Optimization of Robustness and Connectivity in Complex Networks

Benjamin Shargel,[1] Hiroki Sayama,[1,2] Irving R. Epstein,[1,3] and Yaneer Bar-Yam[1]

[1]*New England Complex Systems Institute, Cambridge, Massachusetts 02138*

[2]*Department of Human Communication, University of Electro-Communications, Chofu, Tokyo 182-8585, Japan*

[3]*Department of Chemistry and Volen Center for Complex Systems, Brandeis University, Waltham, Massachusetts 02454*

(Received 22 April 2002; published 13 February 2003)

Scale-free networks rely on a relatively small number of highly connected nodes to achieve a high degree of interconnectivity and robustness to random failure, but suffer from a high sensitivity to directed attack. In this paper we describe a parametrized family of networks and analyze their connectivity and sensitivity, identifying a network that has an interconnectedness closer to that of a scale-free network, a robustness to attack closer to that of an exponential network, and a resistance to failure better than that of either of those networks.

DOI: 10.1103/PhysRevLett.90.068701 PACS numbers: 89.75.Hc, 89.75.Fb

Many complex biological, social, and engineered systems can be modeled as inhomogeneous networks, whose connectivity distributions follow a power law, $P(k) \sim k^{-\gamma}$, for large k [1–5]. A handful of highly connected nodes act as linchpins holding the scale-free network together, shortening the paths between arbitrarily chosen nodes and thereby increasing the network's interconnectivity. Their reliance on these nodes, however, makes these networks sensitive to targeted attack [6–10]. Exponential, or purely random networks [11], are less interconnected and tolerant to failure, but are more robust to attack. Here we present a more general class of complex networks, of which scale free and exponential networks are special cases, by parametrizing two aspects of network construction: growth and preferential attachment. We find that these parameters can be optimized to produce a network that has an interconnectedness close to a scale-free network, a robustness to attack similar to an exponential network, and a resistance to failure that improves on both random and scale-free networks.

The two types of network perturbation we examine here are failure and attack, the removal, respectively, of a random node or of the most connected node in the network [6–8]. The measure of a network's response to failure or attack is the increase in its diameter d, the average shortest path between pairs of nodes in the network.

Exponential networks can be constructed by creating N nodes initially, then randomly connecting pairs of nodes. The randomness inherent in this procedure ensures that no node is more likely to attain a significantly higher connectivity than any other. Scale-free networks, on the other hand, are built up over time with the addition of nodes that selectively connect to existing members of the network. The higher the connectivity of a given node, the more likely it is to receive additional connections, according to the probability $\prod(i) = k_i / \sum_j k_j$.

Most nodes in an exponential network have a connectivity close to the peak value in $P(k)$, but the existence of an exponential tail of more connected nodes makes such networks more sensitive to attack than to failure. This difference is, however, much more dramatic in the scale-free network. Indeed, relative to an exponential network, the connectivity of a scale-free network is concentrated in a few highly connected nodes, leaving the network more vulnerable to attack, but not to failure, because the probability of a critical node's failing is quite small.

The construction of scale-free networks differs from that of exponential networks in that it involves growth and preferential attachment. To examine a larger space of possible networks, we introduce two parameters, p and g, corresponding to preferential attachment and growth, respectively. Each parameter varies continuously from 0 to 1, where 0 indicates that preferential attachment or growth was not used in network construction, 1 signifies that the relevant process was employed to the fullest extent. The exponential network can be generated with $p = g = 0$, and the scale-free with $p = g = 1$. The case $(p, g) = (0, 1)$ has been considered by Callaway *et al.* [12] Our goal of optimizing robustness will lead us to consider the properties of the $(p, g) = (1, 0)$ network.

We generate networks of N nodes and E edges that depend on two parameters p and g as follows. (i) Let $k = 2E/N$ be the average connectivity of the network, $I = (1 - g)N$ be the number of nodes initially created, and $G = gN$ be the number of nodes subsequently grown onto the network. (ii) Create I nodes. (iii) Repeat $Ik/2$ times: Connect two nodes chosen from the probability distribution $\prod(i)' = \min[pk_{\max}, \max(k_i, 1)] / \sum_j \min[pk_{\max}, \max(k_j, 1)]$, where $k_{\max}$ is the maximum connectivity in the network. If the nodes are already connected, pick again. The $\prod(i)'$ distribution is similar to the $\prod(i)$ distribution, except that instead of being purely linear, there is a cutoff point at $pk_{\max}$, where the distribution becomes flat. Thus, the smaller p, the flatter the distribution. Note that disconnected nodes have a nonzero chance of being chosen. (iv) Repeat G times: Create a node and connect it to $k/2$ nodes in the network, where each node again has the probability $\prod(i)'$ of being selected.

