Available online at www.sciencedirect.com
SCIENCE DIRECT®
Physica A 344 (2004) 504–509
PHYSICA A
www.elsevier.com/locate/physa

Tolerance of scale-free networks: from friendly to intentional attack strategies

Lazaros K. Gallos[a], Panos Argyrakis[a], Armin Bunde[b,*], Reuven Cohen[c], Shlomo Havlin[c]

[a] *Department of Physics, University of Thessaloniki, 54124 Thessaloniki, Greece*
[b] *Institut für Theoretische Physik III, Justus-Liebig-Universität Giessen, Heinrich-Buff-Ring 16, 35392 Giessen, Germany*
[c] *Minerva Center and Department of Physics, Bar-Ilan University, 52900 Ramat-Gan, Israel*

Available online 1 September 2004

Abstract

We study the tolerance of a scale-free network (having a connectivity distribution $P(k) \sim k^{-\gamma}$) under systematic variation of the attack strategy. In an attack, the probability that a given node is destroyed, depends on the number of its links k via $W(k) \sim k^{\alpha}$, where α varies from $-\infty$ (most harmless attack) to $+\infty$ (most harmful "intentional" attack). We show that the critical fraction p_c needed to disintegrate the network increases monotonically when α is decreased and study how at p_c the topology of the diluted network depends on the attack strategy.

PACS: 89.75.−Hc; 87.23.Ge

Keywords: Scale-free networks; Structural properties; Attacks

Many networks are characterized by a scale-free degree distribution [1,2] where the fraction of sites having k connections follows a power-law distribution:

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

with an exponent γ usually between 2 and 3. Examples of such networks are social networks, such as the web of sexual contacts [3], movie-actor networks [4], science citations and cooperation networks [5,6]. Computer networks, both physical (such as

* Corresponding author. Tel.: +49-641-99-33360; fax: +49-641-99-33369.
E-mail address: armin.bunde@theo.physik.uni-giessen.de (A. Bunde).

0378-4371/$ - see front matter © 2004 Published by Elsevier B.V.
doi:10.1016/j.physa.2004.06.021

the Internet [7]) and logical (such as the World Wide Web [4], email [8] and trust networks [9]) are also known to obey scale-free degree distributions.

Two "attack scenarios" have been studied extensively on such networks. In the first scenario, nodes are randomly removed [10,11], which corresponds to the common percolation problem studied well in lattice networks [12] or random graphs [13]. Scale-free networks are more resistant to random attacks than random networks, where the distribution of links obeys the Poisson distribution. Above a critical fraction p_c of removed links, the network loses its connectivity and a giant cluster of connected sites no longer exists. For $\gamma < 3$, p_c approaches unity with increasing number of nodes N of the network, indicating that the giant cluster survives even when almost all nodes have been removed [11]. In the second scenario, under an "intentional attack", the highest degree nodes are removed first [10,14]. Since scale-free networks are highly fragile to such targeted attacks and rely heavily on the presence of few nodes of high connectivity, they can easily be destroyed when these nodes (hubs) are removed. Thus, the critical concentration p_c is quite low under an intentional attack.

Here, we study more general attack strategies, where the probability $W(k)$ of choosing a node to be destroyed with probability p depends on its degree k:

$$W(k_i) = \frac{k_i^\alpha}{\sum_{i=1}^{N} k_i^\alpha}, \quad -\infty < \alpha < \infty . \tag{2}$$

For $\alpha > 0$ nodes with larger k are more vulnerable, while for $\alpha < 0$, nodes with lower k are more vulnerable. The limiting cases $\alpha = 0$ and $\alpha \to \infty$ represent the random removal case [10,11], where each node has the same probability to be removed and the targeted intentional attack where only the most connected nodes [10,14] are attacked, respectively.

