI NISHIKAWA[3], KWANGHO PARK[4] and LIANG ZHAO[5]

[1]Department of Electrical Engineering, Arizona State University, Tempe, Arizona 85287, USA

[2]Max-Planck Institute for Physics of Complex Systems, Nothnitzer Strasse 38, 01187 Dresden, Germany

[3]Department of Mathematics, Southern Methodist University, Dallas, TX 75275-0156, USA

[4]Department of Mathematics and Statistics, Arizona State University, Tempe, Arizona 85287, USA

[5]Institute of Mathematics and Computer Science, University of Sao Paulo, Brazil

E-mail: yclai@chaos1.la.asu.edu; motter@mpipks-dresden.mpg.de; tnishi@chaos6.la.asu.edu; kpark@chaos21.eas.asu.edu; zhao@math.la.asu.edu

Abstract. This paper presents a perspective in the study of complex networks by focusing on how dynamics may affect network security under attacks. In particular, we review two related problems: attack-induced cascading breakdown and range-based attacks on links. A cascade in a network means the failure of a substantial fraction of the entire network in a cascading manner, which can be induced by the failure of or attacks on only a few nodes. These have been reported for the internet and for the power grid (e.g., the August 10, 1996 failure of the western United States power grid). We study a mechanism for cascades in complex networks by constructing a model incorporating the flows of information and physical quantities in the network. Using this model we can also show that the cascading phenomenon can be understood as a phase transition in terms of the key parameter characterizing the node capacity. For a parameter value below the phase-transition point, cascading failures can cause the network to disintegrate almost entirely. We will show how to obtain a theoretical estimate for the phase-transition point. The second problem is motivated by the fact that most existing works on the security of complex networks consider attacks on nodes rather than on links. We address attacks on links. Our investigation leads to the finding that many scale-free networks are more sensitive to attacks on short-range than on long-range links. Considering that the small-world phenomenon in complex networks has been identified as being due to the presence of long-range links, i.e., links connecting nodes that would otherwise be separated by a long node-to-node distance, our result, besides its importance concerning network efficiency and security, has the striking implication that the small-world property of scale-free networks is mainly due to short-range links.

Keywords. Scale-free network; network security; attacks; cascading breakdown; phase transition.

PACS Nos 89.75.Hc; 89.20.Hh; 05.10.-a

1. Introduction

Complex networks [1] such as the internet, the electrical power grid, the transportation network etc., are an essential part of a modern society. The security of such a network under random or intentional attacks is of great concern. Recently, an interdisciplinary field among information science and engineering, statistical and nonlinear physics, applied mathematics, and social science has emerged, which brings novel concepts and approaches to the study of complex networks. Issues such as the characterization of the network architecture, dynamics on complex networks, and the effect of attacks on network operation have begun to be addressed. A central point of this review is that the flows of information and other physical quantities in the network can be critically important for network security. This dynamical aspect of the security problem, despite its highly practical relevance, has not been addressed adequately so far. Here, we shall present our initial results in this direction.

Two key concepts in the characterization of complex networks are the small-world [2] and the scale-free [3,4] properties. Large natural or man-made networks are always evolving in that nodes and links are continuously added to and/or deleted from the network. Networks are growing if, on average, the numbers of nodes and links increase with time. Most large networks are sparse, that is, the average number of links per node is much smaller than the total number of nodes in the network. The small-world concept is static in the sense that it does not describe the growth of the network typically seen in nature. Two statistical quantities characterizing the small-world property are the clustering coefficient C and the average network distance L, where the former is the probability that any two nodes are connected to each other, given that they are both connected to a common node, and the latter measures the average minimal number of links connecting any two nodes in the network. Regular networks have high clustering coefficients and large network distances, and random networks are at the opposite of the spectrum of architecture with small network distance and low clustering coefficients [5]. Small-world networks fall somewhere in between these two extremes [2,6]. In particular, a network is small-world if its clustering coefficient is as high as that of a regular network but its average network distance is as small as that of a random network with the same parameters. Watts and Strogatz demonstrated that a small-world network can be constructed by adding to a regular network a few additional random links connecting otherwise distant nodes. The scale-free property, on the other hand, is defined by an algebraic behavior in the probability distribution $P(k)$ of the random variable K, which measures the number of links at a node in the network:

$$P(k) \sim k^{-\gamma}, \tag{1}$$

where $\gamma > 0$ is the scaling exponent. The scale-free property is dynamic because it is the consequence of the natural evolution of the network. The ground-breaking work by Barabási and Albert [3] demonstrates that the algebraic distribution in the connectivity of a scale-free network arises due to the two basic mechanisms in the evolution of the network: growth and preferential attachment, where the former means that the number of nodes in the network increases with time on average

and the latter stipulates that the probability for a new node to be connected to an existing node is proportional to the number of links that this node already has.

A convenient way to address the security of a complex network is to examine how the average network distance, which is somewhat related to the efficiency of communication (or information flow) within the network, is changed under random or intentional attacks [7–10]. Generally, the average distance will not be affected by the removal of a random subset of nodes, but it will increase significantly if the removed nodes are among the most connected ones [7–11]. Most existing studies on network security address mainly static properties, i.e., the effect of different network architectures on the connectivity under attacks. Our concern is that network architecture represents only one aspect of the security problem. How attacks affect the functions of a network, when the flows of information and other physical quantities in the network are taken into consideration, is important and may be more relevant to real-world situations. In particular, we speculate that for many physical networks, the removal of nodes can have a much more devastating consequence when the intrinsic dynamics of flows of physical quantities in the network are taken into account. In a power transmission grid, for instance, each node (power station) deals with a load of power. The removal of nodes, either by random breakdown or by intentional attacks, changes the balance of flows and leads to a global redistribution of loads over all the network. This can trigger a cascade of overload failures [12,13], as the one that happened on August 10, 1996 in the western United States power grid [14,15]. Another example is the Internet [16–18], where the load represents the amount of information a node (e.g., a router) is requested to transmit per unit of time, and overloads correspond to congestion [19]. Internet collapses caused by congestion have been reported since its very beginning [20]. We will first introduce a model for avalanching failures in complex networks and show that it is applicable to realistic networks such as the Internet and power grids. We will then address theoretically and numerically the fundamental mechanism of cascading breakdown. To make analysis amenable, we focus on scale-free networks and investigate cascades triggered by attack on a single node. We will show that cascading breakdown in scale-free networks can be understood in terms of a phase transition. In particular, let α be the tolerance parameter characterizing the capacity of nodes in the network. Cascading breakdown due to attack on a single node is possible only when α is below a critical value α_c. By making use of the degree distribution of scale-free networks and the concept of betweenness [21,22] to characterize the load distribution, we are able to derive a theoretical formula for estimating the phase-transition point α_c, which is verified by numerical experiments. In terms of practical utility, our result enables a possible implementation of predicting and preventing mechanism for cascading breakdown in scale-free networks.