In this algorithm, g determines the proportion of nodes that are grown onto the network. The difference between nodes grown on and those created initially is that the former are connected to the network immediately upon being added and with a guaranteed connectivity of $k/2$. Because nodes created initially do not necessarily receive connections, some of the initial nodes remain disconnected. To attain the desired number of nodes, we carry out steps (ii) and (iii) of the algorithm with extra nodes and then eliminate the necessary number of nodes after construction is completed, choosing disconnected nodes first, followed by randomly selected nodes if necessary.

The parameter p governs how nodes are selected for connection once they have already been added. The greater p is, the more a node's chances of being picked for further connections increases with its connectivity. When $p = 0$ all nodes have an equal chance, and selection is random, while when $p = 1$ a connected node's chances reduce to $\prod(i)$, and selection is maximally preferential.

To explore the (p, g) parameter space, we constructed networks with different parameter values and subjected them to failure and attack. The rate of change of the diameter for random failure is shown in Fig. 1 for simulations with $N = 2000$, $k = 4$. These results suggest that the scale-free network is far from optimal within this family of networks, and the $(1, 0)$ network is much better from this perspective. The sensitivity to attack can be seen in Fig. 2 which shows the diameter after removing 2.5% and 5.0% of the highest connected nodes. The high sensitivity of the scale-free networks suggests a substantial disadvantage when robustness to attack is desirable. Interestingly the $(1, 0)$ network has an advantage in this context as well, with a sensitivity to attack not much more than that of a random network despite starting with a significantly lower initial diameter. Results for values of N ranging from 1000 to 10 000 were similar. The primary effect of increasing k is to reduce the differences between connectivities of all networks.

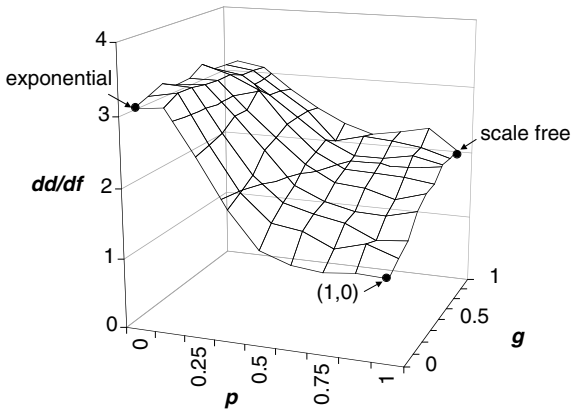

FIG. 1. Comparison of the change in diameter due to random failure for networks as a function of (p, g).

Analytic estimates for network diameters can be obtained using the approximate result [3] $d = [\log(N/z_1)/\log(z_2/z_1)] + 1$ which treats the network as a tree and therefore is only roughly valid. Here $z_1 = \langle k \rangle$ and $z_2 = \langle k^2 \rangle - \langle k \rangle$ are the mean number of first and second neighbors of a node. The first is the same for all studied networks. For the second, each of the network types can be treated using exact or approximate analytic calculations that can be compared with the simulations. For the exponential network the Poisson distribution for $P(k)$ gives

