Available online at www.sciencedirect.com

ScienceDirect

Physica A 381 (2007) 497–514

PHYSICA A

www.elsevier.com/locate/physa

Disaster management in power-law networks: Recovery from and protection against intentional attacks

Behnam A. Rezaei[a,*], Nima Sarshar[a,c], Vwani P. Roychowdhury[a], P. Oscar Boykin[b]

[a]Department of Electrical Engineering, University of California, LA, USA
[b]Department of Electrical and Computer Engineering, University of Florida, Gainesville, USA
[c]Faculty of Engineering, University of Regina, SK, Canada

Received 7 January 2007; received in revised form 6 March 2007
Available online 4 April 2007

Abstract

Susceptibility of power-law (PL) networks to attacks has been traditionally studied in the context of what may be termed as *instantaneous attacks*, where a randomly selected set of nodes and edges are deleted while the network is kept *static*. In this paper, we shift the focus to the study of *progressive* and instantaneous attacks on *reactive* grown and random PL networks, which can respond to attacks and take remedial steps. In the process, we present several techniques that managed networks can adopt to minimize the damages during attacks, and also to efficiently recover from the aftermath of successful attacks. For example, we present (i) compensatory dynamics that minimize the damages inflicted by targeted progressive attacks, such as linear-preferential deletions of nodes in grown PL networks; the resulting dynamic naturally leads to the emergence of networks with PL degree distributions with exponential cutoffs; (ii) distributed healing algorithms that can scale the maximum degree of nodes in a PL network using only local decisions; and (iii) efficient means of creating giant connected components in a PL network that has been fragmented by attacks on a large number of high-degree nodes. Such targeted attacks are considered to be a major vulnerability of PL networks; however, our results show that the introduction of only a small number of random edges, through a *reverse percolation* process, can restore connectivity, which in turn allows restoration of other topological properties of the original network. Thus, the power-law nature of the networks can itself be effectively utilized for protection and recovery purposes.

Keywords: Growing networks; Power law; Attacks; Peer-to-peer (P2P); Scale-free; Preferential deletion; Compensation; Ad hoc networks

1. Introduction

A large number of networks in different contexts have been found to have power-law structures (see Ref. [1] and references therein) characterized by power-law (PL) degree distributions. For a PL degree distribution, the probability of a randomly chosen node to have degree k scales as $P(k) \propto k^{-\gamma}$ for large k; γ is referred to as the exponent of the distribution. Moreover, a PL distribution is considered to be *heavy tailed* if $2<\gamma\leqslant 3$, i.e., when

*Corresponding author.
E-mail addresses: behnam@ee.ucla.edu (B.A. Rezaei), nima.sarshar@uregina.ca (N. Sarshar), vwani@ee.ucla.edu (V.P. Roychowdhury), boykin@ece.ufl.edu (P.O. Boykin).

0378-4371/$ - see front matter © 2007 Published by Elsevier B.V.
doi:10.1016/j.physa.2007.03.047

the mean is bounded but the variance is unbounded. While many of these networks have evolved naturally, driven by dynamical processes over which we do not have much control, there are several classes of other networks, where the underlying dynamics can be altered to make sure that the resulting networks not only have PL structures, but are also resilient to external attacks. Examples of such designer complex networks include, the Internet, national power grids and other infrastructure related networks, computer and communication networks, and more recently peer-to-peer (P2P) networks. With the economy going more global every year, the emergence of different kinds of complex networks that interconnect distributed centers of communication, finance, and manufacturing, will only see a rapid growth. In such networks, attacks are a fact of life, and simple attacks, such as denial-of-service (DOS), can cripple hubs and other nodes, leading to severe disruptions of services. Understanding the effect of attacks, and mechanisms to respond to attacks is thus of great practical importance to many network-based systems.

As reviewed in the following, the study of attacks, including both targeted and random, in PL networks has been mostly restricted to the case of instantaneous or massive attacks carried out on passive networks. In this paper, we shift the focus to the study of progressive and rapid attacks on networks that can respond in an active fashion. In the process, we design several techniques that managed networks can adopt to minimize the damages, and also to efficiently recover from the aftermath of successful attacks. We find that the *PL nature of the networks can be judiciously utilized for such protection and recovery purposes*.

1.1. Instantaneous vs. progressive attacks and reactive vs. non-reactive networks

Susceptibility of networks to attacks has been traditionally studied in the context of what may be termed as *instantaneous attacks*, where a randomly selected set of nodes and edges are deleted while the network is kept static. Hence, for all purposes, the targeted nodes and edges are deleted simultaneously. The effect of such instantaneous attacks is then studied in terms of the *connectivity structure* of the network that is left behind after the attack, i.e., how many connected components are there in the compromised network, and if there exist *giant connected components* that contain a constant fraction of the remaining nodes. It is well known, for example, that in random Erdös–Rényi (ER) networks [2] it is sufficient to remove nodes independently with a probability *above a certain threshold* in order to break up the network into many subnetworks that are *all small in size*. Thus, random ER networks are considered susceptible to random deletions of nodes, or just *instantaneous random attacks* (IRAs). The case where the deleted nodes are picked non-uniformly randomly (e.g., *preferentially* with respect to their degrees) has also been studied; for the purposes of this paper, such attacks will be termed as *instantaneous targeted attacks* (ITAs).

From a network management perspective, a key feature of such attack models is that the network remains *passive* or *non-reactive* during an attack: the removal of nodes and edges occurs without allowing the network to take actions (for example, inserting extra edges or allowing a deleted node to rejoin the network) to minimize the disruptive effects of the attacks. We shall refer to such networks as *non-reactive* networks. On the other hand, if a networked system takes active compensatory measures to maintain its integrity during an attack, or if it takes measures to recover from the damages inflicted by an instantaneous attack, then we will refer to such networks as *reactive* networks. Moreover, an attack that takes place at rates comparable to the response time of a network will be referred to as a *progressive* or *gradual* attack (as opposed to instantaneous attacks). In this paper, instead of only studying the case of instantaneous attacks on non-reactive networks, *we explore the cases of both progressive and instantaneous attacks on reactive and dynamic networks*, and study how the underlying networks can protect against, and recover from such attacks.

1.2. Instantaneous attacks on random and grown PL networks

Both IRAs and ITAs have been studied using the concept of percolation theory. Consider a network of size N in which the largest connected component comprises a fraction λ of the nodes. The site percolation process proceeds as follows: take a constant probability $0 \leqslant p \leqslant 1$ (i.e., independent of the size parameter N) called the *percolation probability*. Delete each node in the network independently with probability $1-p$ and retain it with probability p. For large N, the resulting network will have almost pN nodes. Out of these pN nodes, a set of $S(N,p)$ nodes will form a single connected component of the largest size. The main lesson of percolation theory is that for many families of graphs there exists a $p_c > 0$, such that if $p > p_c$ then $\lim_{N\to\infty} S(N,p)/Np = \lambda'(p) > 0$, and if $p < p_c$, then $\lim_{N\to\infty} S(N,p)/Np = 0$. The critical percolation probability, p_c, is called the *percolation threshold.* This *uniform instant site percolation process* is a particular case of IRAs introduced earlier.