Most existing works on the security of scale-free networks consider attacks on nodes rather than on links (exceptions are refs [23] and [24], to our knowledge). We believe that attacks on links are as important for the network security as those on nodes, and therefore deserve a careful investigation. As we will show, studying the effect of attacks on links can provide an understanding to the fundamental question of why scale-free networks are typically highly efficient. In particular, the efficiency of a scale-free network is determined by the average network distance between nodes. It has been assumed that long-range connections are responsible

for the small average network distance observed in these networks. The intuition is then that scale-free networks are much more sensitive to attacks on long-range than those on short-range links. We will show that in fact, the opposite is true. Thus, the small-world property of scale-free networks is caused by short-range links.

This review is organized as follows. In §2, we introduce a simple model to address the issue of attack-induced avalanches in complex networks [25]. In §3, we present a theory and numerical support to place the cascading phenomenon in the context of phase transition. Range-based attacks on links and the origin of the small-world property in scale-free networks [26] are detailed in §4. A discussion is presented in §5.

2. Attack-induced avalanches in complex networks

Complex networks such as the world-wide web (WWW), the Internet, and electrical power grids, present a surprisingly small average distance between nodes and a highly organized distribution of links per node [2,3,7]. The existence of a giant connected component in the network, however, does not depend on the presence of highly connected nodes. For instance, the WWW has homepages with many thousands of hyperlinks and can remain well-connected after the removal of all homepages with five or more hyperlinks [11]. In addition, the giant component itself is typically a small-world network [6] even after the removal of all highly connected nodes [27]. These pioneering studies on network security address mainly static properties, i.e., the effect of different network architectures. They suggest that the network connectivity, and hence its functionability, is robust against random failure of nodes [7–9] and to some extent is even robust against intentional attacks [11,27]. However, when the intrinsic dynamics of flows of physical quantities in the network is taken into account, attack on a few or even a single node can cause the connected nodes to fail in a cascading manner. We have recently introduced [25] a model for avalanching failure in complex networks and shown that it is applicable to realistic networks such as the Internet and power grids.

For a given network, suppose that at each time step one unit of the relevant quantity, which can be information, energy, etc., is exchanged between every pair of nodes and transmitted along the shortest path connecting them. The load at a node is then the total number of shortest paths passing through the node [21,22,28,29]. The capacity of a node is the maximum load the node can handle. In man-made networks, the capacity is severely limited by cost. Thus, it is natural to assume that the capacity C_j of node j is proportional to its initial load L_j,

$$C_j = (1+\alpha)L_j, \quad j = 1, 2, ..., N, \tag{2}$$

where the constant $\alpha \geq 0$ is the tolerance parameter and N is the initial number of nodes. When all the nodes are on, the network operates in a free-flow state insofar as $\alpha \geq 0$. But, the removal of nodes in general changes the distribution of shortest paths. The load at a particular node can then change. If it increases and becomes larger than the capacity, the corresponding node fails. Any failure leads to a new redistribution of loads and, as a result, subsequent failures can occur. This step-by-step process is what we call a cascading failure. It can stop after a few

steps but it can also propagate and shutdown a considerable fraction of the whole network [29a]. A fundamental question is: under what conditions can such a global cascading process take place?

Here we focus on cascades triggered by the removal of a single node. If a node has a relatively small load, its removal will not cause major changes in the balance of loads, and subsequent overload failures are unlikely to occur. However, when the load at the node is relatively large, its removal is likely to affect loads at other nodes significantly and possibly starts a sequence of overload failures. Our results are the following: global cascades occur if (1) the network exhibits a highly heterogeneous distribution of loads; (2) the removed node is among those with higher load. Otherwise, cascades are not expected. The distribution of loads is in turn highly correlated with the distribution of links: networks with heterogeneous distribution of links are expected to be heterogeneous with respect to load so that on average, nodes with larger number of links will have higher load [29]. This result confirms the robust-yet-fragile property of heterogeneous networks, which was first observed in [7] for the attack on several nodes. The avalanching effect is important, however, because a large damage can be caused in this case by the attack on a single node. While a network with more links can be more resistant against avalanching failures, in practice the number of links is limited by cost.

We study cascades triggered by random breakdown and by intentional attacks. To simulate the former, we choose a trigger at random among all the nodes of the network, as can occur in networks such as power grids [14]. In the case of attack the targeted node is selected from those with highest loads or largest degrees (number of links at a node). We consider heterogeneous networks with algebraic (scale-free) distribution P of links, as observed in real systems [3,4,30,31] and compare them with an equivalent homogeneous configuration. These networks are generated according to the procedure in refs [26,32], where the nodes are connected randomly for a given degree distribution, and self- and repeated links are forbidden. The damage caused by a cascade is quantified in terms of the relative size G of the largest connected component

$$G = N'/N, \tag{3}$$

where N and N' are the number of nodes in the largest component before and after the cascade, respectively.

Figure 1 shows the relative size G of the largest component after a cascade, as a function of the tolerance parameter α, for a scale-free network. We see that on average G remains close to unity in the case of random breakdowns but it is significantly reduced under intentional attacks, even for unrealistically large α. Indeed, the size of the largest component is reduced by more than 20% for $\alpha = 1$, i.e., for a capacity as large as two times the capacity required for the system to operate when all the nodes function normally. This result is in agreement with intuition, because in the case of random breakdown the trigger is probably one of the many nodes with small load, while in the case of intentional attack it is a node with very large load. The damage is larger for smaller values of α, as it is for load-based attacks when compared with degree-based attacks. For instance, in the load-based attack for $\alpha = 0.2$, more than 60% of the nodes are affected. For the 5000-node networks used in our simulations, it means that a cascade triggered by the attack on a single node shuts down and disconnects more than 3000 others!

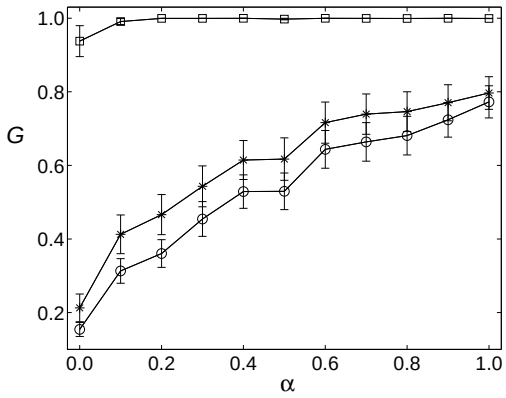

Figure 1. Avalanching failure in scale-free networks, as triggered by the removal of a single node chosen at random (squares), or among those with largest degrees (asterisks) or highest loads (circles), where α is the tolerance parameter and G the relative size of the largest connected component. Each curve corresponds to the average over 5 triggers and 10 realizations of the network. The error bars represent the standard deviation. The networks are generated according to the algebraic distribution (1). For the computations shown we set $\gamma = 3$ and $5000 \leq N \leq 5100$. The average degree in the largest component is $\langle k \rangle \approx 2.0$.