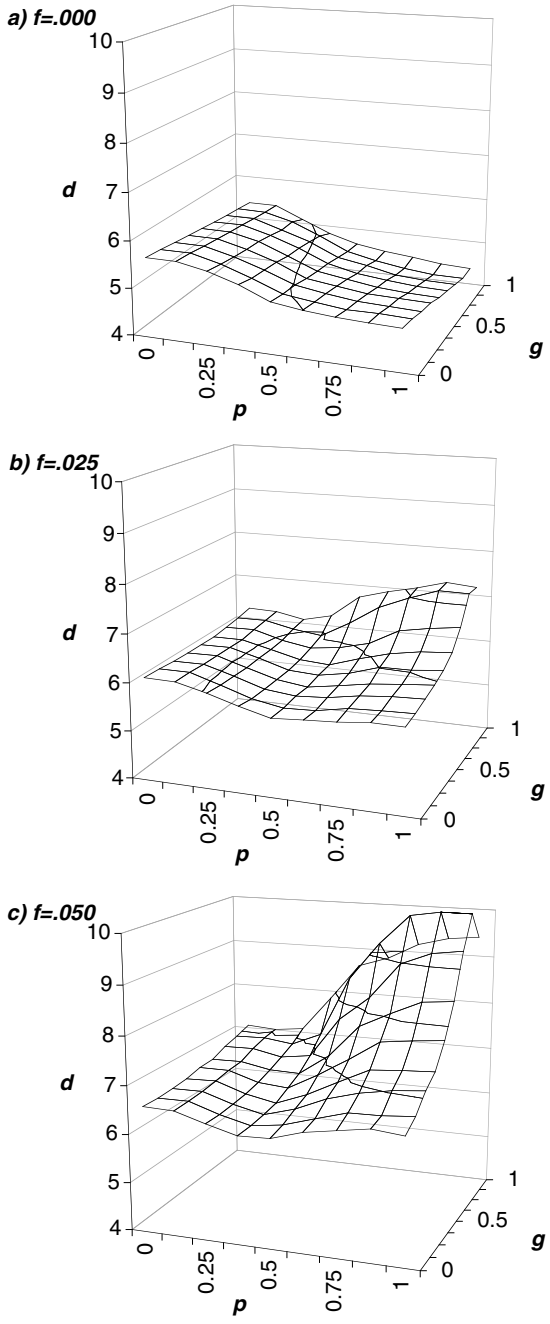

FIG. 2. Diameter as a function of (p, g): (a) original networks; (b),(c) after removal of 2.5% and 5% of the most highly connected nodes (attack), respectively.

$z_2 = \langle k \rangle^2 \approx 16\,(15.7)$, where the simulation results are shown in parenthesis. For the scale-free network, using a power-law distribution for $P(k)$ with low and high k cutoffs, gives $z_2 \approx \langle k \rangle^2 \log[N\langle k \rangle \sqrt{\pi}\Gamma(N)/2\Gamma(N + 1/2)]/2 - \langle k \rangle \approx 31.0\,(45.0)$. The poor accuracy is due to the long tail of the power-law distribution. For the $(0, 1)$ network the second moment of $P(k)$ can be readily calculated using arguments that generalize the treatment of the Poisson distribution of the random network giving $z_2 = (5/4)\langle k \rangle^2 - \langle k \rangle/2 \approx 18\,(17.9)$. For the $(1, 0)$ network a recursive Master equation treatment of $P(k)$ [13] gives $z_2 = (8\langle k \rangle^2 - 10\langle k \rangle + 2)/3 = 30\,(29)$. These give analytic (simulation) results for the diameter of the exponential 5.48 (5.69), scale-free 4.04 (4.36), $(0, 1)$ 5.13 (5.37), and $(1, 0)$ 4.08 (4.91) networks. The results are typically underestimated by 5%–20% due to neglect of network topology. To estimate the effects of failure or attack we replace $N \rightarrow N - 1$, $\langle k \rangle \rightarrow \langle k \rangle[1 - (2k_r - 1)/N]$, and $\langle k^2 \rangle \rightarrow \langle k^2 \rangle\{1 - [k_r(k_r - 1)/\langle k^2 \rangle + 2k_r/\langle k \rangle - 1]/N\}$, where k_r is the connectivity of the removed node which is $\langle k \rangle$ for failure and for attack was estimated analytically as the average of the highest k for N values from the distribution $P(k)$ as $k_r \approx 12.5(12.3), 159(120), 16(20), 39(39)$ for the random, scale free, $(0, 1)$ and $(1, 0)$ networks, respectively. This gives the change in diameter due to the first node removal for attack and failure for the networks, respectively, of 0.013 (0.013) and 0.000 97 (0.0016), 0.92 (0.19) and 0.000 25 (0.0011), 0.017 (0.026) and 0.000 75 (0.0014), 0.039 (0.033) and 0.000 27 (0.00061). Except for the scale-free network, the analytic results are generally within 50% of the simulations with the error due primarily to the neglect of network topology. Inserting the previous simulation results into the expression for the effect of node removal gives results in better agreement with removal simulation results. However, key comparisons, e.g., between the effects of failure on the scale-free and $(1, 0)$ network are not correctly predicted by the analytic estimates indicating the limitations of treatments that assume treelike topologies.