One can generalize the above-mentioned percolation concept of picking nodes randomly but uniformly, to where the nodes to be deleted, are picked randomly, but with a distribution based on their degrees. For example, the case of *targeted instant site percolation process* (or ITAs) might consist of (i) deleting all nodes of degree greater than a pre-specified value of say k_0, or (ii) if the fraction of nodes with degree k in the original network is p_k, then the fraction of nodes of degree k after the attack is reduced to $p'_k = bk^{-q}p_k$, where b is a normalization constant. In both cases, the high-degree nodes are the targets of severe attacks, and the low degree nodes are mostly left alone. An ITA can arise from actual targeted selection of nodes by an active attacker, who searches for, and destroys high degree nodes explicitly. Another important source of ITA is the cascade-based attacks, in which the transfer of the load of a failed node to other nodes will result in a cascade of failures of nodes with high loads (which are usually nodes with higher degrees). Since this avalanche effect takes place in a short time, it can be categorized as an ITA [5].

Throughout this work we distinguish between two major models of PL networks: (i) the random network model, where a power-law network is chosen randomly from all networks with the same PL degree distribution. We call these networks *random PL* networks. These networks are sometimes called equilibrium networks as well [6]. *One* major property of these networks is the lack of correlation between the degree of neighboring nodes. (ii) *Grown PL networks*, on the other hand, are those networks for which the emergence of the PL degree distribution is due to an ongoing dynamical process, like the growth and rewiring. These network models are sometimes called non-equilibrium networks too.

The percolation properties of *random heavy-tailed PL* networks have been studied extensively [7–9] and provide a mixed message when it comes to their vulnerabilities to IRAs and ITAs. For IRAs, the percolation theory reveals a very promising fact: *the percolation threshold of these graphs is zero*. That is, no matter how small the percolation probability, p, is, the remaining nodes in the percolated network has a giant connected component. Thus, random PL networks can withstand IRAs with arbitrarily high rates. Previous studies, however, have also shown that the *random PL networks are more vulnerable to ITAs*, e.g., removal of a large number of only high degree nodes from PL networks is enough to fragment the network such that a giant connected component does not exist [7,10,11]. Thus, by removing a constant fraction of all nodes preferentially, one can destroy the connectivity of the network; note that *the attacker still has to remove almost all the high-degree nodes* to do so, which might be a difficult task to accomplish [10].

In many situations, however, grown PL networks provide a better model for the application in hand. For example, the simple preferential attachment dynamic and its variants can give rise to PL grown networks with several tunable topological characteristics.

Unlike the case of the random PL networks, currently there is *no instantaneous percolation theory for these grown PL networks*. Nevertheless, empirical studies suggest that these networks are also both resilient to random deletions of their nodes (IRAs), and vulnerable to targeted attacks just as in the case of random PL networks [12].

For both random and grown PL networks, while we know that they are vulnerable to severe ITAs, the issue of how to recover from such attacks and glue the fragmented network back together efficiently has not been addressed. We show in Section 4 how the PL structure of the network can in fact be an asset in this recovery process.

1.3. Progressive attacks and grown power-law networks

Recall that in progressive or gradual attacks, the deletions of nodes and edges take place at rates comparable to those at which the dynamic of the grown network itself operates at. For example, a *progressive attack* might correspond to a scenario, where randomly chosen existing nodes in the network (picked preferentially or uniformly with respect to the degree of a node) are removed at the *same rate* at which *the new nodes join in*. What do such progressive attacks do to the grown networks as opposed to the well-studied case of instantaneous attacks?

Consider the simple case of linearly preferentially grown network [13], where in addition to a node joining the network at each time step, a *uniformly* randomly chosen existing node in the network is deleted with probability c at each step. Such a dynamic is considered in detail in Refs. [3,4,6,14]. The work of Moore et al. [4], in particular, calculates the exact degree distribution of the networks resulting from such a dynamic.

It turns out that unlike the instantaneous attack case, where a grown network is resistant to IRAs, *a grown network* is very *vulnerable to random progressive attacks*. However, the *connectivity structure of the attacked network is no longer a relevant measure* to study the effect or severity of the progressive attacks; the network almost always remains connected, or has a giant connected component. As shown in Ref. [14], *the damage to the network manifests itself by forcing the network to rapidly lose its heavy-tailed distribution* (i.e., the PL exponent becomes much greater than 3, even as c increases only marginally), and the resulting grown network starts resembling networks with exponential degree distributions under the attack.

A *reactive* grown network, however, may take *remedial actions*, and one might ask if there exist compensatory dynamics that will restore the heavy-tailed distribution even in the presence of the random progressive attack. It was shown in Ref. [14] that indeed the linear-preferential attachment dynamics can be modified in a very simple and local fashion to preserve the heavy-tailed degree distribution and the PL nature of the grown network. The compensatory procedure is intuitive and greedy: *whenever a node loses a connection*, which can only happen when a neighboring node is deleted due to the progressive attack, *it compensates for it by making a new preferential connection* with a certain probability n. Thus, the *dynamics remain strictly local* (each node reacts only if it is directly impacted by the attack dynamic) and yet, the end result is that the damages to the global topological properties of the network are repaired, even in the limit of extremely high deletion rates (i.e., $c \to 1$).

This particular case study brings out two important differences between instantaneous and progressive attacks: (i) while a grown network might be resistant to IRAs, it can be extremely vulnerable to progressive random attacks. The damage to the network is no longer in terms of a loss in connectivity, but rather in terms of other topological properties of the network. (ii) It is, however, possible to make the dynamical rules of the grown networks to be reactive, and generate networks that are extremely resistant to both gradual and instantaneous random failures and attacks.

1.4. Protecting against and recovering from attacks in reactive power-law networks: a summary of results

We first consider *protection against progressive or gradual targeted attacks in grown networks.* The need to address this type of intentional attacks is *particularly urgent in designer complex networks, such as the P2P networks* (see Section 5 for more details), where performing a comprehensive large-scale attack on all the high-degree nodes is an expensive, and often, a very difficult task. However, *gradual deletions of high-degree nodes* by first crawling the network and identifying the high-degree nodes that serve as conduits for communication among low-degree nodes, and then attacking some of these nodes *might be quite feasible*.

Clearly, if no precaution or compensatory action is taken against such an attack, then as exemplified in the case of progressive random attacks [14], one would lose key topological features, including a loss of its heavy-tailed degree distribution. How to equip the network with proper feed-back strategies to mitigate the damaging effects of the attacks and failures? These feedback strategies, moreover, must obey some stringent criteria: they must be local, in the sense that they should be triggered and adjusted only based on first neighbor information. In Section 2 we introduce one such dynamical compensatory algorithm to mitigate the effect of linear-preferential attacks. In particular, we show that, only with simple local modifications to the dynamics, the network can restore much (but not all) of its heavy tail. *The resulting degree distribution is shown to be a PL with an exponential cutoff at a point that is inversely proportional to the rate of the targeted attack*. Again, there is always a giant connected component, and the main effect of the attack is to introduce an exponential cutoff, and lower the PL exponent marginally. Thus, while the attacked network does lose its unbounded degree variance, the compensatory dynamics manage to preserve the overall PL degree distribution, and as shown next, keep the network in a state, from which it can recover in a local fashion.

We next show in Section 3.1 that a *preferentially attacked network can perform large-scale network repairing and maintenance operations* and selectively add edges, so as to delay the exponential cutoff by increasing k_{max}, the largest degree of all nodes, by any desired scaling factor; thus, this can repair the cutoff problem resulting from linear-preferential attacks. The recovery procedure is local, in the sense that each node independently decides how many preferential connections to create, and no global coordination is necessary. This procedure retains the exponent of the PL distribution, and only increases the maximum-degree of the distribution, so that the exponential cutoff point is not a limiting factor.