In the numerical simulation, we first construct the scale-free networks. For a given value of γ, we employ a Molloy–Reed algorithm [15], where we fix the number of nodes N and assign the degree k (number of links) for each node by drawing a random number from the power-law distribution $P(k) \sim k^{-\gamma}$. The minimum number of k (lower cutoff) is $m = 1$. We do not impose any upper cutoff, so that a given node (in principle) can be connected with up to $k = N - 1$ different nodes. After having specified the number of links for each node, we generate the links starting from an unlinked network. In each step, we randomly choose two nodes. If each of both nodes has at least one link available, we add a link between them. Otherwise, we choose another pair of nodes and repeat this procedure. The selection of pairs and creation of links is repeated until the entire network is created.

For each network configuration, we remove a fraction p of its nodes chosen according to Eq. (2), until we reach the critical point above which a spanning cluster does no longer exist. When a node is removed all its links are destroyed. Some typical configurations of the clusters at criticality are shown in Fig. 1. When α is large, most hubs are removed and the structure is rather linear. In contrast, for "friendly" attacks ($\alpha < 0$) and random removal of nodes ($\alpha = 0$), most hubs remain in the largest cluster. For $\alpha < 0$, the low-degree nodes are preferentially removed and thus their number in the spanning cluster is reduced compared with the random removal case $\alpha = 0$.

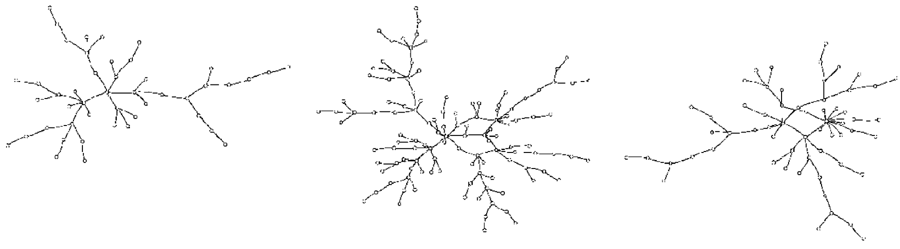

Fig. 1. Largest clusters at criticality, after different attack strategies on the same network of $N = 10^3$ sites. Left to right: $\alpha = 4.0, 0.0, -0.5$. (network visualization was done using the Pajek program).

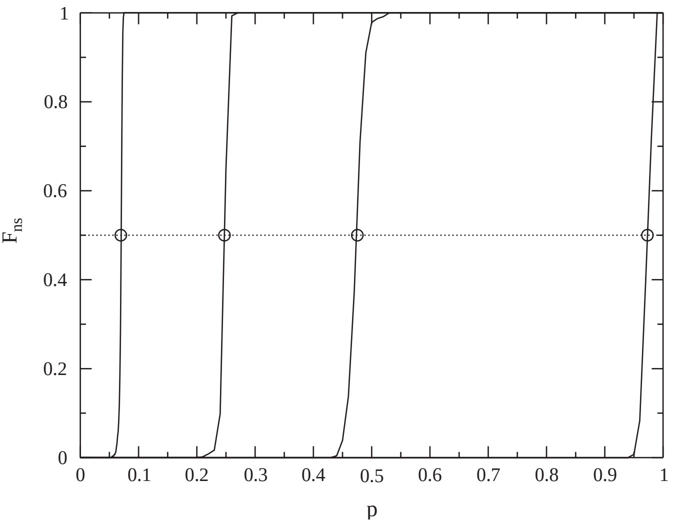

Fig. 2. The ratio of non-spanning configurations vs the fraction of removed nodes p. Lines are simulation data, from networks of $N = 10^6$ nodes, while the circles are the theoretical critical points for networks with $\gamma = 2.5$. Left to right: $\alpha = 4, 1, 0.5$, and 0.

For studying how p_c depends on α, we have determined, for each p value, the fraction of non-spanning configurations $F_{ns}(p)$. For very small values of p, all configurations are spanning and $F_{ns}(p) = 0$, while for p very close to one, all configurations are non-spanning and $F_{ns}(p) = 1$. Fig. 2 shows the functional form of $F_{ns}(p)$ for a network with $\gamma = 2.5$, for different α values. It is natural to associate the intersect of $F_{ns}(p)$ with the line 0.5 as p_c.

