Network Science

Class 8: Network Robustness

Albert-László Barabási

with

Emma K. Towlson, Sebastian Ruf, Michael Danziger, and Louis Shekhtman

www.BarabasiLab.com

Questions 1

1. Percolation theory basics. The forest fire example.
2. Inverse percolation and network robustness.
3. Scale-free network robustness and Molloy-Reed criteria.
4. Critical Threshold in infinite networks
5. Critical Threshold in finite networks
6. Critical Threshold under attacks
7. Cascading failures: examples and empirical results
8. Modeling cascading failures: Failure Propagation model
9. Modeling cascading failures: Branching model
10. Building robustness and halting cascading failures.

Introduction

robust |rōˈbəst, ˈrōˌbəst| adjective

(robuster, robustest) strong and healthy; vigorous: the Caplans are a robust, healthy lot.

- (of an object) sturdy in construction: a robust metal cabinet.
- (of a process, system, organization, etc.) able to withstand or overcome adverse conditions: California's robust property market.

Robustness, means “oak” in latin, being the symbol of strength and longevity in the ancient world.

ROBUSTNESS IN COMPLEX SYSTEMS

Complex systems maintain their basic functions even under errors and failures

Cell → mutations

There are uncountable number of mutations and other errors in our cells, yet, we do not notice their consequences.

Internet → router breakdowns

At any moment hundreds of routers on the internet are broken, yet, the internet as a whole does not loose its functionality.

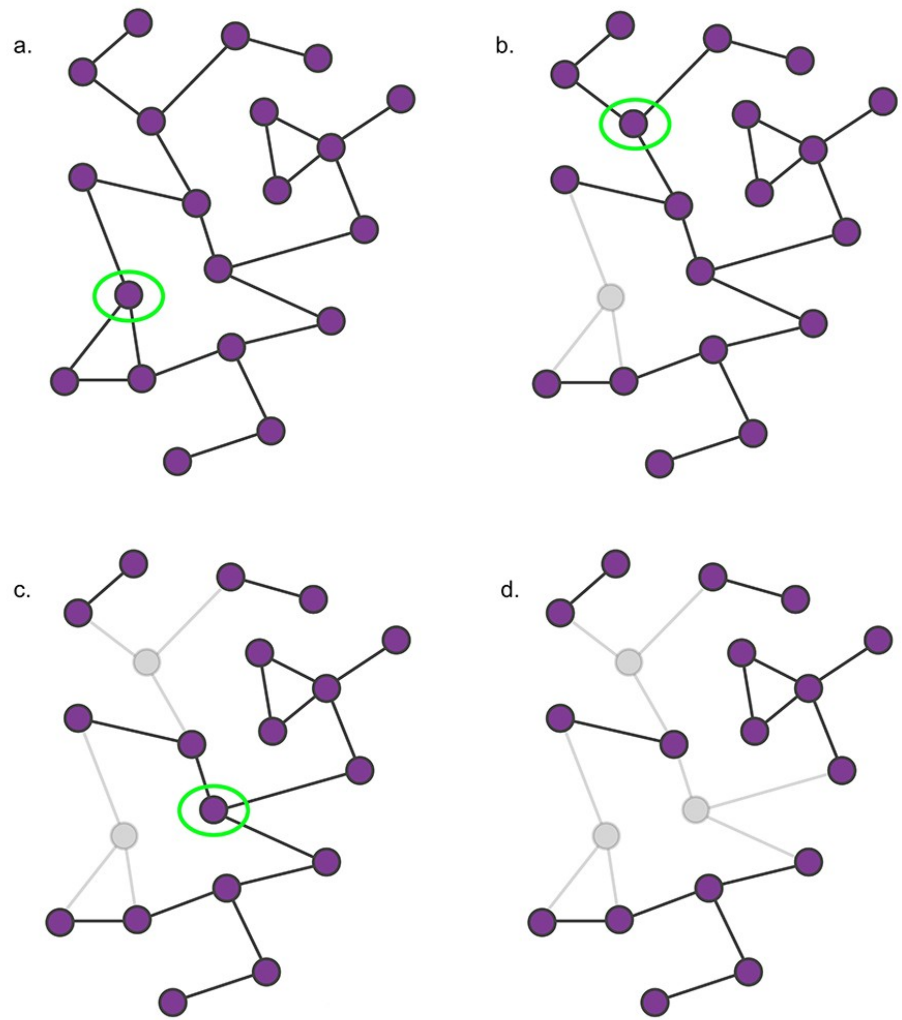
Where does robustness come from?