Next, we consider the case of *recovery from a large-scale targeted attack*. A heavy enough and instantaneous targeted attack will finally fragment any static or dynamic network. In Section 4 we for the first time consider the challenging problem of repairing a complex network fragmented by targeted attacks. The disaster recovery consists of two distinct phases, and the first is to *recover the lost connectivity*. We show that with only a few essential communication paths one can create a giant connected component and glue the network fragments. In particular, we first show (both analytically and numerically) that when PL networks are fragmented due to targeted attacks, it results in small-size connected components, the *size distribution* of which is again *heavy tailed*. This allows us to prove that the connectivity of the whole fragmented network can be restored with only a few successful random connections, via the process of *reverse percolation*. Thus, the nodes of the network will be able to communicate to each other to transfer *vital* "low-rate" messages, as long as a few random connections among the nodes can be established. *Recovery of the topology*, can then be achieved, once connectivity is established. Such a recovery step could consist of applying one of the many dynamical rules [1,13,14] that would allow it to regain its PL structure.

2. Reactive grown networks in presence of linear-preferential attacks and compensation

This section considers a progressive attack, where at each time step in addition to a node joining the network, a preferentially chosen node is deleted with probability r. Nodes that loose neighbors to attack do not sit still, instead they react and replace those lost neighbors; moreover, the attacked nodes rejoin the network as new nodes. We show that such a compensatory dynamic in the presence of linear-preferential progressive attacks naturally leads to a *PL degree distribution with an exponential cutoff*, where the cutoff depends on the preferential deletion rate. Thus, while the attack bounds the maximum degree of the distribution, the compensatory protocol is able to preserve the exponent of the PL distribution. Moreover, as shown in our simulations, as long as each incoming node makes $m \geqslant 2$ random preferential connections, there always exists a giant connected component, even for very high rates of preferential attacks (see Table 1); thus the loss of connectivity is not one of the damaging effects of such progressive attacks.

Our model is a time dynamic one. At each step:

1. A new node s is added to the network and makes m preferential attachments.
2. With probability r a preferentially selected node w is chosen. The preferential selection procedure selects the node w with degree $k(w,t)$ with probability $k(w,t)/\sum_i k(i,t)$. The selected node w is then deleted from the network, were deletion process is:
   - Delete node w and all its edges. Then w starts as a new node and makes m preferential attachments.
   - For all nodes z that were connected to w and have lost an edge, each one compensates by adding an edge preferentially.

Using rate-equation approaches, the steady state degree distribution of the network emerging from the above model is found to be a PL with an exponent, $\gamma = (3+2\varepsilon)/(1+2\varepsilon)$ and an exponential cutoff at $k_c = \langle k\rangle(1/2+\varepsilon)/r = (m/r+1)(1+2\varepsilon)$, where $\varepsilon \equiv r(m+a-1)/2(m+r)$ and a is the second moment of the degree distribution, and is a constant.

Table 1
$s(r)$, the fraction of nodes in the largest connected component for various values of r

r	0.03	0.05	0.2	0.3
$s(r)$	1.0	0.998	0.992	0.975

Obviously, connectivity of the network is preserved even for large values of r.

Table 2
Approximate degree of the exponential cutoff for various values of r

r	0.0	0.01	0.03	0.05	0.07
$k_{c(r)}$	27	20	14	12	8

The network size is 50 K and $m = 2$.

2.1. Simulations

We have performed Monte Carlo simulations to validate the results. We grow the network where at each step a node is added and makes $m = 2$ preferential attachments. Then with probability r we delete a node, choosing a node to be deleted preferentially. Table 2 shows the effect of low rate preferential deletion as imposing an exponential cutoff on the PL degree distribution.

3. Decentralized and distributed healing of sharp cutoffs in PL networks

We consider a connected PL network where the tail (i.e., the set of high degree nodes) is removed. We first show how a local compensation process, involving the creation of new links, can restore the maximum degree to a multiple of the existing cutoff. Each node decides randomly and independently how many preferential edges to insert, and thus the healing process does not need any central coordination mechanism. Such a healing process can be periodically applied by, for example, a network created by the dynamics described in the previous section, where a cutoff in the degree distribution is naturally introduced.

3.1. Healing process

Consider a *short-tailed* PL network of exponent α and maximum degree k_0. The objective of the healing process is to increase the maximum degree of the distribution by a stretch-factor $w = k_{max}/k_0$, so that the maximum degree after the healing process will increase from k_0 to k_{max}, while the PL exponent remains the same.

Healing algorithm: Given a PL network with exponent α, each node i independently decides to compensate with some probability p. The compensation process involves making $(w-1)k_i$ new *preferential* connections where k_i is the degree of the ith node.

Let $P(k)$ and $P'(k)$ be the degree distributions before and after the healing process, respectively, then one can easily show that given $P(k)$ is a short-tailed PL with maximum degree k_0 and $p \approx w^{-\alpha}$, $P'(k)$ follows a PL distribution as $\lambda(w,\alpha)k^{-\alpha}$. Where λ is a constant depending on w and α and cutoff is increased to k_{max}. In other words, the effect of the healing process is simply to stretch the degree distribution by a linear factor. Now since the degree distribution is *power-law* to begin with, such stretching will not change the distribution. Thus PL degree distribution of the original network is the key for the simple healing process to succeed.

Performing preferential attachment locally: While preferential attachment is a global decision process at the first sight, it can be efficiently implemented locally, provided that the network is connected. The idea is to initiate a random walk from a node that is interested in sampling the nodes preferentially. For a long enough walk, the probability that the random walk visits a node with degree k is well known to be proportional to k. The required length of this walk is shown to be at most $O(\log N)$ for most family of random and grown graphs (including PL random graphs and BA networks) [15,16].

3.2. Autonomous healing

So far we have considered a *static case*, i.e., we are given a network with a sharp cutoff, and the nodes randomly decide to introduce new edges to restore the cutoff to a desired value, k_{max}, while retaining the same PL exponent, α, as before. One can modify this static scenario to an *adaptive version*, where instead of all the nodes acting at once, each node reacts whenever it loses an edge unannounced, i.e., due to an attacked node going down. The idea is to naturally detect a heavy attack and initiate the healing process.

Feedback algorithm: Each node i when losing an edge *without prior notice* performs the healing algorithm of Section 3.1 with probability $1/k_i$, where k_i is the degree of the ith node.

Clearly, any targeted deletion of nodes in the tail of the degree distribution, i.e., high degree nodes, will result in the deletion of a constant fraction of the edges of the system. If we further neglect the degree correlation of the nodes, the probability of any edge being deleted when nodes of degree greater than k_0 are deleted will be given by:

$$\widetilde{p} \approx \frac{\Sigma_{k_0}^{k_{max}} kP(k)}{E} = \lambda k_0^{2-\alpha}, \tag{1}$$

for some constant λ in the order of 1. Then, the probability of a node with degree k losing an edge is $\widehat{P}_k \approx k\widetilde{p}$. Thus the probability of a node initiating the healing process is approximately $\widehat{P}_k/k = \widetilde{p}$, a constant depending on only the intensity of the attack. We must re-state that we have not considered second-order effects and degree correlations here. This algorithm is basically intended to detect any large-scale instantaneous deletion of a fraction of network edges. Thus, *the algorithm ensures that a constant fraction of the nodes will always perform the healing algorithm in the case of a large enough attack.*

We have performed the Monte Carlo simulations of the healing and feedback algorithm. Fig. 1 shows how the healing algorithm works for different values of α.