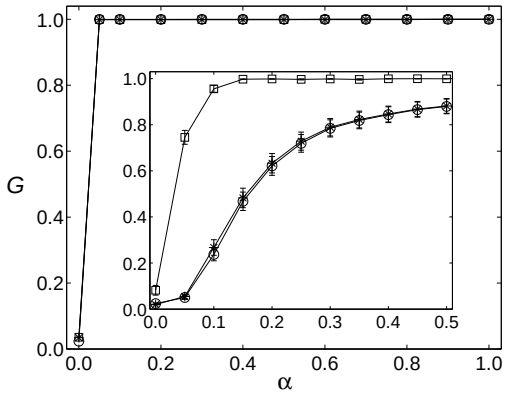

Figure 2. Avalanching failure in homogeneous networks. All nodes are set to have the same degree $k = 3$ and $N = 5000$. In the inset, the networks are generated according to the algebraic distribution (1) for $k \geq 2$, $\gamma = 3$, and $N = 5000$. The resulting average degree is $\langle k \rangle \approx 3.1$. The legends and other parameters are the same as in figure 1.

Figure 2 shows the corresponding results for a homogeneous network with the same number of nodes and exactly three links per node. To make a meaningful comparison we display in the inset results for an algebraic network with about the same average degree (actually larger, which strengthens our conclusions). The homogeneous network does not experience avalanching failures due to either random breakdown or intentional attacks for α as small as 0.05. For the heterogeneous

(scale-free) network, for the same value of α, cascades triggered by the attack on a key node can reduce the largest connected component to less than 10% of the original size, as shown in the inset. Therefore, homogeneous networks appear to be more robust against attacks than the heterogeneous ones. This conclusion does not rely on the particularities of these models, as the same was also observed for classes of networks with exponential and Poisson-like distributions of degrees (e.g., the Erdös–Rényi model [33]): their homogeneity makes them relatively resistant to cascades triggered by attacks. The networks corresponding to the inset of figure 2 are generated according to the same scaling distribution of those in figure 1, except that in this case the minimal number of links at a node is set to be 2. Therefore, this inset shows that the fragility of scale-free networks is due to their heterogeneity and does not rely on the presence of nodes with degree one, which are easily disconnectable. Naturally, the increase of the average degree reduces the damage of the cascade, as can be seen from a comparison between figure 1 and the inset of figure 2.

Many real-world networks are heterogeneous and as such are expected to undergo large-scale cascades if some vital nodes are attacked, but rarely in the case of random breakdown. As an example we consider the Internet at autonomous system level [34], which displays an algebraic distribution of links [7]. The damage caused by triggers of higher load or degree is much larger than that by random breakdown, as shown in figure 3. The avalanching failures are rarely triggered by random breakdown for $\alpha > 0.05$, but more than 20% of the nodes can be disconnected with the intentional attack on only one node for $\alpha \leq 0.4$. We have also considered the electrical power grid of the western United States [35]. The degree distribution in this network is consistent with an exponential [36] and is thus relatively homogeneous. The distribution of loads, however, is more heterogeneous than that displayed by semi-random networks [26,32] with the same distribution of links, indicating that the power grid has structures that are not captured by these models. As a result, global cascades can be triggered by load-based intentional attacks but not by ran-

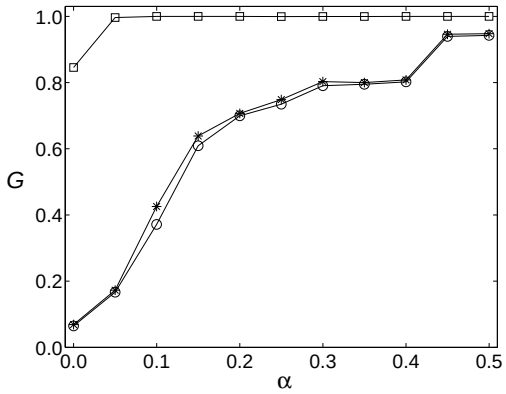

Figure 3. Avalanching failure in the Internet at autonomous system level [34]. The network has $N = 6474$ nodes and $\langle k \rangle \approx 3.88$ links per node, on average. Each curve corresponds to the average over 5 triggers for attacks and 50 for random breakdown. The legends are as defined in figure 1.

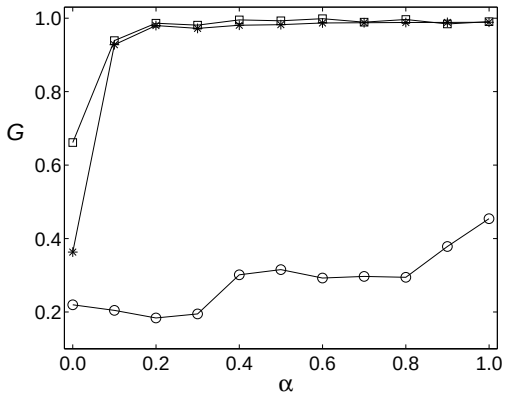

Figure 4. Cascading breakdown in the western US power transmission grid [35], which has $N = 4941$ and $\langle k \rangle \approx 2.67$. The average is obtained via 5 triggers for attacks and 50 for random breakdown. The legends are the same as in figure 1.

dom or degree-based removal of nodes, as shown in figure 4. We see that the attack on a single node with large load reduces the largest connected component to less than a half of its initial size, even when the network is highly tolerant (e.g., $\alpha = 1$).

3. Theory: Phase transition and cascades

To obtain an analytic estimate of the critical value of the tolerance parameter, we focus on the situation where cascading failures are caused by attack on the node with the largest number of links and the failures lead to immediate breakdown of the network. That is, G becomes close to zero after one redistribution of the load. For a node in the network, its load is a function of the degree variable k. For scale-free networks, we have [29,37,38]

$$L(k) \sim k^{\eta}, \tag{4}$$

where $\eta > 0$ is a scaling exponent. To proceed, we write the degree distribution as $P(k) = ak^{-\gamma}$ and the load distribution as $L(k) = bk^{\eta}$, where a and b are positive constants. Let $k_{\max}$ be the largest degree in the network. Before the attack, we have

$$\int_1^{k_{\max}} P(k)\mathrm{d}k = N \quad \text{and} \quad \int_1^{k_{\max}} P(k)L(k)\mathrm{d}k = S, \tag{5}$$

where S is the total load of the network. These two equations give

$$a = \frac{(1-\gamma)N}{[k_{\max}^{1-\gamma} - 1]} \quad \text{and} \quad b = \frac{\beta S}{a(1 - k_{\max}^{-\beta})}, \tag{6}$$

where $\beta \equiv \gamma - \eta - 1$. After the removal of the highest degree node (it is only the first step of the whole cascading process), the degree and load distributions become