There are feedback loops in most complex systems that keep tab on the component's and the system's 'health'.

Could the network structure affect a system's robustness?

Percolation Theory

ROBUSTNESS



Cluster size, <s>: average size of all finite clusters for a given p

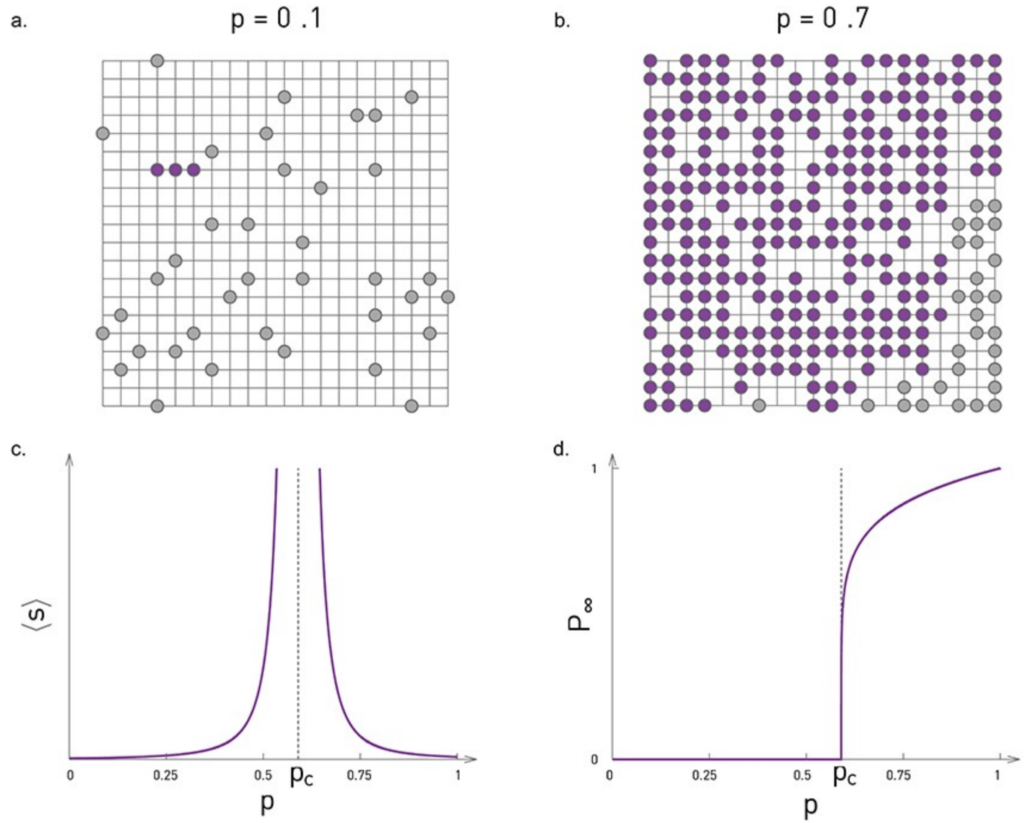
$$\langle s \rangle \sim |p - p_c|^{-\gamma}$$

Order parameter, P_∞: probability that a peeble belongs to the largest cluster.

$$P_\infty \sim (p - p_c)^{\beta}$$

Correlation length: mean distance between two sites on the same cluster.

