Exploiting the Robustness on Power-Law Networks

Yilin Shen, Nam P. Nguyen, My T. Thai [*]

Department of Computer Information Science and Engineering
University of Florida, Gainesville, FL, 32611
{yshen, nanguyen, mythai}@cise.ufl.edu

Abstract. Many complex networks are discovered to follow the power-law distribution in degree sequence, ranging from the Internet, WWW to social networks. Unfortunately, there exist a great number of threats to these complex systems. In this context, it is crucial to understand the behaviors of power-law networks under various threats. Although power-law networks have been found robust under random failures but vulnerable to intentional attacks by experimental observations, it remains hard to theoretically assess their robustness so as to design a more stable complex network. In this paper, we assess the vulnerability of power-law networks with respect to their global pairwise connectivity, i.e. the number of connected node-pairs, where a pair of nodes are connected when there is a functional path between them. According to our in-depth probabilistic analysis under the theory of random power-law graph model, our results illustrate the best range of exponential factors in which the power-law networks are almost surely unaffected by any random failures and less likely to be destructed under adversarial attacks.

Keywords: Power-Law Networks, Robustness, Probabilistic Analysis

1 Introduction

One of the most remarkable discoveries in complex networks is the power-law distribution in their degree sequences, ranging from the Internet [10], WWW [5] to social networks [17]. That is, the number of nodes of degree i in these complex networks is proportional to $i^{-\beta}$ for some exponential factor β. The property of degree heterogeneity indicates that there are only few nodes with a large number of connections in power-law networks, which are often referred to as 'hub' nodes. Some questions are raised naturally: Are power-law networks more vulnerable to intentional attacks or random failures? If so, can we accurately assess the robustness of power-law networks under various threats, thereby designing more stable power-law networks by controlling a constant parameter β?

There are a great number of studies regarding the tolerance of power-law networks against failures and attacks, in which the authors measured the damage of

[*] This work is partially supported by NSF Career Award ♯ 0953284, DTRA, Young Investigator Award, Basic Research Program ♯ HDTRA1-09-1-0061 and DTRA ♯ HDTRA1-08-10.

attacks in various ways. The most popular measurements include the number of removed edges, average path length or betweenness [12,3], clustering coefficients [14], or degeneration of link latency [13], the available number of compromised $s-t$ flows [1], or vibration of the network [9]. Other researches focus on local nodal centrality, i.e. degree centrality, betweenness centrality or closeness centrality. However, since all these measurements cannot precisely reflect the network fragmentation, they may not reveal the accurate breakdown and damage of the power-law networks although they are usually efficiently computable.

To enhance the assessment accuracy in various real networks, a lot of works emerge mainly based on two measurements, the diameter and the size of the largest component in power-law networks. Albert *et al.* [4] first observed that many power-law networks can tolerate failures to a surprising degree but their survivability decreases rapidly under attacks. That is, the performance of complex systems reduces sharply because of the quick increase of the diameter and the fragmentation in these networks. Holme *et al.* [11] further investigated the degree of harms to power-law networks under different strategies of attacks. Cohen *et al.* [7] showed the resilience of Internet to the random breakdown of the nodes based on percolation theory. In [16], Satorras *et al.* showed that the random uniform immunization of individuals does not lead to the eradication of communications in the whole complex social networks. However, these works did not propose any approaches to investigate an appropriate exponential factor β so as to improve the robustness of power-law networks to the greatest extent.

To this end, our work is the first attempt from a theoretical viewpoint in the literature to assess the impact of random failures and intentional attacks on power-law networks based on a more effective measurement as stated in [8], *global pairwise connectivity.* Compared with the measurements mentioned above and in the survey [14], global pairwise connectivity illustrates more accurate assessment of network robustness to the threats by reflecting functionality between all node-pairs in the network. Thereby, it demonstrates the network fragmentation precisely. According to this measurement, we did an in-depth analysis using probability theory on power-law networks under various failures and attacks and derive two significant conclusions: (1) A complex network can tolerate random attacks if its exponential factor is larger than 2.9; (2) Power-law networks with smaller exponential factor β are more robust under all threats.

The rest of paper is organized as follows. In Section 2, we introduce the random power-law model, the measurement of network vulnerability and failure and attack taxonomy. Some useful results in the literature and fundamental results are presented in Section 3. The analysis of the vulnerability of power-law networks under random failure, preferential attacks and degree-centrality attacks are proposed in Section 4, Section 5 and Section 6 respectively. At last, all main theorems are further visualized in Fig. 1.

2 Models, Measurement and Threat Taxonomy

In this section, we first introduce the power-law random graph (PLRG) model, one of the most well-known models. Then we propose an effective metric —

global pairwise connectivity, to measure the vulnerability of power-law networks under various failures and attacks in the next part. Our analysis throughout the whole paper is based on the PLRG model.

2.1 Power-Law Random Graph Model (PLRG)

Given a network represented by an undirected graph $G = (V, E)$ with $|V| = n$ nodes and $|E| = m$ edges, the graph is referred to as power-law graph $G_{(\alpha,\beta)}$ (PLG) if it follows the important property of complex network, power-law degree distribution. The definition of $G_{(\alpha,\beta)}$ is as follows.