$P'(k) = a'k^{-\gamma'}$ and $L'(k) = b'k^{\eta'}$, respectively. Since only a small fraction of nodes are removed from the network, we expect the changes in the algebraic scaling exponents of these distributions to be negligible. We thus write $P'(k) \approx a'k^{-\gamma}$ and $L'(k) \approx b'k^{\eta}$, where the proportional constants a' and b' can be calculated in the same way as for a and b. We obtain $a' = (1-\gamma)(N-1)/[k_{\max}^{1-\gamma} - 1]$ and $b' = \beta S'/a'(1-k_{\max}^{-\beta})$, where S' is the total load of the network after the attack. For nodes with k links, the difference in load before and after the attack can be written as $\Delta L(k) \approx (b'-b)k^{\eta} = (\frac{b'}{b} - 1)L(k)$. Given the capacity $C(k)$, the maximum load increase that the nodes can handle is $C(k) - L(k) = \alpha L(k)$. The nodes still function if $\alpha > (\frac{b'}{b} - 1)$ but they fail if $\alpha < (\frac{b'}{b} - 1)$. The critical value $\alpha_{\rm c}$ of the tolerance parameter is then

$$\begin{aligned}
\alpha_{\rm c} &= \frac{b'}{b} - 1 \\
&\approx \left(\frac{k_{\max'}^{1-\gamma} - 1}{k_{\max}^{1-\gamma} - 1}\right)\left(\frac{1 - k_{\max}^{-\beta}}{1 - k_{\max'}^{-\beta}}\right)\left(\frac{S'}{S}\right) - 1 \\
&\approx \left(\frac{1 - k_{\max}^{-\beta}}{1 - k_{\max'}^{-\beta}}\right)\left(\frac{S'}{S}\right) - 1 \\
&\approx \{1 - (k_{\max}^{-\beta} - k_{\max'}^{-\beta})\}\left(\frac{S'}{S}\right) - 1 \\
&= \left\{1 - k_{\max'}^{-\beta}\left(-1 + \left(\frac{k_{\max}}{k_{\max'}}\right)^{-\beta}\right)\right\}\left(\frac{S'}{S}\right) - 1, \qquad (7)
\end{aligned}$$

where the third line of eq. (7) is obtained from the second line by using the fact $(k_{\max'}^{1-\gamma} - 1)/(k_{\max}^{1-\gamma} - 1) \approx 1$. This is so because both $k_{\max'}^{1-\gamma}$ and $k_{\max}^{1-\gamma}$ approach zero when $N \to \infty$ and $\gamma > 1$. In the limit $N \to \infty$, we have $k_{\max'}^{-\beta} \sim 0$, $k_{\max}/k_{\max'} \sim$ constant, and $S'/S \to 1$, so $\alpha_{\rm c} \approx 0$, indicating that an infinite scale-free network cannot be brought down by a single attack if $\alpha > 0$. On the other hand, for finite-size network, since $k_{\max'}^{-\beta} > 0$, we have $\alpha_{\rm c} > 0$, suggesting that breakdown can occur for $\alpha < \alpha_{\rm c}$. The practical usage of eq. (7) is that it provides a way to monitor the state of (finite) network to assess the risk of cascading breakdown. In particular, the critical value $\alpha_{\rm c}$ can be computed in time and comparison with the pre-designed tolerance parameter value α can be made. If $\alpha_{\rm c}$ shows a tendency of increase and approaches α, early warning can be issued to signal an immediate danger of network breakdown.

To provide numerical support for the theoretical prediction (eq. (7)), we generate scale-free networks using the standard Barabási–Albert model [3], as detailed in ref. [39]. The shortest paths and the load $L(k)$ are computed using the algorithm developed by Newman [21,22]. Figure 5a shows the algebraic scaling of the load for a scale-free network. The scaling exponent of the degree distribution $P(k)$ is $\gamma \approx 3$ (not shown) and the average number of links in the network is $\langle k \rangle = 4$. The open circles in figure 5 indicate the values of the load for the original network. Apparently $L(k)$ follows the expected algebraic distribution, with exponent $\eta \approx 1.6$. Figures 5b and 5c show the exponents η in relation to system size before and after

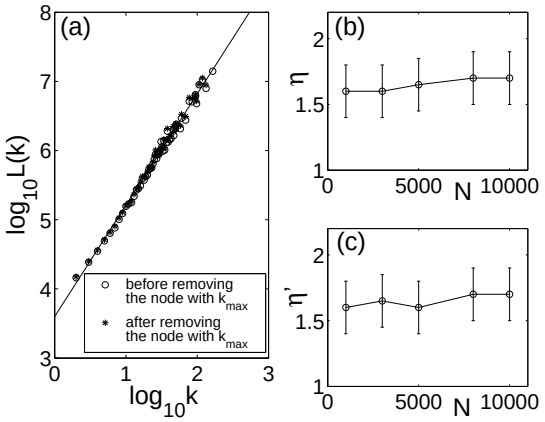

Figure 5. (**a**) Algebraic scaling of the load $L(k)$ for a scale-free network of $N = 10{,}000$ nodes, $\gamma = 3$, and $\langle k \rangle = 4$. The open circles and the asterisks denote the load values before and after an intentional attack that removes the node with the maximum number of links. We have $\eta' \approx \eta \approx 1.6$. (**b,c**) Algebraic scaling exponents of the load in relation to network size, before and after the nodes with the largest degree are removed, respectively. For each network size N, the resulting data were averaged over 25 realizations.

the highest degree node is removed, respectively. In both cases, we obtained $\eta' = \eta = 1.6(2)$. Computer simulations show that the load distribution and cascading behavior observed above holds for various $\langle k \rangle$. To simulate an intentional attack, we remove the node with the maximum number of links ($k_{\max} = 81$ for the realization of the network shown in the figure). The distribution of the load is recalculated after the network stabilizes itself. That is, after the attack the load on the removed node is redistributed to the network and new load to every node is recalculated. Any node with load exceeding its capacity is removed and load is recalculated, and so on, until the process reaches a new equilibrium. The new values of the load are denoted by the asterisks in figure 5. We see that the distribution still follows a power law with approximately the same scaling exponent. This justifies the approximation $\eta' \approx \eta$ used in our theory.

As N is increased, we expect $k_{\max}$ to increase following an algebraic scaling law [39]. This behavior is shown in figure 6a. After the attack and redistribution of load, we find that the ratio $k_{\max}/k'_{\max}$, where $k'_{\max}$ is the new value of the maximum number of links, is constant, regardless of the network size. We also numerically observed that the load ratio S'/S (before and after the attack) is approximately one for large N, as shown in figure 6b.

Figure 7a shows cascading failures when a single node with different degree is removed from the network. We see that, when a node with small degree is removed, the G value remains close to one except when α is close to zero. However, when the node with the largest degree (in this case $k = 81$) is removed, nearly total breakdown of the network, as represented by values of G close to zero, occurs when $\alpha < 0.1$. The phase-transition point α_c is thus about 0.1. With numerical values of $k_{\max} = 81$, $k'_{\max} = 60$, $S \approx 1.86 \times 10^7$ and $S' \approx 1.91 \times 10^7$, theoretically predicted

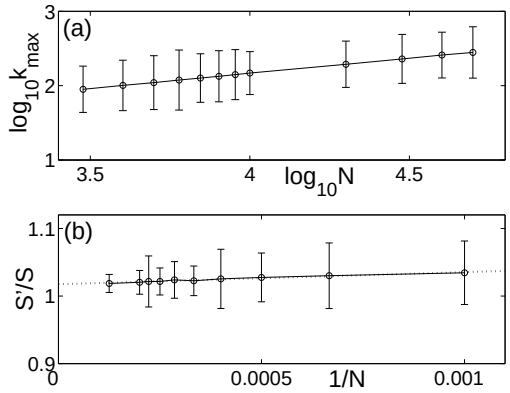

Figure 6. (**a**) Algebraic scaling of $k_{\max}$ with N. For each network size N, 5000 realizations are averaged. (**b**) Load ratio S'/S vs. $1/N$. For each network size N, 25 realizations were averaged.