One possible goal of network design is to optimize interconnectivity and robustness to failure and attack. While the tradeoff between these various parameters is not simple, still a general trend can be observed from the figures. As one increases p, network interconnectivity increases significantly. Increasing g and p together increases sensitivity to attack, increasing either one separately has much less effect. Robustness to failure improves with p and declines with g. There is not, as might be expected, an inherent tradeoff between robustness to failure and to attack. One solution to our optimization problem is then to set p to its maximum value and g to its minimum, i.e., a $(1, 0)$ network. The $(1, 0)$ network begins with a diameter closer to the scale-free network, but demonstrates better robustness to failure and a robustness to attack close to that of an exponential network.

Analysis of the connectivity distribution of the $(1, 0)$ network alongside those of the exponential and scale-free networks sheds light on its surprising capabilities (Fig. 3). The peak and rapid falloff of the exponential network's distribution indicate that many nodes have connectivities at or around the mean with relatively little variation. The near linearity of the scale-free distribution shows, in contrast, that the vast majority of nodes have low connectivity, despite the presence of a few highly connected nodes, whose numbers decay as a power law. The distribution of the $(1, 0)$ network lies between the exponential and scale-free distributions; it bends downward like the exponential distribution, but with much less curvature and a broader tail. As compared to the scale-free distribution, connectivity that would otherwise reside in the lower and higher ranges of the distribution has been redistributed to the middle.

A temporal bias caused by node addition, and absent in the $(1, 0)$ network, affects both the connectivity distribution and the topology of scale-free networks. As nodes created earlier have more chances to be selected for connection than those created later [14], the distribution develops a broader tail, and its peak shifts to the left. Moreover, connections made early on by the initial nodes tend to be amplified over time due to positive feedback, further skewing the distribution. In the early period of its construction, a scale-free network will be highly interconnected, because the initial nodes can only connect to each other. As more nodes are added, they selectively connect to this inner hub and, to a lesser extent, to the nodes surrounding it, forming layers around them. Two nodes that are not connected to each other when they are added cannot be connected later in the process even if they both become highly connected. This process produces a treelike structure that is dependent on the earlier nodes to hold it together.

The lack of temporal bias in the $(1, 0)$ network leads to more redundancy in the network. Since nodes are not constrained to connect only with the subset of already created nodes, more cycles form in the network. This is especially true of the highly connected nodes, since they

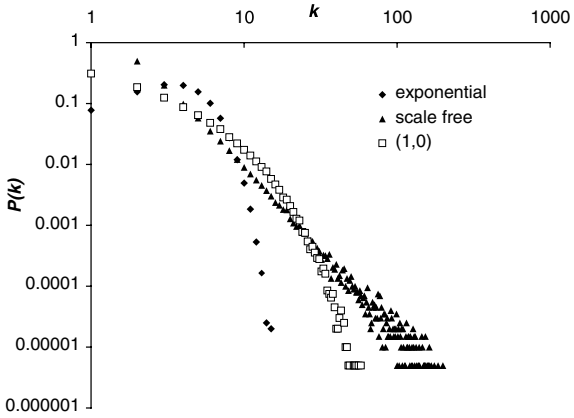

FIG. 3. Connectivity distributions of an exponential, $(1, 0)$, and scale-free network.

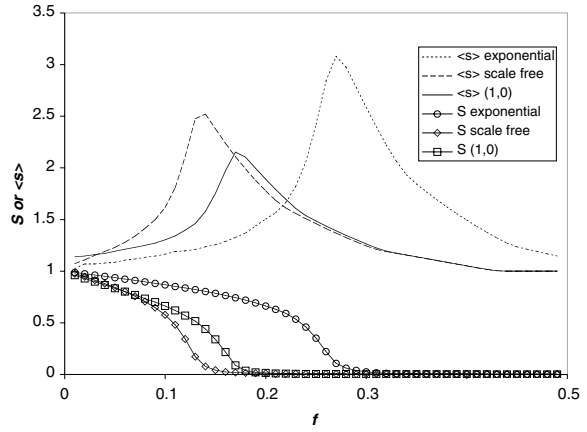

FIG. 4. Fragmentation analysis of the random, scale free, and $(1, 0)$ networks under attack showing the relative maximum cluster size, S, and average cluster size of other clusters $\langle s \rangle$.

are the most likely to be paired up when edges are added. The densely connected web thus formed ensures that even if a highly connected node is taken out, little damage is done to the diameter of the network, since there is always a profusion of alternate paths.