Definition 2.1 ((α,β) Graph $G_{(\alpha,\beta)}$). *A graph $G_{(\alpha,\beta)} = (V, E)$ is called a (α, β) power-law graph where the maximum degree is $\Delta = \lfloor e^{\alpha/\beta} \rfloor$ and the number of nodes of degree i is:*

$$y_i = \begin{cases} \lfloor \frac{e^\alpha}{i^\beta} \rfloor, & \text{if } i > 1 \text{ or } \sum_{i=1}^{\Delta} \lfloor \frac{e^\alpha}{i^\beta} \rfloor \text{ is even} \\ \lfloor e^\alpha \rfloor + 1, & \text{otherwise} \end{cases} \tag{2.1}$$

where the number of nodes n and edges m are almost surely (a.s.) $e^\alpha \zeta(\beta)$ and $e^\alpha \zeta(\beta - 1)$ respectively. Here $\zeta(t) = \sum_{i=1}^{\infty} \frac{1}{i^t}$ is the Riemann Zeta function. *Notice that since $n = e^\alpha \zeta(\beta) + O(n^{\frac{1}{\beta}} - 1)$ and $m = e^\alpha \zeta(\beta - 1) + O(n^{\frac{2}{\beta}} - 1)$, there is only a very small error $o(1)$ when $\beta > 2$. For simplicity, we define $n \doteq e^\alpha \zeta(\beta)$ and $m \doteq e^\alpha \zeta(\beta - 1)$.*

Definition 2.2 (PLRG Model). *Let $\boldsymbol{d} = (d_1, d_2, \ldots, d_n)$ be a sequence of integers corresponding to $(1, \ldots, 1, 2, \ldots, 2, \ldots, \Delta)$ where the number of i is equal to y_i. The PLRG model generates a random graph as follows. Consider $D = \sum_{i=1}^{n} d_i$ mini-nodes lying in n clusters of each size d_i where $1 \leq i \leq n$, we construct a random perfect matching among the mini-nodes and generate a graph on the n original nodes as suggested by this perfect matching in the natural way: two original nodes are connected by an edge if and only if at least one edge in the random perfect matching connects the mini-nodes of their corresponding clusters.*

2.2 Vulnerability Measurements

In order to assess the vulnerability more accurately, we study the global pairwise connectivity $\mathbb{P}$ in residual power-law networks after the failures and attacks, i.e. the number of connected node-pairs. Clearly, there are a.s. no large connected components when $\mathbb{P}$ decreases to some degree. To this end, the fragmentation of the whole network can be accurately assessed by global pairwise connectivity instead of other connectivity measurements [14].

2.3 Threat Taxonomy

Taking most threats into account, we study the vulnerability of power-law networks under uniform random failure and two types of intentional attacks, preferential attack and degree-centrality attack.

Definition 2.3 (Uniform Random Failure). *Each node in $G_{(\alpha,\beta)}$ fails randomly with the same probability.*

Definition 2.4 (Preferential Attack). *Each node in $G_{(\alpha,\beta)}$ is attacked with higher probability if it has a larger degree.*

Definition 2.5 (Degree-Centrality Attack). *The adversary only attacks the set of centrality nodes with maximum degrees in $G_{(\alpha,\beta)}$.*

The residual network of the power-law network $G_{(\alpha,\beta)}$ is defined as G_r, G_p and G_c after the occurrence of uniform random failure, preferential attack and degree-centrality attack. Their corresponding expected degree sequences are denoted as $\boldsymbol{d}_r$, $\boldsymbol{d}_p$ and $\boldsymbol{d}_c$, where the number of d_i^r, d_i^p and d_i^c are referred to as y_i^r, y_i^p and y_i^c.

3 Preliminaries

In this section, we first present some useful results in the literature. Then we derive some fundamental results in power-law networks, which can be used to evaluate the vulnerability of power-law networks in the rest of paper. The following two lemmas illustrate an important relationship between the size of largest connected components and the degree sequence in random networks.

Lemma 3.1 (M. Molloy and B. Reed [15]). *In a random graph G with $\lambda_i n$ nodes of degree i where $\sum_{i=1}^{\Delta} \lambda_i = 1$ with maximum degree Δ, $Q = \sum_{i \geq 1} i(i-2)\lambda_i$ is a metric to decide whether there is giant components in G. The giant components exist if $Q > 0$ and $\Delta < n^{1/4} - \epsilon$. Otherwise, there is a.s. no giant component if $Q < 0$ and $\Delta < n^{1/8} - \epsilon$.*

Lemma 3.2 (F. Chung *et al.* [6]). *The giant component a.s. exists if the expected average degree $\overline{d}$ is at least 1, and there is a.s. no giant component if the expected second-order average degree $\tilde{d}$ is at most 1. Furthermore, all components have volume at most $\sqrt{n}\log n$ with probability at least $1 - o(1)$ if $\tilde{d} < 1$. Here the expected average degree $\overline{d}$ and second-order average degree $\tilde{d}$ are defined as*

$$\overline{d} = \frac{1}{n}\sum_{i=1}^{n} d_i,\ \tilde{d} = \frac{\sum_{i=1}^{n} d_i^2}{\sum_{i=1}^{n} d_i} = \frac{\sum_{i=1}^{n} d_i^2}{2m}$$

where d_i is the elements in the degree sequence.