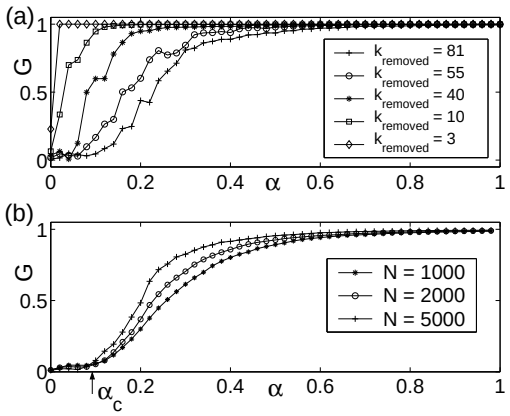

Figure 7. Cascading failure in scale-free network in relation to the tolerance parameter α. (**a**) Removal of the nodes with different number of links for $N = 2000$. In the case of the removal of the node with the highest degree, the phase-transition point is $\alpha_c \approx 0.1$, meaning that for $\alpha < \alpha_c$, the networks disintegrate almost entirely under intentional attack on a single node. (**b**) Phase transitions for networks of different sizes. The resulting data points were averaged over 25 realizations.

value of α_c in eq. (7) gives $\alpha_c \approx 0.1$, which is consistent with numerics. This phase transition phenomenon seems to be robust for different sizes of network, as shown in figure 7b, G vs. α for $N = 1000$, $N = 2000$ and $N = 5000$, respectively.

What about attacks that target more than one node? In this case, we expect that the phase transition will occur for higher values of the tolerance parameter, because it becomes more difficult for the network to maintain its integrity at lower tolerance, as compared with the case of attack on a single node. Figure 8 shows G vs. both α and N_{trigger}, the number of nodes that an attack targets. Here

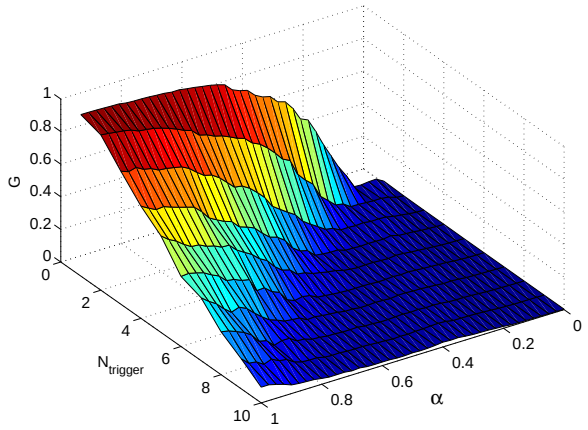

Figure 8. For a scale-free network of $N = 2000$ nodes under attack targeting multiple nodes, G vs. α and $N_{\rm trigger}$, the number of targeted nodes. For each parameter value, G is averaged over 30 realizations.

the removed nodes are those with the highest numbers of links. We see that, as $N_{\rm trigger}$ is increased, the phase-transition point $\alpha_{\rm c}$ also increases. Roughly we have $\alpha_{\rm c} \sim N_{\rm trigger}$. Note that the number of targeted nodes, while more than one, is still far small compared to the total number of nodes in the network. Practically, this means that, even if the network is designed to have a high tolerance by stipulating high capacities for its nodes, cascading failures triggered by attack on a very small subset of nodes are capable of bringing down the entire network.

4. Range-based attacks on links in complex networks

Many real networks have been identified to have an amazingly small average shortest path since Watts and Strogatz (WS) [2] introduced their model of small-world networks. This model is constructed from a sparse regular network by rewiring a small fraction of links at random. Watts [6] introduced the concept of range to characterize different types of links: the range of a link l_{ij} connecting nodes i and j is the length of the shortest path between nodes i and j in the absence of l_{ij} (see also ref. [40]). In this sense, typically, local connections are short-range links but rewired connections are long-range links. A key feature in the WS model is that it clearly identifies the small shortest paths observed in locally structured, sparse networks as being due to long-range connections, while short-range links are responsible for high clustering. This remarkable observation matches very well with the known results for the Erdös–Rényi (ER) model of random graphs [33], where almost all links are long-range connections and the average shortest path increases only logarithmically with the number N of nodes [5]. In regular networks, on the other hand, all the links have small range and the average shortest path increases with a power of N.

The WS and ER models explain some important features of real networks, such as the small-world phenomenon. However, since these models are homogeneous,

their connectivity distribution $P(k)$, where k is the number of links connected to a node, has an exponential tail, in contrast to the algebraic one that characterizes scale-free networks recently discovered in a variety of real-world situations [3,4]. Scale-free networks are heterogeneous as their connectivity can vary significantly from node to node and a considerable number of links can be associated with a few highly connected nodes. As most scale-free networks possess the small-world property, it has been tacitly assumed that long-range connections are responsible for the small average shortest path exhibited by these networks. In addition to the insights provided by the WS model, the main argument for this comes from the observation that the removal of a link l_{ij} of range R increases the length of the shortest path between nodes i and j by $R-1$. The length of the shortest path between nodes connected by a short-range link is then robust against the removal of the link because the second shortest path between these two nodes is still short. But this is not true for long-range links, as they connect nodes that would otherwise be separated by a long shortest path.

Our goal here is to understand the contribution of short-range links to the small-world property in scale-free networks, by analysing the impact of attacks on short-range links vs. those on long-range links. Attack here is defined as the deliberate removal of a subset of selected links. Different aspects of attacks on complex networks have been analysed recently [7,9–11,40–42]. However, to our best knowledge, almost all the previous works consider attacks on nodes rather than on links, with very few exceptions [23,24].

To study range-based attacks on links, we consider the following models of scale-free networks: (1) semi-random model [32]; (2) BA model [3] and its generalization with aging [43]. In each case we generate scale-free networks with the small-world property and a tunable scaling exponent. Because of the small-world property, one might intuitively think that these networks are much more sensitive to attacks on long-range than on short-range links. Surprisingly, our analysis and numerical computation show exactly the opposite for many scale-free networks. This result has an unexpected implication: short-range links are vital for efficient communication between nodes in these networks. Our findings are based on the observation that the average shortest path is a global quantity which is mainly determined by links with large load, where the load of a link is defined as the number of shortest paths passing through the link [29,44]. For scale-free networks with exponent γ in a finite interval about 3, due to heterogeneity, the load is on average larger for links with shorter range, making the short-range attack more destructive. For very large values of γ, the corresponding networks become homogeneous and, as a result, the opposite occurs.