$$\zeta \sim |p - p_c|^{-\nu}$$

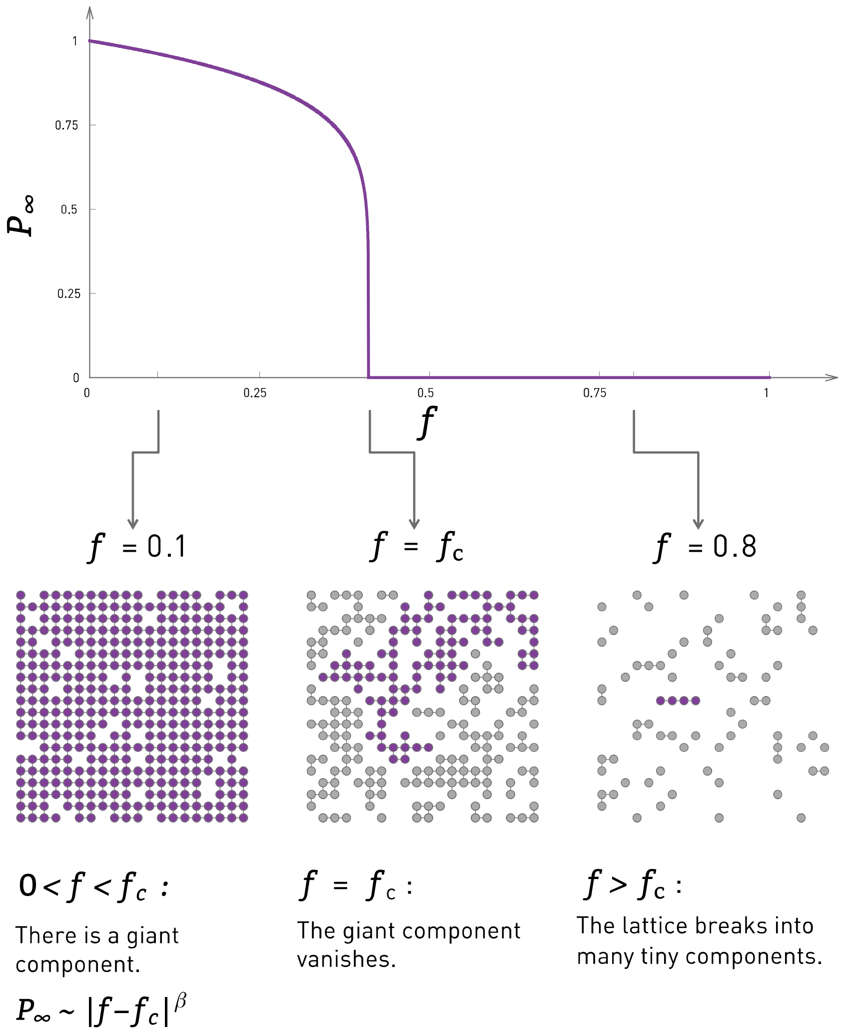


- The value of p_c depends on the lattice type, hence it is not universal. For example, for a two-dimensional square lattice (Figure 8.4) we have $p_c \approx 0.593$, while for a two-dimensional triangular lattice $p_c = 1/2$ (site percolation).

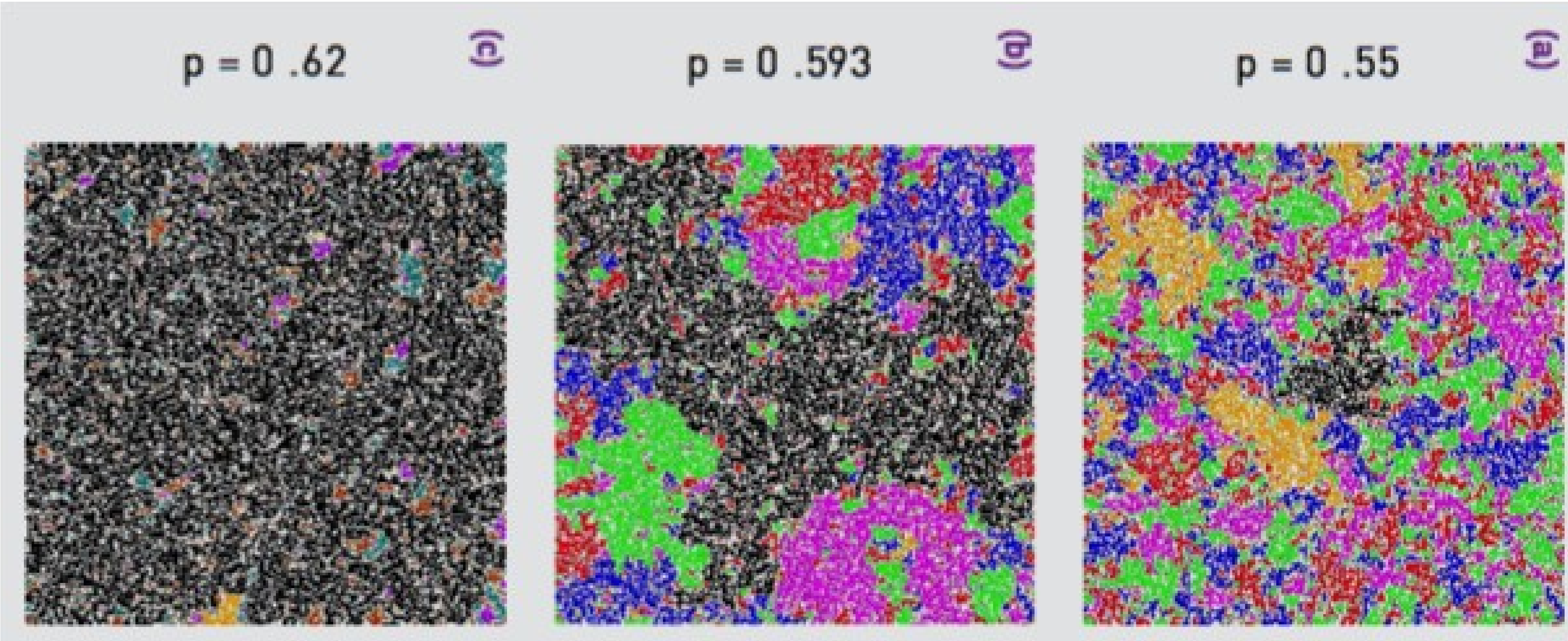
- The value of p_c also changes with the lattice dimension: for a square lattice $p_c \approx 0.593$ ($d = 2$); for a simple cubic lattice ($d = 3$) $p_c \approx 0.3116$. Therefore in $d = 3$ we need to cover a smaller fraction of the nodes with pebbles to reach the percolation transition.