Note that most results in the paper follow from Lemma 3.2 unless the assessment of network under random attacks since Lemma 3.2 is comparatively stronger than Lemma 3.1. Specially, from Lemma 3.1, we know

$$Q = \sum_{i \geq 1} i(i-2)\lambda_i = C\sum_{i=1}^{n} d_i^2 - 2d_i = C\overline{d}(\tilde{d} - 2)$$

That is, there is a.s. no giant component when $\tilde{d} < 2$ but the size of largest connected component can be a.s. decided only when $\tilde{d} < 1$. Then, we propose our following fundamental results.

Corollary 3.1. *All connected components a.s. have size at most $\frac{1}{2}\sqrt{n}\log n + 1$ if $\tilde{d} < 1$.*

Proof. Consider a connected component containing a subset of nodes S, the volume of S is defined as $Vol(S) = \sum_{v_i \in S} d_i$. Since there are at least $|S|-1$ edges in a connected component of size $|S|$, we have $2(|S|-1) \leq Vol(S) \leq \sqrt{n}\log n$. Therefore, the size of S is upper bounded by $\frac{1}{2}\sqrt{n}\log n + 1$.

Lemma 3.3. *Suppose that the maximum size of connected components in a graph $G = (V, E)$ is ℓ, the pairwise connectivity $\mathbb{P}$ is at most $\frac{n(\ell-1)}{2}$.*

Proof. To prove the upper bound, we consider the worst case that the whole network consists of all connected components of size ℓ except some leftover nodes. Suppose that there are c_1 connect components of size ℓ and the number of leftover nodes is c_2, we have $n = c_1\ell + c_2$. Therefore, the pairwise connectivity $\mathbb{P}$ is

$$\mathbb{P} \leq c_1\binom{\ell}{2} + \binom{c_2}{2} \leq c_1\binom{\ell}{2} + \frac{c_2}{\ell}\binom{\ell}{2} = \frac{c_1\ell + c_2}{\ell}\binom{\ell}{2} = \frac{n(\ell-1)}{2}$$

Theorem 3.1. *In a (α, β) graph $G_{(\alpha,\beta)}$,*

- *If $\beta < 3.47875$, the pairwise connectivity $\mathbb{P}$ is $\Theta(n^2)$;*
- *If $\beta \geq 3.47875$, the range of pairwise connectivity $\mathbb{P}$ is a.s. at most $\frac{1}{2}n\left(c(\beta)n^{\frac{2}{\beta}}\log n - 1\right)$.*

where $c(\beta) = 16/\left[\zeta(\beta)\left(2 - \frac{\zeta(\beta-2)}{\zeta(\beta-1)}\right)\right]^2$ is a constant on any given β.

Proof. When $\beta < 3.47875$, according to Lemma 3.1, since $Q > 0$, there exists one giant component of size $\Theta(n)$. Therefore, the pairwise connectivity $\mathbb{P}$ is $\Theta(n^2)$.

When $\beta \geq 3.47875$, according to Aiello *et al.* [2], a connected component S in the (α, β) graph a.s. has the size at most $c(\beta)n^{\frac{2}{\beta}}\log n$. Then the upper bound of $\mathbb{P}$ follows straightforward from Lemma 3.3.

4 Uniform Random Failures

In this section, we study the global pairwise connectivity $\mathbb{P}$ in G_r, i.e. the residual power-law networks under uniform random failures. In other words, each node has the same probability p to fail. Before proving the main theorem (Theorem 4.1), we show the expected degree distribution in G_r as follows.

Lemma 4.1. *The expected degree distribution of graph G_r is*

$$E(y_i^r) = (1-p)^{i+1}\sum_{k=i}^{\Delta}\binom{k}{i}\frac{e^{\alpha}}{k^{\beta}}p^{k-i}$$

where degree i is $1 \leq i \leq \Delta$.

Proof. Consider some node v of degree k in $G_{(\alpha,\beta)}$: if $k < i$, it is clear that v has probability $p_k = 0$ to become a node of degree i in G_r; if $k \geq i$, v will become a node of of degree i in G_r if and only if v itself does not fail but $k - i$ of its neighbors fail. Hence, the probability p_k that a node v of degree $k \geq i$ in $G_{(\alpha,\beta)}$ becomes a node of degree i in G_r is $\binom{k}{i}(1-p)[p^{k-i}(1-p)^i]$, i.e. $\binom{k}{i}p^{k-i}(1-p)^{i+1}$.