For a given network, our strategy of attack on links is as follows. We first compute the range for all the links. We then measure the efficiency of the network as links are successively removed according to their ranges: for short-range attacks, links with shorter ranges are removed first; for long-range attacks, links with longer ranges are removed first [44a]. In both cases, the choice among links with the same range is made at random. The efficiency is measured by the shortest paths between pairs of nodes. The shortest path between two given nodes i and j is defined as the minimal number d_{ij} of links necessary to follow from one node to the other. A convenient quantity to characterize the efficiency is then

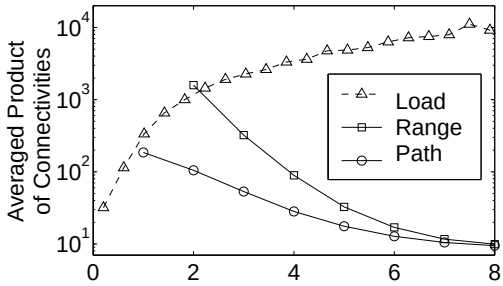

Figure 9. Averaged product of connectivities as a function of the shortest path, range, and load for $\gamma = 3$, where the load is binned and normalized by 10^4. Each curve corresponds to the average over 10 realizations for $N = 5000$, $k_{\min} = 3$, and $k_{\max} = 500$.

$$E = \frac{2}{N(N-1)} \sum \frac{1}{d_{ij}}, \tag{8}$$

where the sum is over all $N(N-1)/2$ pairs of nodes. The network is more efficient when it has small shortest paths, which according to our definition corresponds to large E. Definition (8) was introduced in ref. [45] to generalize the concept of small world, as it applies to any network regardless of its connectedness.

We first consider the semi-random model, as follows. We start with N nodes $\{1, 2, \ldots, N\}$ and a list of N integers representing their connectivities, i.e., the number of end-links of each node: $\{k_1, k_2, \ldots, k_N\}$, where $k_i \leq N-1$ and $\sum_{i=1}^{N} k_i$ is even. In the case of scale-free networks, this connectivity sequence is generated according to the algebraic distribution (1). Next, we pick up pairs of end-links at random and connect them to form a link and repeat this process until the last pair is connected, prohibiting self- and repeated links. In order to have non-trivial networks in the limits of small and large γ, we bound the connectivity so that $k_{\min} \leq k_i \leq k_{\max}$ for $i = 1, 2, \ldots, N$, where $k_{\min}$ and $k_{\max}$ are constant integers. For $\gamma \to \infty$, the network becomes a regular random graph, which is homogeneous with all the nodes having the same connectivity $k_{\min}$. For $\gamma \to 0$, most of the links are associated with nodes with connectivity on the order of $k_{\max}$, and the network becomes densely connected. The most interesting regime corresponds to intermediate values of γ, because in this case the network is highly heterogeneous but still sparse, having the number of links much smaller than $N(N-1)/2$. Consider then this case.

Employing the generating function formalism of ref. [32], we have derived an expression for the expected value of the shortest path between nodes with connectivity k_i and k_j, i.e.,

$$d_{ij} = \frac{\ln(Nz_1/k_i k_j)}{\ln(z_2/z_1)} + 1, \tag{9}$$

where z_1 and z_2 are the average numbers of first and second neighbors, respectively. Accordingly, nodes with larger connectivity are on average closer to each other than those with smaller connectivity. The remarkable property of eq. (9) is that d_{ij}

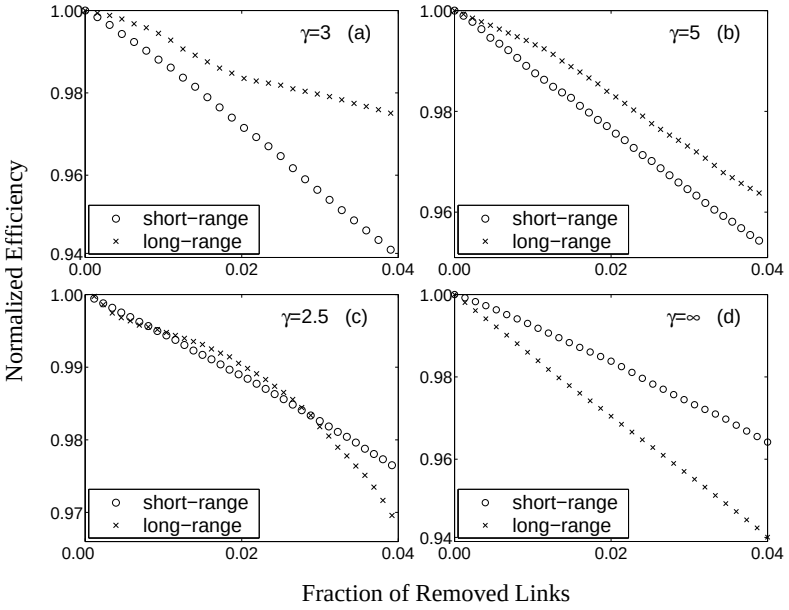

Figure 10. Normalized efficiency for short- and long-range attacks as a function of the fraction of removed links. All the parameters other than γ are the same as in figure 9.

depends only on the product of the connectivities k_i and k_j. This relation suggests that the range is also correlated with the product of the connectivities [45a] so that short-range links tend to link together highly connected nodes, while long-range links tend to connect nodes with very few links. Moreover, links between nodes with large connectivities are expected to be passed through by a large number of shortest paths. That is, on average these links should possess a higher load [24] than those connected to nodes with few links. These have been confirmed numerically, as shown in figure 9 for $\gamma = 3$, where we plot the product of connectivities averaged over all pairs of nodes separated by a given shortest path length, or connected by a link with a given range or load.

Combining the above analyses for range and load, we observe that high load should be associated mainly with short-range links. With the understanding that links with higher load should contribute more to the shortness of the paths between nodes, this correlation between load and range implies that attacks on short-range links are more destructive than those on long-range links, in contrast to what one might naively think.

Now we present numerical verification of our main result concerning the effect of attacks on links. In figure 10 we show the efficiency (normalized by its initial value) for both short- and long-range attacks, for different values of γ. Notably, short-range attacks are more destructive than long-range ones for intermediate values of γ, as shown in figures 10a and 10b for $\gamma = 3$ and $\gamma = 5$, respectively. The corresponding relation between the average load and range, plotted in figure 11 for $\gamma = 3$ (open circles), confirms that higher load on links with shorter range

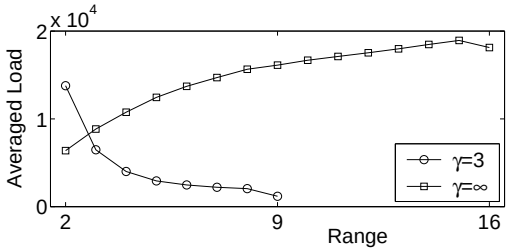

Figure 11. Comparison between heterogeneous and homogeneous networks: averaged load as a function of the range for $\gamma = 3$ and $\gamma = \infty$. All the parameters other than γ are the same as in figure 9.

is the mechanism underlying this phenomenon. Long-range attacks become more destructive only for networks with sufficiently small or large values of γ. In figures 10c and 10d we show the results for $\gamma = 2.5$ and $\gamma = \infty$, respectively. The exchange of the roles of attacks on short- and long-range links for networks with small values of γ is due to the appearance of a densely connected subnetwork of nodes with large connectivity. In this case there are so many redundant short-range connections that the removal of one will not increase the average shortest path by much because, for a given pair of nodes, there are in general more than one path of minimal length which pass through different short-range links. For networks with large values of γ, switching of the roles of short- and long-range attacks is caused by the homogenization of the network. In a homogeneous network all the nodes have approximately the same connectivity. Therefore, links with higher load are precisely those between distant nodes, i.e., those with larger range, as shown in figure 11 for $\gamma = \infty$ (open squares).