- In contrast with p_c, the critical exponents do not depend on the lattice type, but only on the lattice dimension. In two dimensions, the case shown in Figure 8.4, we have $\gamma_p = 43/18$, $\beta_c = 5/36$, and $\nu = 4/3$, for any lattice. In three dimensions $\gamma_p = 1.80$, $\beta_c = 0.41$, and $\nu = 0.88$. For any $d > 6$ we have $\gamma_p = 1$, $\beta_c = 1$, $\nu = 1/2$, hence for large d the exponents are independent of d as well [2].

Section 8.2 Network Breakdown: Inverse percolation



What, however, if the underlying network is not as regular as a square lattice? As we will see in the coming sections, the answer depends on the precise network topology. Yet, for random networks the answer continues to be provided by percolation theory: Random networks under random node failures share the same scaling exponents as infinite-dimensional percolation. Hence the critical exponents for a random network are $\gamma_p = 1$, $\beta_c = 1$ and $\nu = 1$, corresponding to the $d > 6$ percolation exponents encountered earlier. The critical exponents for a scale-free network are provided in ADVANCED TOPICS 8.A.


p = 0 .62
p = 0 .593
p = 0 .55

Robustness of scale-free networks

ROBUSTNESS OF SCALE-FREE NETWORKS

The interest in the robustness problem has three origins:

→Robustness of complex systems is an important problem in many areas

→Many real networks are not regular, but have a scale-free topology

→*In scale-free networks the scenario described above is not valid*

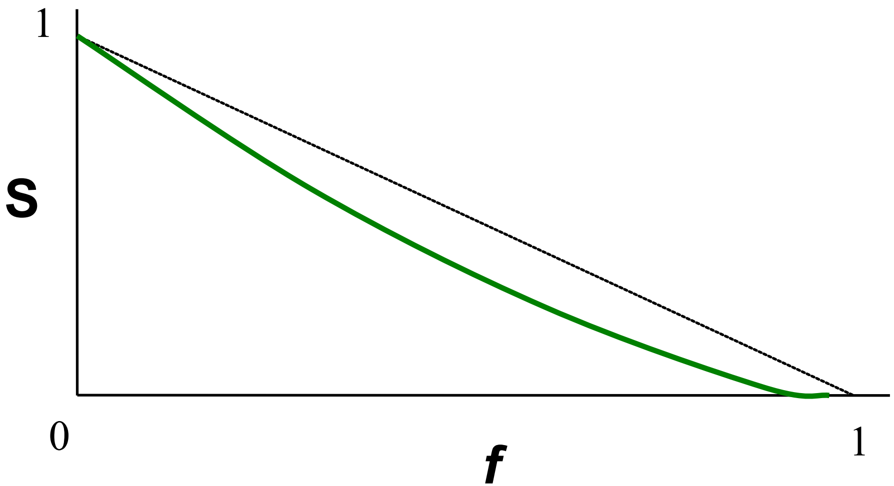
Albert, Jeong, Barabási, *Nature* **406** 378 (2000)

ROBUSTNESS OF SCALE-FREE NETWORKS

Scale-free networks do not appear to break apart under random failures.