Thus, according to the basic definition of expected value, the expected number of nodes of degree i in G_r is

$$E(y_i^r) = \sum_{k=1}^{\Delta} p_k \frac{e^\alpha}{k^\beta} = (1-p)^{i+1} \sum_{k=i}^{\Delta} \binom{k}{i} \frac{e^\alpha}{k^\beta} p^{k-i}$$

Theorem 4.1 (Main Theorem). *In a residual graph G_r of $G_{(\alpha,\beta)}$ after uniform random failures,*

- *If $\beta < \beta_0$, the expected pairwise connectivity $E(\mathbb{P})$ is a.s. $\Theta(n^2)$;*
- *If $\beta \geq \beta_0$, the range of pairwise connectivity $\mathbb{P}$ is a.s. at most $\frac{1}{2}n\left(c_r(\beta)n^{\frac{2}{\beta}}\log n - 1\right)$.*

where β_0 satisfies that $(1-p)\zeta(\beta_0 - 2) - (2-p)\zeta(\beta_0 - 1) = 0$ and $c_r(\beta) = 16/\left[\zeta(\beta)\left(2 - p - (1-p)\frac{\zeta(\beta-2)}{\zeta(\beta-1)}\right)\right]^2$.

Proof. Consider Lemma 3.2, unfortunately we cannot apply it here since the second-order average degree $\tilde{d} = p + (1-p)\frac{\zeta(\beta-2)}{\zeta(\beta-1)}$ is always larger than 1 for any p and β. Then we use Lemma 3.1 to find a threshold β_0 based on its expected degree distribution and analyze the pairwise connectivity of residual graph G_r in the case of $\beta > \beta_0$ and $\beta < \beta_0$ respectively. To compute β_0, we calculate Q_r in Lemma 3.1 for G_r as follows:

$$\begin{aligned} Q_r &= \sum_{i=1}^{\Delta} i(i-2)(1-p)^{i+1} \sum_{k=i}^{\Delta} \binom{k}{i} \frac{e^\alpha}{k^\beta} p^{k-i} && (4.1) \\ &= e^\alpha (1-p) \sum_{i=1}^{\Delta} \frac{1}{i^\beta} \sum_{j=1}^{i} j(j-2) \binom{i}{j} p^{i-j}(1-p)^j && (4.2) \\ &= e^\alpha (1-p)^2 \sum_{i=1}^{\Delta} \frac{i^2(1-p) - i(2-p)}{i^\beta} && (4.3) \\ &\doteq e^\alpha (1-p)^2 \left[(1-p)\zeta(\beta-2) - (2-p)\zeta(\beta-1)\right] && (4.4) \end{aligned}$$

where step (4.3) follows similarly from the expected value and variance of binomial distribution.

Consider the threshold β_0 satisfies $(1-p)\zeta(\beta-2) - p\zeta(\beta-1) = 0$. When $\beta < \beta_0$, we have $Q_r > 0$. Thus, the expected pairwise connectivity $E(\mathbb{P})$ is a.s. $\Theta(n^2)$ according to Lemma 3.1.

When $\beta \geq \beta_0$, we use the following branching process method (Algorithm 1) according to the expected degree sequence $E(y_i^r)$. E_i and L_i are the set

Algorithm 1: Branching Process Method

```
i ← 0;
E_0 = L_0 = {v} by picking an arbitrary node v;
while |L_i| ≠ 0 do
    i ← i + 1;
    Choose an arbitrary u from L_{i-1} and expose all its neighbors N(u);
    E_i = E_{i-1} ∪ N(u);
    L_i = (L_i \ ({u}) ∪ (N(u) \ E_{i-1});
end
```

of exposed nodes and live nodes in iteration i respectively, where live nodes are referred to as the subset of exposed nodes whose neighbors have not been exposed. Note that $|L_i| = 0$ if and only if the entire component is exposed. For simplicity, we define random variables $\mathcal{E}_i = |E_i|$ and $\mathcal{L}_i = |L_i|$. Let $\mathcal{T}$ denote the whole number of iterations in branching process, that is, $\mathcal{T}$ also measures the size of connected component since exactly one node is exposed in each iteration. We further define an edge to be a "backedge" if it connects u and some node in E_{i-1}. We denote $D_i = |N(u)|$ and $B_i = |N(u) \cap E_{i-1}| - 1$ measuring the degree of the node exposed in iteration i and the number of "backedge". By definition, we have $\mathcal{L}_i - \mathcal{L}_{i-1} = D_i - B_i - 2$.