To demonstrate the generality of our results, we turn next to dynamic models of scale-free networks, where the algebraic scaling results from growth with preferential attachment, as observed in many realistic networks [3,4]. For concreteness, we consider the BA model [3] and its generalization with aging of nodes due to Dorogovtsev and Mendes [43]. The model is constructed as follows. We start at $t = 0$ with N_0 nodes and zero links. At each successive time step we add a new node with $m \leq N_0$ links so that each new link is connected to some old node i with probability $\Pi_i \sim \tau_i^{-\alpha}(k_i + 1)$, where τ_i is the age of the node i and k_i is its connectivity. The standard BA model with scaling exponent $\gamma = 3$ is recovered by taking $\alpha = 0$. In general, scale-free networks with $\gamma > 2$ are generated by choosing values of α in the interval $(-\infty, 1]$ [43], where γ approaches the value of 2 as $\alpha \to -\infty$ and becomes infinite as $\alpha \to 1$.

Most of the arguments and conclusions presented for the semi-random model are also valid for the growth model. In particular, the short-range attack is still expected to be more destructive than the long-range one at intermediate values of γ, while the opposite is expected for sufficiently large γ. However, there is an important difference for $2 < \gamma < 3$. Since new links come with new nodes, the subnetwork of highly connected nodes must be sparse. Accordingly, for this model there will be no switching concerning the effect of short- vs. long-range attacks at a small value of γ.

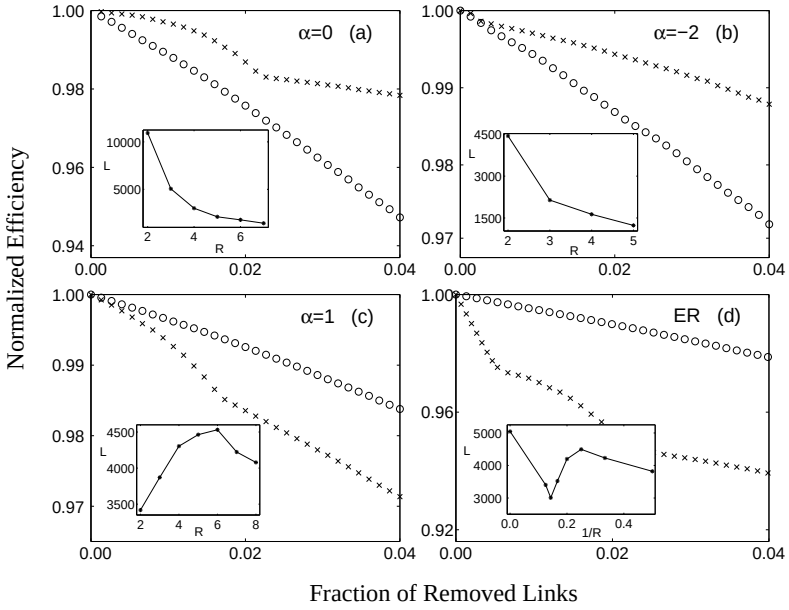

Figure 12. Normalized efficiency for short-range attacks (○) and long-range attacks (×) as a function of the fraction of removed links. Each graph corresponds to the average over 10 realizations for: (**a**)–(**c**) $N = 5000$, $N_0 = 3$, and $m = 3$; (**d**) $N = 5000$ and $z_1 = 6$. The corresponding relations between averaged loads L and ranges R are plotted in the insets. Observe that in inset (**d**) the horizontal axis is R^{-1}.

Our predictions are confirmed by numerical simulations, as shown in figure 12 for different values of α (γ). Indeed, short-range attacks are more destructive for $\alpha = 0$ ($\gamma = 3$) and also for $\alpha = -2$ ($\gamma \approx 2.3$), while long-range attacks are more destructive for $\alpha = 1$ ($\gamma = \infty$). In all cases the best strategy of attack is consistent with the correlation between load and range, as shown in the insets of figures 12a–c.

It is instructive to compare the results for scale-free networks with those for homogeneous networks with Poisson-like distribution of connectivities. In figure 12d we show the efficiency for the ER random model. In this model we start with N nodes and zero links. Then for each pair of nodes, with probability p, we add a link between them. The resulting network has on average $z_1 = p(N-1)$ links per node. This network is more sensitive to attacks on long-range links because of the strong concentration of load on links with range infinity (see the inset). Incidentally, the long-range attack is also more destructive in the WS model [2], where the rewired connections tend to have higher load. The same tendency displayed in figures 10 and 12 was observed for any fraction of removed links. In particular, short-range attack is still the most effective one for scale-free networks with scaling exponent around 3. We observe, however, that the removed fraction shown in these figures is already unrealistically large for many practical situations.

5. Discussions

In this paper, we have addressed two problems concerning attacks on and security of complex networks. The importance of studying attacks on complex networks is two-fold. Firstly, it can identify the vulnerabilities of real-world networks, which can be used either for protection (e.g., of Internet) or for destruction (e.g., of metabolic networks targeted by drugs). Secondly, it provides guidance in designing more robust artificial networks (e.g., power grids).

Our result on cascading process in complex networks indicates that many natural and man-made networks, while being naturally evolved to be quite resistant to random failure of nodes, are vulnerable to the presence of a few nodes with exceptionally large load: the attack on a single important node (one of those with high load) is likely to trigger a cascade of overload failures capable of disabling the network almost entirely. Such an event has dramatic consequences on the network performance, because the functionability of a network relies on the ability of the nodes to communicate efficiently with each other. From the perspective of security, an effective attack relies on identifying vulnerabilities and is far from being random. Our society is geographically distributed in a way that natural hazards are by no means random [46]. An example is the crowding of people, communication, transportation and financial centers around seismic areas, like the Pacific Rim. Natural disasters and intentional attacks can then have devastating consequences on the complex networks underlying the society. These consequences will be more severe if the damage on one or few nodes is capable of spreading over the entire network. In this sense a cascade-based attack can be much more destructive than any other strategies of attack previously considered [7,9–11,24,26,41,42].