In order to confirm the disparity in redundancy between the different network types, fragmentation analysis [6] was performed by measuring the number and size of isolated clusters in the networks as they were subjected to attack. Figure 4 illustrates both the size of the maximum cluster, S, relative to the size of the network, and the average size $\langle s \rangle$ of all clusters excluding the maximum one. This experiment was carried out on exponential, scale-free and $(1, 0)$ networks, $N = 2000$ and $k = 4$, with each network subject to removal of up to half its nodes. For the $(1, 0)$ network the rate of decrease of S and the critical node fraction at which the maximum of $\langle s \rangle$ occurs both lie between the corresponding values for the random and scale-free networks. However, the maximum of $\langle s \rangle$ for the $(1, 0)$ network is significantly lower than that of either the random or scale-free networks, indicating that nodes become disconnected in smaller clusters, due to improved network redundancy among the highly connected nodes in the core.

The connectivity distribution of a somewhat different parametrized set of networks, constructed using growth and rewiring, has been investigated [15], but their robustness to attack and failure was not studied. We constructed networks of the type described in Ref. [15] and compared them with $(1, 0)$ networks of equivalent connectivity. We found that, for comparable connectivity, the robustness of the $(1, 0)$ network is superior to that of this entire alternative class of networks.

We have presented a general framework for complex networks based on two parameters, p and g, which regulate the growth and preferential attachment used in network construction. Within this framework, exponential and scale-free networks represent two corners of the parameter space. We find that the benefits of p, with regard to interconnectivity and robustness to failure and attack, outweigh its costs, while those of g do not. Optimizing the values of the parameters according to this logic allows us to create a novel network with an aggregate of properties superior to those of the standard networks. Such a network has potential for application in engineering [16], social policy and management [17], and other fields that attempt to design systems which depend on interconnectivity but face exposure to failure and attack. For problems such as these, exponential and scale-free networks are suboptimal due to the one's limited degree of interconnectivity and the other's sensitivity to attack. By combining an assessment of the relative importance of interconnectivity and robustness to failure and attack with measures of parameter sensitivity, one should be able to construct a metric for optimal choice among the class of (p, g) networks for any particular application.

This work was supported in part by the NSF (Grants No. 0083885 and No. CHE-9988463).

[1] A.-L. Barabási and R. Albert, Science **286**, 509 (1999).
[2] R. Albert, H. Jeong, and A.-L. Barabási, Nature (London) **401**, 130 (1999).
[3] M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys. Rev. E **64**, 026118 (2001).
[4] S. H. Strogatz, Nature (London) **410**, 268 (2001).
[5] M. E. J. Newman, D. J. Watts, and S. H. Strogatz, Proc. Natl. Acad. Sci. U.S.A. **99**, 2566 (2002).
[6] R. Albert, H. Jeong, and A.-L. Barabási, Nature (London) **406**, 378 (2000); **409**, 542(E) (2001).
[7] H. Jeong, B. Tombor, R. Albert, Z. Oltvai, and A.-L. Barabási, Nature (London) **407**, 651 (2000).
[8] R.V. Sole and J. M. Montoya, Proc. R. Soc. London, Ser. B **268**, 2039 (2001).
[9] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **85**, 4626 (2000).
[10] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys. Rev. Lett. **85**, 5468 (2000).
[11] P. Erdös and A. Rényi, Pub. Math. Inst. Hung. Acad. Sci. **5**, 17 (1960).
[12] D. S. Callaway, J. E. Hopcroft, J. M. Kleinberg, M. E. J. Newman, and S. H. Strogatz, Phys. Rev. E **64**, 041902 (2001).
[13] I. R. Epstein, and Y. Bar-Yam (unpublished).
[14] B. A. Huberman and L. A. Adamic, Nature (London) **401**, 131 (1999).
[15] R. Albert, and A.-L. Barabási, Phys. Rev. Lett. **85**, 5234 (2000).
[16] K. Claffy, T. E. Monk, and D. McRobb, Nature Web Matters (online), http://helix.nature.com/webmatters/tomog/tomog.html (1999).
[17] S. Wasserman and K. Faust, *Social Network Analysis* (Cambridge University Press, Cambridge, U.K., 1994).