We have determined p_c as a function of γ and α. Representative results are shown in Fig. 3, where, for five attack strategies with $\alpha = 4, 0.5, 0, -0.5, -1$, p_c is plotted versus the network parameter γ. We show also the results of a mean-field-type analysis that will be published elsewhere [16].

The analytical results are in good agreement with the simulations. The deviations from the asymptotic limit ($N \to \infty$) are more prominent in the case of low γ values and/or negative α values.

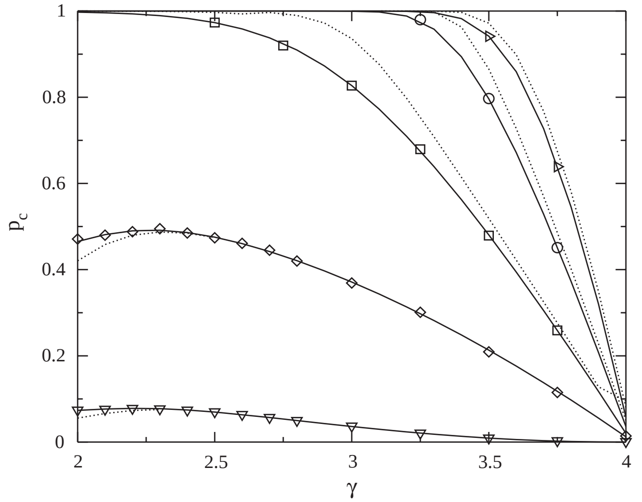

Fig. 3. Values of p_c vs γ for different α values: (bottom to top) $\alpha = 4, 0.5, 0, -0.5, -1$. Symbols represent simulation data ($N = 10^6$ nodes) from 100 to 300 runs. Solid lines are the theoretical predictions for finite-size networks, while dashed lines correspond to infinite-size networks.

Next, we study the topology of the networks right at the critical point, as a function of γ and α. For given γ and α, we determined, for each pairs of nodes, the shortest topological distance between the nodes on the diluted network. The shortest topological distance is the minimum number of links, by which the pair is connected. The mean shortest distance $\langle \ell \rangle$ is related to the cluster size N_c by $N_c \sim \langle \ell \rangle^{d_\ell}$ where d_ℓ is the topological ("chemical") dimension of the network. For random removal and $3 < \gamma < 4$, it has been suggested [17] that

$$d_\ell = \frac{\gamma - 2}{\gamma - 3}, \quad 3 < \gamma < 4 , \tag{3}$$

while for intentional attacks d_ℓ should be identical to 2 for all γ values.

Fig. 4 shows $\langle \ell \rangle$ as a function of the network size N_c at criticality, in a double-logarithmic presentation. For $\alpha = 0.0$ and $\gamma = 3.5$, the slope is consistent with $d_\ell = 3$. For $\gamma = 2.5$ and $\alpha \leqslant 0$, there is no theoretical prediction, but it is plausible that $\langle \ell \rangle$ scales as $\ln N_c$. Indeed, the lower symbols in Fig. 4 do not seem to follow a straight line. The same data, plotted in a semi-logarithmic fashion, are closer to a straight line, but due to uncertainties in the data, a definite conclusion cannot be extracted. For $\alpha > 0$, we can see that the data scale quite nicely, both for $\gamma = 3.5$ and 2.5 and yield a slope 1/2 or $d_\ell = 2$, as theoretically predicted for the $\alpha = \infty$-case, independent of γ. Thus for the same network, with $\gamma = 3.5$ for example, the topological structure of the diluted network, characterized by the chemical dimension, depends on the way criticality is reached. We can also see that, even by relaxing the "intensity" of the intentional attack by lowering α, the topology of the network at criticality remains the same. This means that for all positive α-values, the network structure is similar to the network structure under