4. Restoring connectivity in a fragmented power-law network

Any network will breakdown under a sufficiently heavy targeted attack, and the question we ask is how many random connections among the nodes in the fragmented network we need to establish before a giant connected component emerges. The goal of this section is to show that both *grown and random* PL networks are very amenable to quick bootstrapping from an attack, and with almost no global coordination. In particular, we will show that even under very intense attacks, only an infinitesimally small probability of success for new connections is enough to quickly reconnect most of the broken network.

For example, consider a linearly preferentially grown PL network of size 50,000 and average degree 4, that has undergone a very heavy targeted attack in which all nodes of degree more than 50 are lost. For a particular simulation, the size of the largest component was only 371 after the attack. Now assume that all the nodes try to initiate only one random connection to some other node in the network in a hope to restore the connectivity. If the probability of success of each of these attempts is only 5%, our simulations show that a very large component of size more than 20,000 forms. This probability of success will go asymptotically to zero as the network size increases. Of course, other reconstruction algorithms will be required to repair the topological damages to the network, as was the subject of the algorithms in Section 3.1.

The results in this section will follow the following pattern: first we will argue that grown PL networks fragmented under a targeted attack, have components whose size distributions are heavy-tailed PLs. Thus, even though the average size of the connected components is bounded, the variance is unbounded (or very large). While a proof for grown networks is difficult in general, we show analytically that for a linearly preferentially grown *tree* network (i.e., each node joining the network makes exactly one preferential connection) the removal of the highest degree node indeed creates disconnected components with a PL size distribution. We then show, using the generating functions formalism, that the same phenomenon can be observed in *random PL networks* for special forms of targeted attacks.

Next, we prove that as long as we have components with heavy-tailed size distribution, then only a vanishingly small number of random connections will glue the fragments together into a giant connected component.

4.1. Distribution of the size of components after attack: grown power-law graphs

Generally, instantaneous percolation (and hence attack) on grown graphs is hard to analyze. For some special cases, however, the statistics of the connected components after a preferential attack can be tracked.

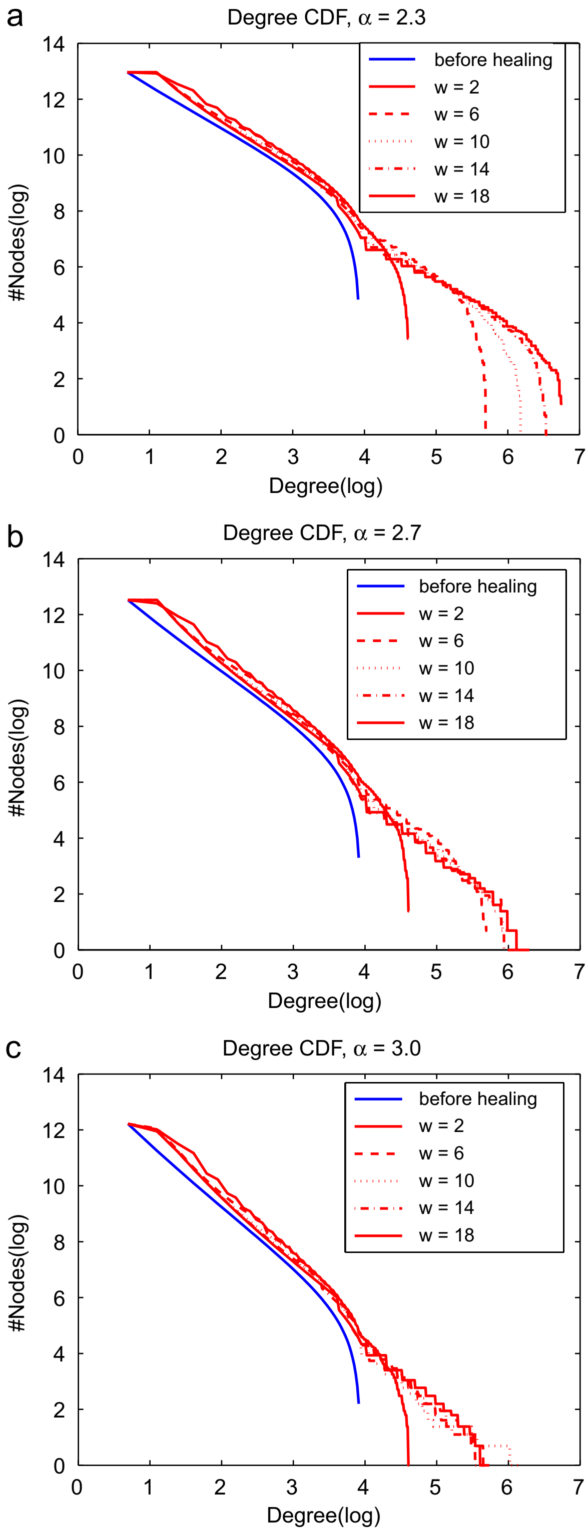

Fig. 1. Degree distribution before and after healing for various values of power-law exponent α and stretch factors w: the power-law exponent from the fit to the degree distribution from top to down is; $\gamma \approx 2.4, 2.7, 3.2$, respectively.

In this section, we compute the distribution of the sizes of the connected components for graphs grown under the preferential attachment (Barabasi–Albert graphs) with $m = 1$: at each time step, a new node is added to the network and initiates *one* preferentially targeted link. The probability that the ith node receives this link is $k(i,t)/\sum_{j=1}^{t} k(j,t)$, where $k(i,t)$ is the degree of the ith node at time t.

At some time $t \gg 1$, a preferential attack occurs, and deletes the oldest node $i = 1$. As a result of such attack, the network will be fragmented into many connected components. We now show that the size of these components have a PL distribution, and in particular, the probability that a randomly chosen component has size C is $\propto C^{-3/2}$.

Before continuing, we need the following observations: (i) Since $m = 1$, the network topology is a tree. (ii) Take any node i and consider the subtree rooted at i and consisting of all the nodes younger than i. The size of this subtree, denoted by $T(i,t)$ can be calculated as follows: at time $t = i$, this subtree has had only one node (with one link to some other node $j < i$), thus $T(i,i) = 1$, while there has been i other links in the network. The rate of change of $T(i,t)$ can be written as:

$$\frac{\partial T(i,t)}{\partial t} = \frac{(2T(i,t) - 1)}{2t}.$$

If 1 can be neglected compare to $2T(i,t)$ (which is certainly true when $t \gg i$), one gets: $T(i,t) = (t/i)$.