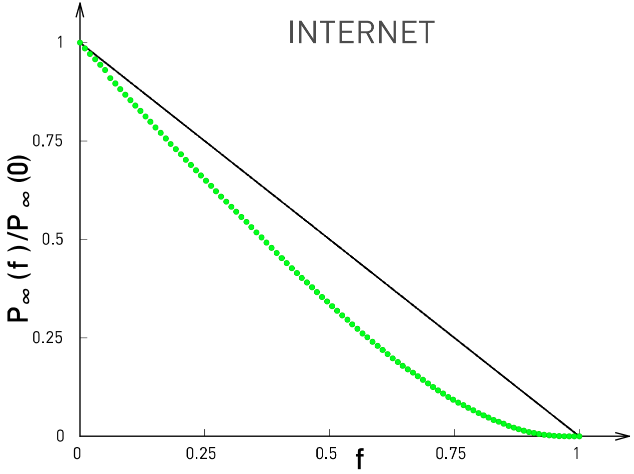
Reason: the hubs.

The likelihood of removing a hub is small.

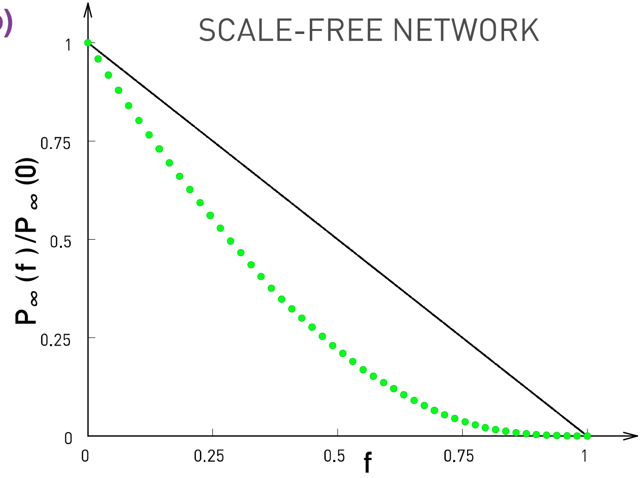


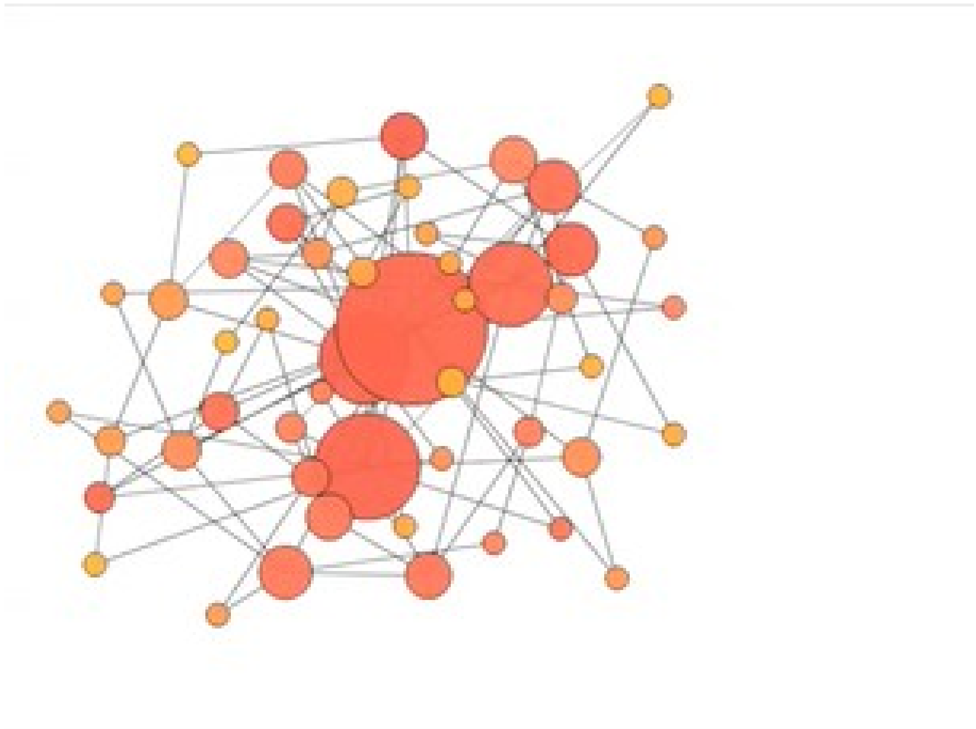
Albert, Jeong, Barabási, *Nature* **406** 378 (2000)

(a)


INTERNET
$P_\infty(f)/P_\infty(0)$
1
0.75
0.5
0.25
0
0
0.25
0.5
f
0.75
1

(b)