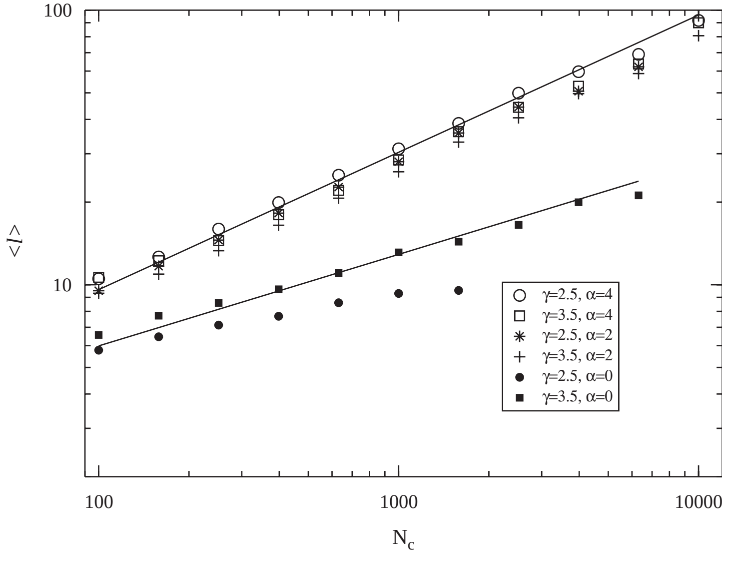

Fig. 4. Mean shortest chemical distance $\langle \ell \rangle$ between any two nodes of the giant cluster at criticality, as a function of the cluster size N_c. The results correspond to networks of initially $N = 10^4, 10^5$, and 10^6 nodes. 1000 different configurations have been used for each N, except for $N = 10^6$ (100 configurations). The data have been logarithmically binned. The values of α and γ are shown in the plot. The upper line represents the theoretical slope of 1/2, while the lower line has a slope of 1/3.

the most intentional attack, where the biggest hubs are removed first. This behavior is reflected by the considerable gap between the critical points for $\alpha = 0$ and $\alpha > 0.5$ (see Fig. 3).

This work was supported by the DAAD, an IKYDA fellowship and by the Israel Science Foundation.

References

[1] R. Albert, A.-L. Barabasi, Rev. Mod. Phys. 74 (2002) 47.
[2] S.N. Dorogovtsev, J.F.F. Mendes, Adv. Phys. 51 (2002) 1079.
[3] F. Liljeros, et al., Nature (London) 411 (2001) 907.
[4] A.-L. Barabasi, R. Albert, Science 286 (1999) 509.
[5] A.-L. Barabasi, et al., Physica (Amsterdam) 311 A (2002) 590.
[6] M.E.J. Newman, D.J. Watts, S.H. Strogatz, Proc. Natl. Acad. Sci. USA 99 (2002) 2566.
[7] S.-H. Yook, H. Jeong, A.-L. Barabasi, Proc. Natl. Acad. Sci. USA 99 (2002) 13382.
[8] H. Ebel, L.-I. Mielsch, S. Bornholdt, Phys. Rev. E 66 (2002) 035103(R).
[9] H. Guardiola, et al., cond-mat/0206240 (2002).
[10] R. Albert, H. Jeong, A.-L. Barabasi, Nature 406 (2000) 378;
R. Albert, H. Jeong, A.-L. Barabasi, Nature 409 (2001) 542.
[11] R. Cohen, K. Erez, D. Ben-Avraham, S. Havlin, Phys. Rev. Lett. 85 (2000) 4626.
[12] A. Bunde, S. Havlin (Eds.), Fractals and Disordered Systems, Springer, New York, 1996.

[13] P. Erdös, A. Rényi, Publ. Math. 6 (1959) 290.
[14] R. Cohen, K. Erez, D. Ben-Avraham, S. Havlin, Phys. Rev. Lett. 86 (2001) 3682.
[15] M. Molloy, B. Reed, Comb. Probab. Comput. 7 (1998) 295.
[16] L.K. Gallos, et al., preprint.
[17] R. Cohen, S. Havlin, D. Ben-Avraham, in: S. Bornholdt, H.G. Shuster (Eds.), Handbook of Graphs and Networks, Wiley-VCH, New York, 2002 (Chapter 4).