Now, note that from the rate-equations, the degree of a node inserted at time i, at a later time t is given by: $k(i,t) = (t/i)^{\beta}$ for $\beta = \frac{1}{2}$. Thus the degree of the first node is around $k(1,t) = t^{1/2}$. Thus, once the first node is deleted, exactly $k(1,t)$ connected components will be created (remember the network is tree). Lets enumerate these components by the sets $C_1, C_2, \ldots, C_{k(1,t)}$. Let κ_j, $j = 1, 2, \ldots, k(1,t)$ be the oldest node in each C_j. By construction of the network, the node κ_j must have been connected to the first node ($i = 1$). Now note that the size of the subtree C_j is simply $|C_j| = T(\kappa_j, t) = (t/\kappa_j)$. This will allow us to find the probability that a randomly chosen connected component has size C as follows:

$$\begin{aligned} P_C &= \frac{\#Components\ of\ size\ C}{k(1,t)} \\ &\propto \left(\frac{Pr\{\kappa\ connected\ to\ 1\}}{k(1,t)} \times \left|\frac{\partial \kappa}{\partial C}\right| \right)_{\kappa^*: T(\kappa^*,t)=C} \\ &\propto \frac{(\kappa^*)^{\beta}}{\kappa^*} \times \left|\frac{\partial \kappa}{\partial C}\right|_{\kappa^*: T(\kappa^*,t)=C}. \end{aligned}$$

Now, note that $T(\kappa^*, t) = (t/\kappa^*) = C$, and $|\partial\kappa/\partial C| = tC^{-2}$. Therefore

$$P_C \propto \frac{C^{-\beta}}{C-1} \times C^{-2} = C^{-3/2}.$$

In Ref. [17], Newman et al. have shown that for any *static* random graph, the distribution of the size of the components just before the phase transition and the appearance of a giant connected component obeys the same scaling law as $P_C \propto C^{-3/2}$. So interestingly, while the deletion of a key node (the first node) fragments the network into many components (around $t^{1/2}$ different pieces), the distribution of the sizes of these components obeys a PL.

For more complex randomly grown graphs, no theory of percolation currently exists to obtain the distribution of the connected components. Simulations, however, indicate that the same observations still hold for many such networks. One such simulation is reported for networks grown with the deletion compensation protocol introduced in Ref. [14], and is reported in Fig. 2.

4.2. Distribution of the size of components after attack: static power-law graphs

We now show that the same observations hold for some form of random targeted attacks on static PL networks as well. The size distribution of the connected components of any static random network on a given degree distribution can be found analytically using the generating functions formalism [17]. In particular, the

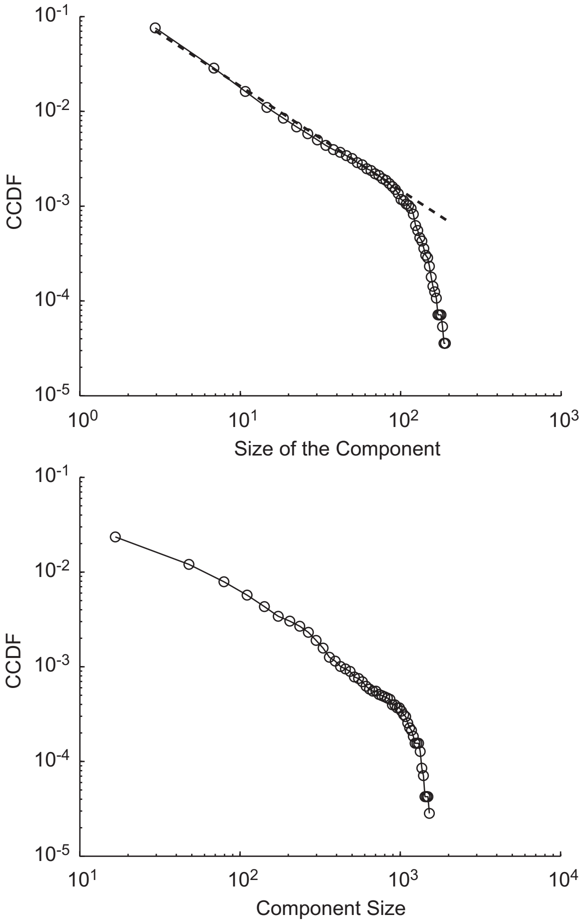

Fig. 2. The distribution of the size of the connected components for heavily attacked networks of size 50,000 after a targeted attack that deleted all the nodes with degree greater than 50. (top) Linearly preferentially grown PL network (Barabasi–Albert model) when the average degree is 4. (bottom) Deletion–compensation networks of Ref. [14], with $\gamma \approx 2.3$ and average degree 6.

variance of the distribution of the size of these components is derived analytically in Appendix B, which also contains a brief introduction to generating functions formalism.

Consider the generating functions of an attacked network:

$$G_0(x) = \sum_{i=1}^{\infty} q_k p_k x^{-k} = \sum_{i=1}^{K} q_k p_k x^{-k},$$
$$G_1(x) = \frac{G_0'(x)}{G_0'(1)}, \tag{2}$$

where q_k is the probability that a node with degree k is deleted through the attack and K is the maximum (or cutoff) degree of the nodes in the network. One defining characteristic of PL networks is their relatively large cutoff degree.

This would define a form of targeted attack if q_k decreases with k. In particular, we examine a targeted attack for which $q_k = bk^{-q}$ where q is a measure of the how targeted the attack is and b is a normalization constant. Then, the generating functions of the attacked network for an original PL graph with exponent τ are:

$$G_0(x) = \sum_{k=1}^{K} c_1 k^{-\tau-q} x^{-k}, \tag{3}$$

$$G_1'(1) = c' \sum_{k=1}^{K} k^{-\tau-q+2} = O(K^{-\tau-q+3}), \tag{4}$$

for some positive constants c, c' when $\tau + q \geqslant 2$. In particular, for the linear targeted attack, $q = 1$, this value is always finite for any $\tau > 2$.

It should be noted that such preferential attack would in effect increase the value of τ by an amount of q. Thus following the approach of Aiello et al. [18], one can show that no giant connected component will exist when $\tau + q > \beta_c \approx 3.478$.

Although the network might not have any giant connected component, the variance of the distribution of the sizes might still diverge. This is shown through $G_1''(1)$ (see Eq. (B.4)):

$$G_1''(1) = \sum_{k=3}^{K} k(k-1)(k-2)bk^{-\tau-q} \propto K^{-\tau-q+4}, \tag{5}$$

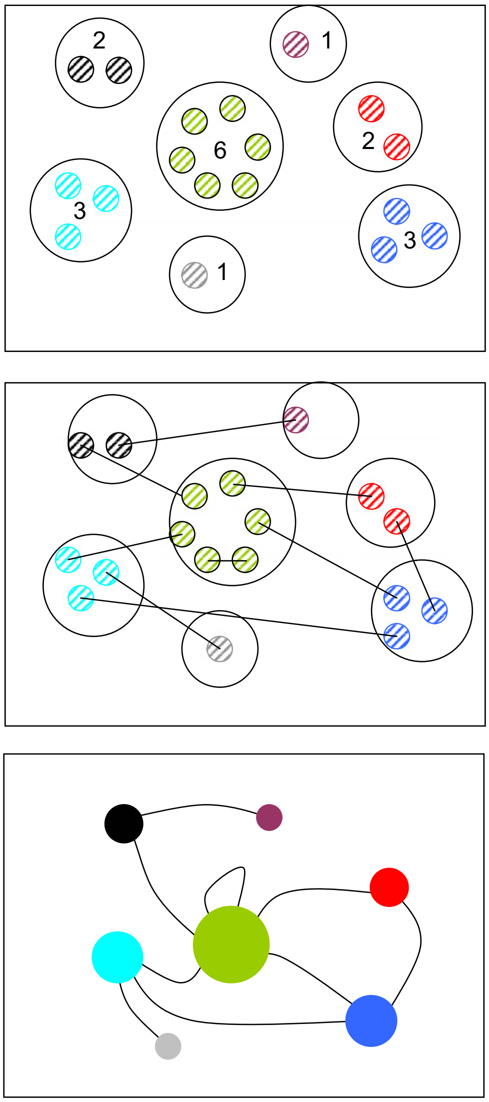

Fig. 3. Constructing a random graph on degree distribution, $n_1 = 2$, $n_2 = 2$, $n_3 = 2$, $n_4 = 0$, $n_5 = 0$, $n_6 = 1$. For any node of degree i, i dummy copies are created. Then a random matching is performed on this hyper graph. All the dummy nodes corresponding to one real node, are then collapsed into one nodes, to form the actual graph.

which diverges for any q provided that $q < 4 - \tau$. In particular, for the linearly targeted attack, $q = 1$, the variance of the size of connected components diverges if $2 < \tau < 3$, even though the average component size is finite at least when $\tau > 2.349$.