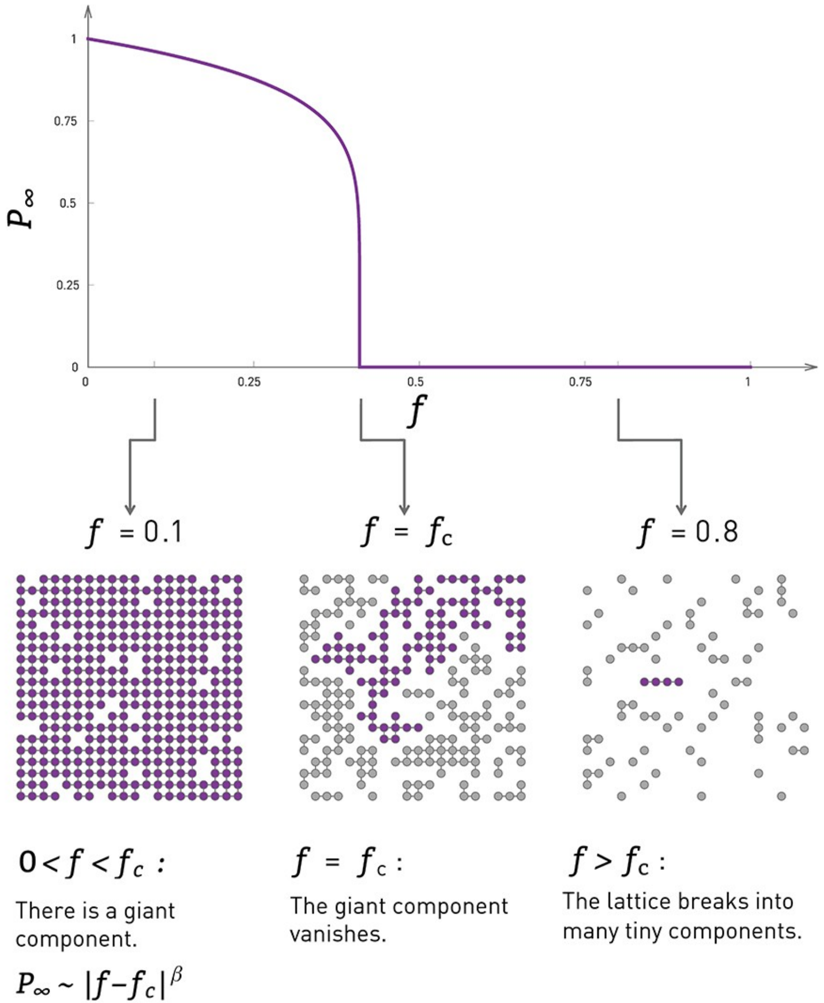

SCALE-FREE NETWORK
$P_\infty(f)/P_\infty(0)$
1
0.75
0.5
0.25
0
0
0.25
0.5
f
0.75
1



What is the value of f_c?

Molloy-Reed criteria:

$$\kappa \equiv \frac{\langle k^2 \rangle}{\langle k \rangle} = 2$$



[6]. For a giant component to exist each node that belongs to it must be connected to at least two other nodes on average (Figure 8.8). Therefore, the average degree k_i of a randomly chosen node i that is part of the giant component should be at least 2. Denote with $P(k_i \mid i \leftrightarrow j)$ the joint probability that a node in a network with degree k_i is connected to a node j that is part of the giant component. This conditional probability allows us to determine the expected degree of node i as

$$\langle k_i \mid i \leftrightarrow j \rangle = \sum_{k_i} k_i P(k_i \mid i \leftrightarrow j) = 2 \, . \tag{8.26}$$

$$\langle k_i \mid i \leftrightarrow j \rangle = \sum_{k_i} k_i P(k_i \mid i \leftrightarrow j) = 2 \,. \tag{8.26}$$