Then we calculate $E(D_i)$, $E(B_i)$ and $E(\mathcal{L}_i)$ respectively. Consider one edge in original graph G, it still exists if and only if both endpoints are not failed. That is, the expected number of edges $|E_r|$ in G_r is $(1-p)^2|E|$. Therefore,

$$\begin{aligned} E(D_i) &= \sum_{i=1}^{\varDelta} i \frac{i(1-p)^{i+1} \sum_{k=i}^{\varDelta} \binom{k}{i} \frac{e^{\alpha}}{k^{\beta}} p^{k-i}}{(1-p)^2|E|} \\ &= \frac{1}{\zeta(\beta-1)} \sum_{i=1}^{\varDelta} \frac{i^2(1-p)+ip}{i^{\beta}} \doteq (1-p)\frac{\zeta(\beta-2)}{\zeta(\beta-1)} + p \end{aligned}$$

Since $|N(u) \cap E_{i-1}| \geq 1$, we have $E(B_i) \geq 0$. By substituting $E(D_i)$ and $E(B_i)$ into $\mathcal{L}_i - \mathcal{L}_{i-1} = D_i - 2 - B_i$, we have

$$\begin{aligned} E(\mathcal{L}_i) &= \mathcal{L}_1 + \sum_{j=2}^{i} E(\mathcal{L}_j - \mathcal{L}_{j-1}) = d_0 + \sum_{j=2}^{i} E(D_j - B_j - 2) \\ &\leq d_0 + (i-1)\left((1-p)\frac{\zeta(\beta-2)}{\zeta(\beta-1)} + p - 2\right) = d_0 - \lambda(p,\beta)(i-1) \end{aligned}$$

where $\lambda(p,\beta) = 2 - p - (1-p)\frac{\zeta(\beta-2)}{\zeta(\beta-1)}$ and the initial node is supposed to have degree d_0.

Since $|\mathcal{L}_j - \mathcal{L}_{j-1}| \leq \varDelta = e^{\frac{\alpha}{\beta}}$, according to Azuma's martingale inequality,

$$Pr\left[|\mathcal{L}_i - E(\mathcal{L}_i)| > \mathcal{T}\right] \leq 2e^{\frac{-\mathcal{T}^2}{2ie^{\frac{2\alpha}{\beta}}}}$$

where $i = \frac{16}{(\lambda(p,\beta))^2} e^{\frac{2\alpha}{\beta}} \log n = c_r(\beta) n^{\frac{2}{\beta}} \log n$ and $\mathcal{T} = \lambda(p,\beta)i/2$. Since we know

$$E(\mathcal{L}_i) + \mathcal{T} \leq d_0 - \lambda(p,\beta)(i-1) + \frac{\lambda(p,\beta)}{2} i < 0$$

for any d_0. Therefore,

$$Pr\left[\mathcal{T} > \frac{16}{(\lambda(p,\beta))^2} e^{\frac{2\alpha}{\beta}} \log n\right] = Pr[\mathcal{T} > i] \leq Pr[\mathcal{L}_i > 0]$$

$$\leq Pr[\mathcal{L}_i > E(\mathcal{L}_i) + \mathcal{T})] \leq 2e^{\frac{-\mathcal{T}^2}{2ie^{\frac{2\alpha}{\beta}}}} = \frac{2}{n^2}$$

Therefore, the probability that there is an non-failure node v in a connected component of size larger than $c_r(\beta)n^{\frac{2}{\beta}} \log n$ is at most $n\frac{2}{n^2} = o(1)$, i.e. graph G_r has the largest connected component of size a.s. $c_r(\beta)n^{\frac{2}{\beta}} \log n$. Thus, the range of pairwise connectivity in P_r follows from Lemma 3.3 straightforward.

5 Preferential Attacks

In this section, we study the global pairwise connectivity $\mathbb{P}$ in G_p, i.e. the residual power-law networks under preferential attacks. In preferential attacks, each node in the network is attacked with different probability according to its degree. By defining p_i to be the probability of a node of degree i to be attacked, we study the global pairwise connectivity $\mathbb{P}$ of complex network under two following preferential attack schemes: interactive attacks and expected attacks, where their corresponding residual graphs are denoted as G_p^I and G_p^E respectively.

5.1 Interactive Attacks $\left(p_i = 1 - \frac{1}{i^{\beta'}}\right)$

In this scheme, the intruder can attack the network interactively according to their own preferences. By choosing a different parameter β', the network will be attacked in different degrees. Specifically, a node of degree i in $G_{(\alpha,\beta)}$ has probability $1 - \frac{1}{i^{\beta'}}$ to be attacked in this context. It is easy to see that a node of larger degree, often referred to as a "hub", has more probability to be attacked. Before proving the main theorem (Theorem 5.1), we prove the expected degree distribution in G_p^I as follows.

Lemma 5.1. *In graph $G_{(\alpha,\beta)}$, the probability that a node v of degree i incident to another node u of degree x is $\frac{ix}{e^\alpha \zeta(\beta-1)}$.*

Proof. Consider a node v of degree i, in the matching of mini-nodes, at least one of i mini-nodes for v connects to another one of x for node u of degree x. We have

$$\frac{\binom{i}{1}\binom{x}{1} f(N-2)}{f(N)} = \frac{ix}{N-1} = \frac{ix}{N} + O(\frac{1}{N^2}) \doteq \frac{ix}{e^\alpha \zeta(\beta-1)}$$

where $f(n) = (n-1)!!$ representing the number of perfect matchings for N nodes and $N = e^\alpha \zeta(\beta - 1)$ denotes the number of mini-nodes.