4.3. The reverse percolation process

The main idea behind the results in this section is what we will refer to as the *reverse percolation* process: consider an attacked network, as in Fig. 3. Now let us start adding random edges between the nodes of this network of many small components. As the number of such random links increases, different components of the network will start to *glue* together until a giant connected component occurs which contains most of the nodes of the network. Let us call $Q(k)$ the distribution of the sizes of these small components, that is, $Q(k)$ is the fraction of these components that have size k. We claim that the reverse percolation process corresponds to a percolation on a random graph with degree distribution $P(k) \equiv Q(k)$. To see this we need to recall the

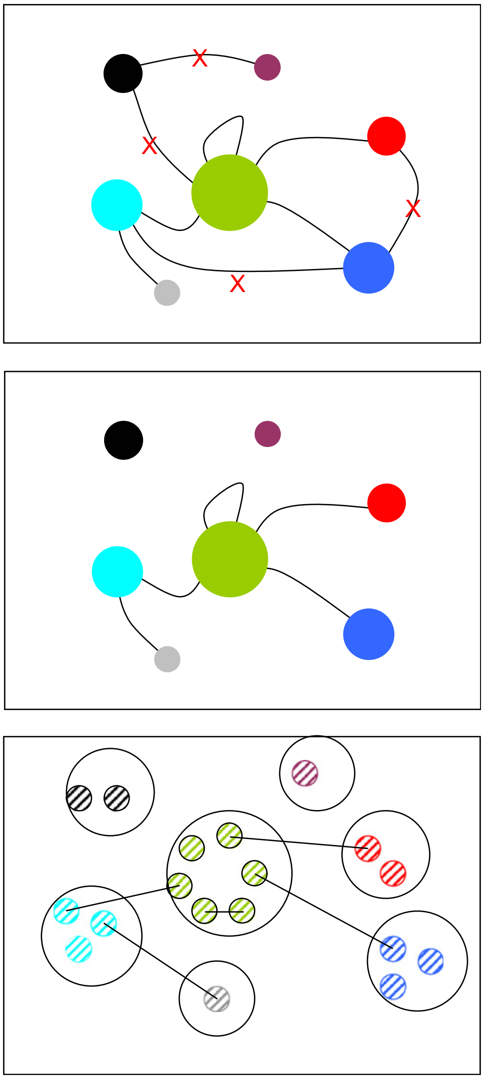

Fig. 4. Percolation and reverse percolation process: bond percolation corresponds to random deletion of the links of a network. In the top figure, 4 out of 10 links of the random network generated in Fig. 3, are deleted, resulting in the middle graph. This was equivalent to doing the random graph matching on the hyper graph with only $10 - 4 = 6$ links instead of 10 links (the bottom figure).

method with which a random graph with a prescribed degree distribution $P(k)$ is built on N nodes [19] (see Fig. 3).

To construct a random graph with degree distribution $P(k)$, one can proceed as follows [19]: for any k, there will be $NP(k)$ nodes of degree k in the network, labelled as $V_1^k, V_k^2, \ldots, V_{NP(k)}^k$. For each of these nodes create k dummy duplicate nodes. To be specific, call the duplicates of the i'th node as $V_{i,1}^k, V_{i,2}^k, \ldots, V_{i,k}^k$. Now on this hyper graph, one can start a random matching. After the matching, one will collapse the duplicates of a node i into one node, and therefore all the links to the duplicates will now be links to the collapsed node itself. A *reverse percolation process* with probability p can be interpreted as introducing random edges, i.e., doing the random matching with a fraction p of all the links in the hyper graph.

With this construction in mind, the validity of our claim is readily understood. In the connectivity restoration process, *any connected component can be viewed as the duplicate nodes of a single node*, and the insertion of random edges can be viewed as a (reverse) percolation process on a graph whose degree distribution is equal to the distribution of the component sizes of the real broken graph (see Fig. 4). In the usual percolation process, keep each edge with probability p, which in the random graph construction process, basically involves doing random matching with probability p, in the network with duplicated nodes. With this correspondence, many of the well-known results for the percolation process on random graphs with a given degree distribution can be readily applied to the gluing process.

In particular, the percolation threshold, corresponding to the probability of successful attempts required for a giant component to appear can be calculated as: $q_c = \langle C\rangle/(\langle C^2\rangle - \langle C\rangle^2)$ where $\langle C\rangle, \langle C^2\rangle$ are the average and variance of the distribution of the connected components (see, for instance, for Ref. [7]). While the average size of the connected components in a heavily attacked network is finite, it is possible for the variance of this distribution to be very large. In that case, the corresponding percolation threshold will be small. In other words, one would only require an infinitesimally small fraction of random links to glue most of the disjoint components together. In particular, if the distribution of the size of the connected components follows a PL distribution with exponent $2<\alpha<3$ and maximum component size $C_{max}\gg 1$, then only $O(C_{max}^{\alpha-3})$ successful random links per component is enough to ensure that most of the disconnected components are reconnected.

5. Concluding remarks

We have addressed the issue of attack management in PL networks that are reactive, and can take local steps to combat attacks. In particular, we have shown how grown networks can cope with both random and linear-preferential progressive attacks, where nodes are deleted as the network grows. We also presented a number of recovery schemes, including repairing of sharp cutoffs in PL degree distributions, and restoration of connectivity in networks fragmented by large-scale targeted attacks. All these compensatory mechanisms are shown to be local, in the sense that global coordination among the nodes is not required, and the nodes initiate new edges only in reaction to changes in their immediate environment.

There are several interesting implications of the results presented in this paper in terms of complex network theory as well. For example, Section 2 presents a network dynamic that leads to the emergence of PL degree distributions with exponential cutoffs; perhaps, such a mechanism can model existing networks where such degree distributions have been observed empirically. Similarly, when one studies the distribution of the size of the connected components in the networks generated by the dynamic in Section 2, then one observes that there is always a giant connected component, but more interestingly, the rest of the components have a power-law size distribution. Such a component size distribution has been observed, for example, in the world wide web (WWW) network, and one wonders if a low-grade preferential deletion of high-degree nodes in the web is one of the dynamical forces shaping the underlying connectivity structure.