In other words, $\langle k_i \mid i \leftrightarrow j \rangle$ should be equal or exceed two, the condition for node i to be part of the giant component. We can write the probability appearing in the sum (8.26) as

$$P(k_i \mid i \leftrightarrow j) = \frac{P(k_i, i \leftrightarrow j)}{P(i \leftrightarrow j)} = \frac{P(i \leftrightarrow j \mid k_i) p(k_i)}{P(i \leftrightarrow j)} \,, \tag{8.27}$$

where we used Bayes' theorem in the last term. For a network with degree distribution p_k, in the absence of degree correlations, we can write

$$P(i \leftrightarrow j) = \frac{2L}{N(N-1)} = \frac{\langle k \rangle}{N-1} \,, \qquad P(i \leftrightarrow j \mid k_i) = \frac{k_i}{N-1} \,, \tag{8.28}$$

which express the fact that we can choose between $N - 1$ nodes to link to, each with probability $1/(N - 1)$ and that we can try this k_i times. We can now return to (8.26), obtaining

$$\sum_{k_i} k_i P(k_i \mid i \leftrightarrow j) = \sum_{k_i} k_i \frac{P(i \leftrightarrow j \mid k_i) p(k_i)}{P(i \leftrightarrow j)} = \sum_{k_i} k_i \frac{k_i p(k_i)}{\langle k \rangle} = \frac{\sum_{k_i} k_i^2 p(k_i)}{\langle k \rangle} \tag{8.29}$$

With that we arrive at the Molloy-Reed criterion (8.4), providing the condition to have a giant component as

$$\kappa \equiv \frac{\langle k^2 \rangle}{\langle k \rangle} > 2 \,. \tag{8.30}$$

Molloy-Reed criteria:

$$\kappa \equiv \frac{\langle k^2 \rangle}{\langle k \rangle} = 2$$

Networks with $\kappa < 2$ lack a giant component, being fragmented into many disconnected components. The Molloy-Reed criterion (8.4) links the network's integrity, as expressed by the presence or the absence of a giant component, to $\langle k \rangle$ and $\langle k^2 \rangle$. It is valid for any degree distribution p_k.

Erdos-Renyi network:

$$\langle k^2 \rangle = \langle k \rangle (1 + \langle k \rangle)$$

$$\kappa \equiv \frac{\langle k^2 \rangle}{\langle k \rangle} = \frac{\langle k \rangle (1 + \langle k \rangle)}{\langle k \rangle} = 1 + \langle k \rangle = 2$$

$$\langle k \rangle > 1$$

Critical Threshold for arbitrary P(K)

Robustness: we remove a fraction *f* of the nodes.

At what threshold f_c will the network fall apart (no giant component)?

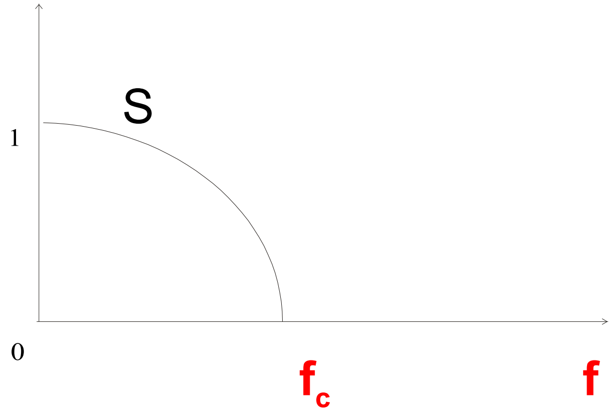
Random node removal changes

the degree of individuals nodes [k → k' ≤k)

the degree distribution [P(k) → P'(k')]

Breakdown threshold:

$$f_c = 1 - \frac{1}{\frac{\langle k^2 \rangle}{\langle k \rangle} - 1}$$



$f<f_c$: the network is still connected (there is a giant cluster)

$f>f_c$: the network becomes disconnected (giant cluster vanishes)

Cohen et al., Phys. Rev. Lett. 85, 4626 (2000).

BREAKDOWN THRESHOLD FOR ARBITRARY P(k)

Problem: What are the consequences of removing a fraction *f* of all nodes?

At what threshold f_c will the network fall apart (no giant component)?

Random node removal changes

the degree of individual nodes [k → k' ≤k]

the degree distribution [P(k) → P'(k')]

A node with degree *k* will loose some links and become a node with degree *k'* with probability:

$$\binom{k}{k'} f^{k-k'} (1-f)^{k'} \qquad k' \leq k$$

Remove k-k' links, each with probability f

Leave k' links untouched, each with probability 1-f

The prob. that we had a *k* degree node was *P(k)*, so the probability that we will have a new node with degree *k'* :

$$P'(k') = \sum_{k=k'}^{\infty} P(k) \binom{k}{k'} f^{k-k'} (1-f)^{k'}$$

Let us asume that we know <k> and <k^2> for the original degree distribution P(k)
→ calculate <k'> , <k'^{2}> for the new degree distribution P'(k').

Cohen et al., Phys. Rev. Lett. 85, 4626 (2000).