Lemma 5.2. *For a node v of degree i, the expected number of non-failure neighbors $E(N_p^I(i))$ of v is $i\frac{\zeta(\beta+\beta'-1)}{\zeta(\beta-1)}$.*

Proof. According to Lemma 5.1, node v has probability $\frac{ix}{e^{\alpha}\zeta(\beta-1)}$ to connect to node u of degree x. Since node u of degree x has the non-failure probability $\frac{1}{x^{\beta'}}$, then we have the expected non-failure neighbor of v to be

$$E(N_p^I(i)) \doteq \sum_{x=1}^{\Delta} \frac{ix}{e^{\alpha}\zeta(\beta-1)} \frac{1}{x^{\beta'}} \frac{e^{\alpha}}{x^{\beta}} \doteq i\frac{\zeta(\beta+\beta'-1)}{\zeta(\beta-1)}$$

Lemma 5.3. *The expected degree distribution of graph G_p^I is*

$$E(y_i^p) \doteq \frac{e^{\alpha}}{\left(i\frac{\zeta(\beta-1)}{\zeta(\beta+\beta'-1)}\right)^{\beta+\beta'}}$$

where $i \in \left\{\frac{\zeta(\beta+\beta'-1)}{\zeta(\beta-1)}, 2\frac{\zeta(\beta+\beta'-1)}{\zeta(\beta-1)}, \ldots, \Delta\frac{\zeta(\beta+\beta'-1)}{\zeta(\beta-1)}\right\}$.

Proof. Consider the set of nodes of degree i in G_p, they are correspondent to the nodes of degree x in the original graph. Hence, the expected unattacked nodes in this set is $\frac{e^{\alpha}}{x^{\beta}}\frac{1}{x^{\beta'}} = \frac{e^{\alpha}}{x^{\beta+\beta'}}$. From Lemma 5.4, we know the relation between i and x is $i \doteq x\frac{\zeta(\beta+\beta'-1)}{\zeta(\beta-1)}$. Therefore, we have the expected number of nodes of degree i in G_p^I to be $\frac{e^{\alpha}}{\left(i\frac{\zeta(\beta-1)}{\zeta(\beta+\beta'-1)}\right)^{\beta+\beta'}}$.

Theorem 5.1 (Main Theorem). *In a residual graph G_p^I of $G_{(\alpha,\beta)}$ after interactive preferential attacks,*

- *If $\beta+\beta' < 3.47875$, the expected pairwise connectivity $E(\mathbb{P})$ is $\Theta(n^2)$;*
- *If $\beta+\beta' \geq 3.47875$, the range of pairwise connectivity $\mathbb{P}$ is a.s. at most $\frac{1}{2}n\left(c(\beta)n^{\frac{2}{\beta}}\log n - 1\right)$.*

where $c(\beta) = 16/\left[\zeta(\beta)\left(2-\frac{\zeta(\beta-2)}{\zeta(\beta-1)}\right)\right]^2$ is a constant on any given β.

Proof. The proof follows the same as Theorem 3.1.

5.2 Expected Attacks $\left(p_i = c\frac{i}{e^{\alpha}\zeta(\beta-1)}\right)$

In expected attacks, the intruders are usually interested in investigating the size of expected number of nodes to attack such that the network can be almost surely fragmented. To this end, we consider that the probability of each node to be attacked is proportional to its degree, i.e. a node of degree i is attacked with probability $p_i = c\frac{i}{e^{\alpha}\zeta(\beta-1)}$, in which the expected failure nodes is equal to c since $\sum_i \frac{e^{\alpha}}{i^{\beta}}p_i = c$.

Lemma 5.4. *For a node v of degree i, the expected number of non-failure neighbors $E(N_p^E(i))$ of v is $i\left(1-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right)$.*

Proof. According to Lemma 5.1, node v has probability $\frac{ix}{e^{\alpha}\zeta(\beta-1)}$ to connect to node u of degree x. Since node u of degree x has the non-failure probability $1-c\frac{x}{e^{\alpha}\zeta(\beta-1)}$, then we have the expected non-failure neighbor of v to be

$$E(N_p(i)) \doteq \sum_{x=1}^{\mathit{\Delta}} \frac{ix}{e^{\alpha}\zeta(\beta-1)}\left(1-\frac{cx}{e^{\alpha}\zeta(\beta-1)}\right)\frac{e^{\alpha}}{x^{\beta}} \doteq i\left(1-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right)$$

Lemma 5.5. *The expected degree distribution of graph G_p^E is*

$$E(y_i^p) \doteq \frac{e^{\alpha}}{i^{\beta}}\left(1-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right)^{\beta}\left(1-\frac{ci}{(e^{\alpha}\zeta(\beta-1))\left(1-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right)}\right)$$

where $i \in \left\{\left(1-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right), 2\left(1-\frac{\zeta(c\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right), \ldots, \mathit{\Delta}\left(1-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right)\right\}$.

Proof. The proof follows similarly as the proof in Lemma 5.3.