We have also shown that for a wide interval of the scaling exponent γ, scale-free networks are more vulnerable to short- than long-range attacks, which results from a higher concentration of load on short-range links. In contrast to the load-based strategies of attacks considered in ref. [24], which are based on global information, short-range attacks are quasi-local in that, for a given range R, they require information only up to the $(R-1)$th neighbors. Our findings have important implications that go beyond the issue of attack itself, as they provide insights into the structure and dynamics of scale-free networks. In particular, they show that short-range links are more important than long-range links for efficient communication between nodes, which is the opposite to what one might expect from other classes of small-world networks. For instance, in the network of sexual contacts, which is known to be scale free [47], this means that the rapid spread of a disease may be mainly due to short-range contacts between people with large number of partners, in sharp contrast to its homogeneous counterpart [40].

Acknowledgement

This work was supported by AFOSR and NSF.

References

[1] S H Strogatz, *Nature (London)* **410**, 268 (2001)
[2] D J Watts and S H Strogatz, *Nature (London)* **393**, 440 (1998)

[3] A-L Barabási and R Albert, *Science* **286**, 509 (1999)
[4] R Albert and A-L Barabási, *Rev. Mod. Phys.* **74**, 47 (2002)
[5] B Bollobás, *Random graphs* (Academic Press, London, 1985)
[6] D J Watts, *Small worlds* (Princeton University Press, Princeton, 1999)
[7] R Albert, H Jeong and A-L Barabási, *Nature (London)* **406**, 378 (2000)
[8] R Cohen, K Erez, D ben-Avraham and S Havlin, *Phys. Rev. Lett.* **85**, 4626 (2000)
[9] D S Callaway, M E J Newman, S H Strogatz and D J Watts, *Phys. Rev. Lett.* **85**, 5468 (2000)
[10] R Cohen, K Erez, D ben-Avraham and S Havlin, *Phys. Rev. Lett.* **86**, 3682 (2001)
[11] A Broder, R Kumar, F Maghoul, P Raghavan, S Rajagopalan, R Stata, A Tomkins and J Wiener, *Comput. Netw.* **33**, 309 (2000)
[12] D J Watts, *Proc. Natl. Acad. Sci. USA* **99**, 5766 (2002)
[13] Y Moreno, J B Gómez and A F Pacheco, *Europhys. Lett.* **58**, 630 (2002)
[14] B A Carreras, D E Newman, I Dolrou and A B Poole, in *Proceedings of Hawaii International Conference on System Sciences*, January 4–7, 2000, Maui, Hawaii
[15] M L Sachtjen, B A Carreras and V E Lynch, *Phys. Rev.* **E61**, 4877 (2000)
[16] R Pastor-Satorras, A Vázquez and A Vespignani, *Phys. Rev. Lett.* **87**, 258701 (2001)
[17] W Willinger, R Govindan, S Jamin, V Paxson and S Shenker, *Proc. Natl. Acad. Sci. USA* **99**, 2573 (2002)
[18] K-I Goh, B Kahng and D Kim, *Phys. Rev. Lett.* **88**, 108701 (2002)
[19] R Guimerà, A Arenas, A Días-Guilera and F Giralt, e-print cond-mat/0206077
[20] V Jacobson, in *Proceedings of SIGCOMM '88* (ACM, Standford, 1998)
[21] M E J Newman, *Phys. Rev.* **E64**, 016132 (2001)
[22] M E J Newman, *Proc. Natl. Acad. Sci. USA* **98**, 404 (2001)
[23] M Girvan and M E J Newman, *Proc. Natl. Acad. Sci. USA* **99**, 8271 (2002)
[24] P Holme, B J Kim, C N Yoon and S K Han, *Phys. Rev.* **E65**, 056109 (2002)
[25] A E Motter and Y-C Lai, *Phys. Rev.* **E66**, 065102(R) (2002)
[26] A E Motter, T Nishikawa and Y-C Lai, *Phys. Rev.* **E66**, 065103(R) (2002)
[27] A P S de Moura, Y-C Lai and A E Motter, *Phys. Rev.* **E68**, 017102 (2003)
[28] P Holme and B J Kim, *Phys. Rev.* **E65**, 066109 (2002)
[29] K-I Goh, B Kahng and D Kim, *Phys. Rev. Lett.* **87**, 278701 (2001)
[29a] A different model and mechanism for overload breakdown in growing networks has been considered in [28]. These authors focus on overloads caused by the growth of the network. Their model assigns the same capacity to every node in the network. In their analysis, when a node is overloaded, the links to that node are removed but the node itself is not removed and can be reconnected in the future. Their conclusion is that, to avoid overloads, the capacity must grow with the size of the network. Our model is different from the model in [28] as we assume the capacity to be node-dependent and the failed nodes to be permanently removed from the network. More importantly, we address the issues of intentional attack and random breakdown, and we study how the network collapses under overload failures induced by them. We assume that the time-scale for these events is much smaller than the time-scale in which the network grows
[30] S Redner, *Eur. Phys. J.* **B4**, 131 (1998)
[31] M Faloutsos, P Faloutsos and C Faloutsos, *Comput. Commun. Rev.* **29**, 251 (1999)
[32] M E J Newman, S H Strogatz and D J Watts, *Phys. Rev.* **E64**, 026118 (2001)
[33] P Erdös and A Rényi, *Publ. Math. Inst. Hung. Acad. Sci.* **5**, 17 (1960)
[34] http://moat.nlanr.net/AS/Data/ASconnlist.20000102.946809601
[35] ftp://ftp.santafe.edu/pub/duncan/power_unweighted

[36] L A N Amaral, A Scala, M Barthélémy and H E Stanley, *Proc. Natl. Acad. Sci. USA* **97**, 11149 (2000)
[37] K-I Goh, C-M Ghim, B Kahng and D Kim, *Phys. Rev. Lett.* **91**, 1898041 (2003)
[38] K Park, Y-C Lai and N Ye, *Phys. Rev.* **E70**, 026109 (2004)
[39] A-L Barabasi, R Albert and H Jeong, *Physica* **A272**, 173 (1999)
[40] S A Pandit and R E Amritkar, *Phys. Rev.* **E60**, R1119 (1999)
[41] R V Solé and J M Montoya, *Proc. R. Soc. London* **B268**, 2039 (2001)
[42] H Jeong, S P Mason, A-L Barabási and Z N Oltvai, *Nature (London)* **411**, 41 (2001)
[43] S N Dorogovtsev and J F F Mendes, *Phys. Rev.* **E62**, 1842 (2000)
[44] M E J Newman, *Phys. Rev.* **E64**, 016132 (2001)
[44a] We choose to sort the links according to the initial distribution of ranges, instead of an updated distribution, because we want to address the relative importance of short-range and long-range links for the original network. In addition, in terms of attack efficiency, updating is time consuming
[45] V Latora and M Marchiori, *Phys. Rev. Lett.* **87**, 198701 (2001)
[45a] Indeed, the range of a link can be regarded as the length of the second shortest path between the nodes that are connected to the link. Since we are considering the semi-random model, for which everything other than the connectivity distribution is random, the length of the second shortest path should also be correlated with the product of connectivities
[46] D Kennedy, *Science* **295**, 405 (2002)
[47] F Liljeros, C R Edling, L A N Amaral, H E Stanley and Y Aberg, *Nature (London)* **411**, 907 (2001)