Appendix A. Finding k_c and γ

We adopt the same rate equation approach as Refs. [14,20] for our analysis. Label each node with its insertion time to network, i. Define degree of ith node at time t as $k(i,t)$. When a node is deleted its joining time is reset. Let $S(t) = \sum_i k(i,t) = 2E(t) = 2(m+r)t$ and total number of nodes at time t, $N(t) = t$. The mean degree is $\langle k\rangle = 2(m+r)$. We want to find $P(k)$, i.e., probability that a randomly chosen node has degree k at steady state ($t \to \infty$). We also define $f(t)$ as average number of edges deleted at time t when a node is deleted preferentially, that is the average degree of a node chosen preferentially: $f(t) = \langle k(i,t)^2 \rangle / \langle k \rangle$. Note that obviously $\langle k \rangle \leqslant f(t) \leqslant E(t)$. Define the probability that ith node is not deleted before time t (is still in the network) as $D(i,t)$. The initial conditions are $D(i,i) = 1$, and $k(i,i) = m$. Next we write master equations for $k(i,t)$ and $D(i,t)$

$$\frac{\partial k(i,t)}{\partial t} = m\frac{k(i,t)}{S(t)} + rm\frac{k(i,t)}{S(t)} + rf(t)\frac{k(i,t)}{S(t)}, \tag{A.1}$$

where the first term corresponds to m preferential attachments, the second term corresponds to deleted node rejoining the network, and the last term represents preferential compensation of on average $rf(t)$ edges. Note that since each node compensates for lost edges there is no negative term in the equation. Also at time $t+1$ the probability that ith node still exist in the network is given by:

$$D(i,t+1) = D(i,t)\left(1 - r\frac{k(i,t)}{S(t)}\right),$$

$$D(i,t+1) - D(i,t) = -rD(i,t)\frac{k(i,t)}{S(t)},$$

$$\frac{\partial D(i,t)}{\partial t} = -rD(i,t)\frac{k(i,t)}{S(t)},$$

$$\begin{aligned}\ln\frac{D(i,s)}{D(i,i)} &= -\int_i^s \frac{rk(i,t)}{2(m+r)t}\,\mathrm{d}t \\ &= -\frac{r}{\langle k \rangle}\int_i^s \frac{k(i,t)}{t}\,\mathrm{d}t,\end{aligned}$$

$$D(i,s) = \exp\left(-\frac{r}{\langle k \rangle}\int_i^s \frac{k(i,t)}{t}\,\mathrm{d}t\right). \tag{A.2}$$

Define $\widetilde{k(i,s)} = \int_i^s \frac{k(i,t)}{t}\,\mathrm{d}t$, then $D(i,s) = \exp(-r\widetilde{k(i,s)}/\langle k \rangle)$. Note if $k(i,t)$ is lower bounded by Ct^β then $\widetilde{k(i,t)} \geqslant 1/\beta k(i,t)$:

$$\begin{aligned}&k(i,t) \geqslant Ct^\beta, \\ &\widetilde{k(i,t)} \geqslant \frac{k(i,t)}{\beta}.\end{aligned} \tag{A.3}$$

In order to solve for $k(i,t)$, we need to know $f(t)$, which depends on $k(i,t)$:

$$f(t) = \frac{\langle k^2 \rangle}{\langle k \rangle} = \frac{1}{N(t)\langle k \rangle}\sum_{i=0}^{t} k(i,t)^2 D(i,t). \tag{A.4}$$

When Eq. (A.3) is valid then:

$$\begin{aligned}f(t) &= \frac{1}{N(t)\langle k \rangle}\sum_{i=0}^{t} k(i,t)^2 D(i,t) \\ &= \frac{1}{t\langle k \rangle}\sum_{i=0}^{t} k(i,t)^2 \exp\left(-\frac{r}{\langle k \rangle}\widetilde{k(i,t)}\right) \\ &\leqslant \frac{1}{t\langle k \rangle}\sum_{i=0}^{t} k(i,t)^2 \exp\left(-\frac{r}{\beta\langle k \rangle}k(i,t)\right).\end{aligned}$$

Since $x^2\exp(-\alpha x)\leqslant \frac{4e^{-2}}{\alpha^2}$:

$$\begin{aligned} f(t) &\leqslant \frac{1}{t\langle k\rangle}\sum_{i=0}^{t}\frac{(\beta\langle k\rangle)^2}{r^2}4e^{-2} \\ &= \frac{4e^{-2}\beta^2\langle k\rangle}{r^2}. \end{aligned} \tag{A.5}$$

Thus we see that if $k(i,t)$ is a finite polynomial of positive powers of t, then $f(t)$ is a constant.

We know that $f(t)\leqslant E(t)=(m+r)t$, but edge deletion may reduce it further. Hence we consider the case where $f(t)=at^b$. We consider this for two cases, first where $b=0$, and second where $b>0$. If $f(t)=a$ then Eq. (A.1) becomes

$$\begin{aligned} \frac{\partial k(i,t)}{\partial t} &= (m(1+r)+ra)\frac{k(i,t)}{S(t)} \\ &= (m+r+r(m+a-1))\frac{k(i,t)}{2(m+r)t} \\ &= \left(\frac{1}{2}+\frac{r(m+a-1)}{2(m+r)}\right)\frac{k(i,t)}{t}, \end{aligned}$$

so, using $\varepsilon\equiv r(m+a-1)/2(m+r)$

$$\begin{aligned} \frac{\partial k(i,t)}{k(i,t)} &= \left(\frac{1}{2}+\varepsilon\right)1/t, \\ \ln\frac{k(i,t)}{k(i,i)} &= \left(\frac{1}{2}+\varepsilon\right)\ln(t/i), \\ k(i,t) &= m\left(\frac{t}{i}\right)^{1/2+\varepsilon}. \end{aligned} \tag{A.6}$$

Eq. (A.5) already showed that if $k(i,t)$ grows as a power of t, $f(t)$ is constant. The above shows that when we assume that $f(t)=a$, we see that $k(i,t)$ grows as a power of t/i.

We calculate $P(k,t)$ from $k(i,t)$ and $D(i,t)$ using Eq. (A.2):

$$\begin{aligned} D(i,s) &= \exp\left(-\frac{r}{\langle k\rangle}\int_i^s\frac{k(i,t)}{t}\,dt\right) \\ &= \exp\left(-\frac{r}{\langle k\rangle}\int_i^s m\left(\frac{t}{i}\right)^{1/2+\varepsilon}\frac{1}{t}\,dt\right) \\ &= \exp\left(-\frac{rm}{i^{1/2+\varepsilon}\langle k\rangle}\int_i^s t^{\varepsilon-1/2}\,dt\right) \\ &= \exp\left(-\frac{r}{(1/2+\varepsilon)\langle k\rangle}(k(i,t)-m)\right), \end{aligned}$$

$$\begin{aligned} P(k,t) &= \frac{1}{N(t)}\cdot\sum_{i:k(i,t)=k}D(i,t) \\ &= \frac{1}{t}D(i,t)\left|\frac{\partial i}{\partial k}\right|. \end{aligned} \tag{A.7}$$

If $k(i,t)=m(t/i)^{1/2+\varepsilon}$:

$$k(i,t)=m(t/i)^{1/2+\varepsilon},$$

$$(k(i,t)/m)^{2/(1+2\varepsilon)}=t/i,$$

$$i = t\left(\frac{k}{m}\right)^{-2/(1+2\varepsilon)},$$

$$\frac{\partial i}{\partial k} = t\frac{2}{1+2\varepsilon}\left(\frac{k}{m}\right)^{(-3-2\varepsilon)/(1+2\varepsilon)}.$$

Thus:

$$\begin{aligned} P(k,t) &= \frac{1}{t}D(i,t)\left|\frac{\partial i}{\partial k}\right| \\ &= \frac{1}{t}\exp\left(-\frac{r}{(1/2+\varepsilon)\langle k\rangle}(k-m)\right)t\frac{2}{1+2\varepsilon}\left(\frac{k}{m}\right)^{(-3-2\varepsilon)/(1+2\varepsilon)} \\ &= \exp\left(-\frac{r}{(1/2+\varepsilon)\langle k\rangle}(k-m)\right)\frac{2}{1+2\varepsilon}\left(\frac{k}{m}\right)^{(-3-2\varepsilon)/(1+2\varepsilon)}. \end{aligned}$$

So, when we assume that $f(t) = a$, or that $\langle k^2\rangle = a\langle k\rangle$, we see that we get a PL degree distribution with an exponential cutoff at $k_c = \langle k\rangle(1/2+\varepsilon)/r = (m/r+1)(1+2\varepsilon)$. As $r \to 0$, $k_c \to \infty$, as expected.