Theorem 5.2 (Main Theorem). *In a residual graph G_p^E of $G_{(\alpha,\beta)}$ after expected preferential attacks,*

- *The pairwise connectivity $\mathbb{P}$ is a.s. $\Theta(n^2)$*
  if $c < \min\left\{c \middle| \frac{\sum_{x=1}^{\mathit{\Delta}} \frac{e^{\alpha}}{x^{\beta}}\left(1-\frac{cx}{e^{\alpha}\zeta(\beta-1)}\right)\left(x\left(1-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right)\right)}{n-c} > 1\right\}$;
- *The pairwise connectivity $\mathbb{P}$ is a.s. at most $\frac{1}{4}n^{\frac{3}{2}}\log n$*
  if $c > \max\left\{c \middle| \left(1-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right)\frac{\zeta(\beta-2)-\frac{c\zeta(\beta-3)}{e^{\alpha}\zeta(\beta-1)}}{\zeta(\beta-1)-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)}} < 1\right\}$.

Proof. In the proof, we first calculate the expected average degree $\overline{y}_p^E$ as

$$\overline{y}_p^E \doteq \frac{\sum_{x=1}^{\mathit{\Delta}} \frac{e^{\alpha}}{x^{\beta}}\left(1-\frac{cx}{e^{\alpha}\zeta(\beta-1)}\right)\left(x\left(1-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right)\right)}{n-c}$$

and second-order average degree $\tilde{y}_p^E$ as

$$\begin{aligned}\tilde{y}_p^E &\doteq \frac{\sum_{x=1}^{\mathit{\Delta}} \frac{e^{\alpha}}{x^{\beta}}\left(1-\frac{cx}{e^{\alpha}\zeta(\beta-1)}\right)\left(x\left(1-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right)\right)^2}{\sum_{x=1}^{\mathit{\Delta}} \frac{e^{\alpha}}{x^{\beta}}\left(1-\frac{cx}{e^{\alpha}\zeta(\beta-1)}\right)\left(x\left(1-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right)\right)}\\ &\doteq \left(1-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)^2}\right)\frac{\zeta(\beta-2)-\frac{c\zeta(\beta-3)}{e^{\alpha}\zeta(\beta-1)}}{\zeta(\beta-1)-\frac{c\zeta(\beta-2)}{e^{\alpha}\zeta(\beta-1)}}\end{aligned}$$

According to Lemma 3.2 and Corollary 3.1, there exists one giant component if $\overline{y}_p^E > 1$ and all components have size at most $\frac{1}{2}\sqrt{n}\log n + 1$ if $\tilde{y}_p^E < 1$, the proof follows from Lemma 3.3.

6 Degree-Centrality Attacks

Unlike the above random threats, in degree-centrality attack, the intruders intentional attack the "hubs", that is, the set of nodes with highest degrees. Suppose that all nodes of degree larger than x_0 are attacked simultaneously, we have the following results.

Lemma 6.1. *For a node v of degree i in original graph $G_{(\alpha,\beta)}$, the expected number of neighbors of degree larger than x_0 is $\frac{i}{\zeta(\beta-1)}\sum_{i=x_0+1}^{\Delta}\frac{1}{i^{\beta-1}}$.*

Proof. According to Lemma 5.4, the probability that a node v of degree i incident to a node u of degree x is $\frac{ix}{e^{\alpha}\zeta(\beta-1)}$. Therefore, we have the expected number of neighbors of degree larger than x_0 to be

$$E(N_c(i)) \doteq \sum_{x=x_0+1}^{\Delta}\frac{ix}{e^{\alpha}\zeta(\beta-1)}\frac{e^{\alpha}}{x^{\beta}} = \frac{i}{\zeta(\beta-1)}\sum_{x=x_0+1}^{\Delta}\frac{1}{x^{\beta-1}}$$

Lemma 6.2. *The expected degree sequence in G_c is*

$$E(y_i^c) \doteq \frac{e^{\alpha}}{i^{\beta}}\left(\frac{1}{\zeta(\beta-1)}\sum_{x=1}^{x_0}\frac{1}{x^{\beta-1}}\right)^{\beta}$$

where $i \in \left\{\left(\frac{1}{\zeta(\beta-1)}\sum_{x=1}^{x_0}\frac{1}{x^{\beta-1}}\right), 2\left(\frac{1}{\zeta(\beta-1)}\sum_{x=1}^{x_0}\frac{1}{x^{\beta-1}}\right), \ldots, x_0\left(\frac{1}{\zeta(\beta-1)}\sum_{x=1}^{x_0}\frac{1}{x^{\beta-1}}\right)\right\}$.

Theorem 6.1 (Main Theorem). *In a residual graph G_c of $G_{(\alpha,\beta)}$ after degree-centrality attacks,*

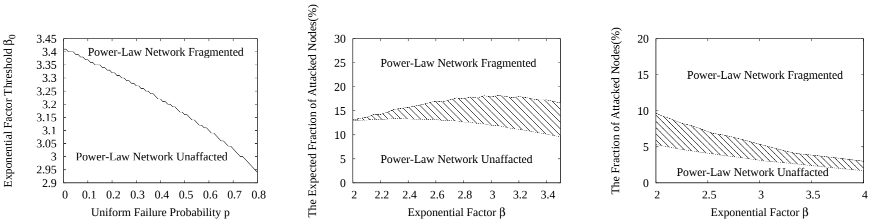
- *The pairwise connectivity $\mathbb{P}$ is a.s. $\Theta(n^2)$ if $x_0 > \min\left\{x_0\middle|\frac{1}{\zeta(\beta-1)}\frac{\left(\sum_{x=1}^{x_0}\frac{1}{x^{\beta-1}}\right)^2}{\sum_{x=1}^{x_0}\frac{1}{x^{\beta}}} > 1\right\}$;*
- *The pairwise connectivity $\mathbb{P}$ is a.s. at most $\frac{1}{4}n^{\frac{3}{2}}\log n$ if $x_0 < \max\left\{x_0\middle|\frac{1}{\zeta(\beta-1)}\sum_{x=1}^{x_0}\frac{1}{x^{\beta-2}} < 1\right\}$.*

The proof of Lemma 6.2 and Theorem 6.1 follows from Lemma 6.1 and the proof of Theorem 5.2 respectively.

Discussion: Fig. 1 visualizes the above results for main theorems correspondent to the vulnerability of power-law networks under various threats.

References

1. Modeling s-t path availability to support disaster vulnerability assessment of network infrastructure. *Computers & Operations Research*, 36(1):16 – 26, 2009.
2. W. Aiello, F. Chung, and L. Lu. A random graph model for power law graphs. *Experimental Math*, 10:53–66, 2000.
3. R. Albert, I. Albert, and G. L. Nakarado. Structural vulnerability of the north american power grid. *Phys. Rev. E*, 69(2):025103, Feb 2004.



(a) UR Failures (b) EP Attacks (c) DC Attacks

Fig. 1. The Visualization of Exponential Factor β under various Failures and Attacks: In uniform random (UR) failures, Fig. 1(a) illustrates the relationship between threshold β_0 and failure probability p as stated in Theorem 4.1. Power-law networks of exponential factor $\beta > 2.9$ are shown to be unaffected under UR failures even though each node fails with unrealistic probability 0.8. With respect to adversarial attacks, Fig. 1(b) and Fig. 1(c) associate the exponential factor β with the expected fraction of attacked nodes under expected preferential (EP) attacks and under degree-centrality (DC) attacks according to Theorem 5.2 and 6.1. The power-law network of $\beta = 2$ survives when less than 13% expected fraction of nodes are attacked in EP attacks and less 5% fraction of nodes are attacked in DC attacks. (Note that the shadow area in these two figures are the uncertain area, i.e. power-law networks may be either unaffected or fragmented, which should be avoided.)

4. R. Albert, H. Jeong, and A. Barabasi. Error and attack tolerance of complex networks. *Nature*, 406(6794):378–382, July 2000.
5. R. Albert, H. Jeong, and A. L. Barabasi. The diameter of the world wide web. *Nature*, 401:130–131, 1999.
6. F. Chung and L. Lu. Connected components in random graphs with given expected degree sequences. *ANNALS OF COMBINATORICS*, pages 125–145.
7. R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin. Resilience of the Internet to Random Breakdowns. *Physical Review Letters*, 85(21):4626+, November 2000.
8. T. N. Dinh, Y. Xuan, M. T. Thai, E. K. Park, and T. Znati. On approximation of new optimization methods for assessing network vulnerability. In *INFOCOM*, pages 2678–2686, 2010.
9. E. Estrada and N. Hatano. A vibrational approach to node centrality and vulnerability in complex networks. *Physica A: Statistical Mechanics and its Applications*, 389(17):3648 – 3660, 2010.
10. M. Faloutsos, P. Faloutsos, and C. Faloutsos. On power-law relationships of the internet topology. In *Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication*, SIGCOMM '99, pages 251–262, New York, NY, USA, 1999. ACM.
11. P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han. Attack vulnerability of complex networks. *Phys. Rev. E*, 65(5):056109, May 2002.
12. M. Kaiser and C. C. Hilgetag. Edge vulnerability in neural and metabolic networks. *Biological Cybernetics*, 90:311–317, 2004. 10.1007/s00422-004-0479-1.
13. V. Latora and M. Marchiori. Vulnerability and protection of infrastructure networks. *Phys. Rev. E*, 71(1):015103, Jan 2005.
14. Luciano, F. Rodrigues, G. Travieso, and V. P. R. Boas. *Advances in Physics*.
15. M. Molloy and B. Reed. A critical point for random graphs with a given degree sequence. *Random Struct. Algorithms*, 6:161–179, March 1995.
16. R. P. Satorras and A. Vespignani. Immunization of complex networks. *Phys. Rev. E*, 65(3):036104, Feb 2002.
17. S. Redner. How popular is your paper? An empirical study of the citation distribution. *The European Physical Journal B - Condensed Matter and Complex Systems*, 4(2):131–134, August 1998.