Now we consider the case of $f(t) = at^b$ with $b>0$:

$$\begin{aligned} \frac{\partial k(i,t)}{\partial t} &= (m(1+r)+rat^b)\frac{k(i,t)}{S(t)} \\ &= \left(\frac{m+r+r(m-1)}{2(m+r)}\frac{1}{t}+\frac{ra}{2(m+r)}t^{b-1}\right)k(i,t), \end{aligned}$$

$$\ln\frac{k(i,t)}{k(i,i)} = \left(\frac{m+r+r(m-1)}{2(m+r)}\ln t+\frac{ra}{2(m+r)}\frac{t^b}{b}\right),$$

$$\ln\frac{k(i,t)}{m} = \left(\frac{1}{2}+\beta\right)\ln(t/i)+\gamma\frac{t^b-i^b}{b},$$

$$\begin{aligned} k(i,t) &= m\left(\frac{t}{i}\right)^{1/2+\beta}\exp\left(\frac{\gamma}{b}(t^b-i^b)\right) \\ &\geqslant m\left(\frac{t}{i}\right)^{1/2+\beta} \end{aligned}$$

with $\beta = r(m-1)/2(m+r)$ and $\gamma = ra/2(m+r)$. We see that even if we assume that $f(t) = at^b$, then we find that $k(i,t)\geqslant m(t/i)^{1/2+\beta}$, but then according to Eq. (A.5), $f(t)$ is upper bounded by a constant, which implies that $k(i,t)$ only grows as a power of t as we saw in Eq. (A.6).

This result clearly shows that preferential deletion of nodes will impose an exponential cutoff on PL degree distribution of the growing networks thus removing high degree tail of the network which are essential for its functionality [21].

Appendix B. Variance of the distribution of the size of connected components in static random networks

Consider a random network on a given degree distribution $P(k)$ [17], that is the probability that a randomly chosen node has degree k is, $P(k)$.

$$G_0(x) = \sum_{k=1}^{\infty} P(k)x^{-k} = \sum_{i=1}^{K} P(k)x^{-k},$$

$$G_1(x) = \frac{G_0'(x)}{G_0'(1)},$$

as the generating functions of the degree of a node arrived at by choosing a random node or link, respectively, where K is the maximum degree of the nodes in the network. For the family of PL networks, we assume that the cutoff degree K diverges as the network size N goes to infinity.

Similarly, one can define $H_1(x), H_0(x)$ as the generating function of the size of the connected components arrived at by following a random link and node, respectively.

When a giant connected component does not exist and therefore the graph is tree like, these four functions should be related through the following consistency equation:

$$H_1(x) = xG_1(H_1(x)), \tag{B.1}$$

$$H_0(x) = xG_0(H_1(x)). \tag{B.2}$$

The average distribution of the sizes of the connected components is:

$$\langle s \rangle = H_1'(1) = 1 + \frac{G_1'(1)}{1 - G_1'(1)}.$$

The phase transition happens when $G_1'(1) = 1$ and a giant connected component appears (or disappears).

The known literature has always been interested in the average size of the connected components due to its phase transition and physically measurable properties. We will, however, examine the properties of the second moment of the distribution of the size of the connected components.

Twice differentiating $H_1(x)$ in (B.1):

$$H_1''(x) = G_1'(H_1(x))H_1'(x) + H_1'(x)G_1'(H_1(x)) + xH_1''G_1'(H_1(x)) + x(H_1'(x))^2 G_1''(H_1(x)). \tag{B.3}$$

Once differentiating $H_1(x)$ in (B.1) results in:

$$H_1'(1) = \frac{2}{1 - G_1'(1)}.$$

Plugging this into (B.3) evaluated at $x = 1$ will result in:

$$E\{size^2\} = H_1''(1) = \frac{4G_1'(1)}{(1 - G_1'(1))^2} + \frac{4G_1''(1)}{(1 - G_1'(1))^3}. \tag{B.4}$$

This second moment can diverge in two cases. First, if $G_1'(1) \to 1$, and second $G_1''(1) \to \infty$. When a giant connected component does not exist, $G_1'(1) < 1$, the second moment can still diverge provided that $G_1''(1)$ diverges.

References

[1] R. Albert, A.-L. Barabási, Rev. Mod. Phys. 74 (2002) 47 URL ⟨http://www.nd.edu/∼networks/PDF/rmp.pdf⟩.
[2] B. Bollobás, Random Graphs, second ed., Academic Press, New York, 2001.
[3] C. Cooper, A. Frieze, J. Vera, Random deletion in a scale-free random graph process, Internet Math. 1 (4) (2003) 463–483.
[4] C. Moore, G. Ghoshal, M.E.J. Newman, Phys. Rev. E 74 (2006) 036121.
[5] A.E. Motter, Y.C. Lai, Phys. Rev. E 66 (2002) 065102.
[6] S.N. Dorogovtsev, J.F.F. Mendes, Adv. Phys. 51 (2002) 1079.
[7] S.H.S.D.S. Callaway, M.E.J. Newman, D.J. Watts, Phys. Rev. Lett. 85 (2000) 5468.
[8] H.J.R. Albert, A.-L. Barabási, Nature 378–382 (2000).
[9] A. Broder, R. Kumar, F. Maghoul, P. Raghavan, S. Rajagopalan, R. Stata, A. Tomkins, J. Wiener, Comput. Networks 309 (2000).
[10] D.B.R. Cohen, K. Erez, S. Havlin, Phys. Rev. Lett. 86 (2001) 3682.
[11] S. Dorogovtsev, J.F.F. Mendes, Phys. Rev. Lett. 87 (2001) 219801.
[12] S.-T. Park, A. Khrabrov, D. Pennock, S. Lawrence, C.L. Giles, L. Ungar, in: IEEE Infocom 2003, San Francisco, CA, 2003.
[13] A.-L. Barabási, R. Albert, Science 286 (1999) 509.
[14] N. Sarshar, V. Roychowdhury, Phys. Rev. E 69 (2004) 026101.
[15] C. Gkantsidis, M. Mihail, A. Saberi, SIGMETRICS, 2003.
[16] M. Mihail, C.H. Papadimitriou, A. Saberi, FOCS, 2003.
[17] M.E.J. Newman, S.H. Strogatz, D.J. Watts, Phys. Rev. E 64 (2001) 026118.

[18] W. Aiello, F. Chung, L. Lu, in: Proceedings of the 32nd Annual ACM Symposium on Theory of Computing, ACM Press, New York, 2000, pp. 171–180.
[19] M. Molloy, B. Reed, Random Struct. Algorithms 6 (1995) 161.
[20] S.N. Dorogovtsev, J.F.F. Mendes, Phys. Rev. E 63 (2001) 056125.
[21] N. Sarshar, P.O. Boykin, V. Roychowdhury, in: Proceedings of the Fourth IEEE International Conference on Peer-to-Peer Computing (2004), cond-mat/0406152.