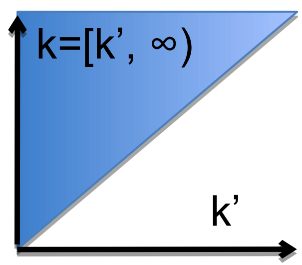
BREAKDOWN THRESHOLD FOR ARBITRARY P(K)

$$P'(k') = \sum_{k=k'}^{\infty} P(k) \binom{k}{k'} f^{k-k'} (1-f)^{k'}$$

Degree distribution after we removed *f* fraction of nodes.

$$< k' >_f = \sum_{k'=0}^{\infty} k' P'(k') = \sum_{k'=0}^{\infty} k' \sum_{k=k'}^{\infty} P(k) \frac{k!}{k'!(k-k')!} f^{k-k'} (1-f)^{k'} = \sum_{k'=0}^{\infty} \sum_{k=k'}^{\infty} P(k) \frac{k(k-1)!}{(k'-1)!(k-k')!} f^{k-k'} (1-f)^{k'-1} (1-f)$$

The sum is done over the triangel shown in the right, so we can replace it with



$$\sum_{k'=0}^{\infty} \sum_{k=k'}^{\infty} = \sum_{k=0}^{\infty} \sum_{k'=0}^{k}$$

$$< k' >_f = \sum_{k'=0}^{\infty} \sum_{k=k'}^{\infty} P(k) \frac{k(k-1)!}{(k'-1)!(k-k')!} f^{k-k'} (1-f)^{k'-1} (1-f) = \sum_{k=0}^{\infty} (1-f) k P(k) \sum_{k'=0}^{k} \frac{(k-1)!}{(k'-1)!(k-k')!} f^{k-k'} (1-f)^{k'-1} =$$

$$\sum_{k'=0}^{k} \sum_{k=0}^{\infty} (1-f) k P(k) \sum_{k'=0}^{k} \binom{k-1}{k'-1} f^{k-k'} (1-f)^{k'-1} = \sum_{k=0}^{\infty} (1-f) k P(k) = \boxed{(1-f) < k >}$$

Cohen et al., Phys. Rev. Lett. 85, 4626 (2000).

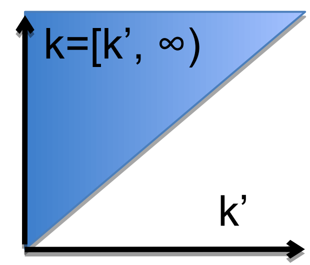
BREAKDOWN THRESHOLD FOR ARBITRARY P(K)

$$P'(k') = \sum_{k=k'}^{\infty} P(k) \binom{k}{k'} f^{k-k'} (1-f)^{k'}$$

Degree distribution after we removed f fraction of nodes.

$$< k'^2 >_f = < k'(k'-1) - k' >_f = \sum_{k'=0}^{\infty} k'(k'-1) P'(k') - < k' >_f$$

The sum is done over the triangel shown in the right, i.e. we can replace it with



$$\sum_{k'=0}^{\infty} \sum_{k=k'}^{\infty} = \sum_{k=0}^{\infty} \sum_{k'=0}^{k}$$

$$< k'(1-k') >_f = \sum_{k'=0}^{\infty} \sum_{k=k'}^{\infty} P(k) \frac{k(k-1)(k-2)!}{(k'-2)!(k-k')!} f^{k-k'} (1-f)^{k-2'} (1-f)^2 = \sum_{k=0}^{\infty} (1-f)^2 k(k-1) P(k) \sum_{k'=0}^{k} \frac{(k-2)!}{(k'-2)!(k-k')!} f^{k-k'} (1-f)^{k'-2} =$$

$$\sum_{k'=0}^{k} \sum_{k=0}^{\infty} (1-f)^2 k(k-1) P(k) \sum_{k'=0}^{k} \binom{k-2}{k'-2} f^{k-k'} (1-f)^{k'-2} = \sum_{k=0}^{\infty} (1-f)^2 k(k-1) P(k) = (1-f)^2 < k(k-1) >$$

$$< k'^2 >_f = < k'(k'-1) - k' >_f = (1-f)^2 (< k^2 > - < k >) - (1-f) < k > = (1-f)^2 < k^2 > + f(1-f) < k >$$

Cohen et al., Phys. Rev. Lett. 85, 4626 (2000).

BREAKDOWN THRESHOLD FOR ARBITRARY P(K)

Robustness: we remove a fraction *f* of the nodes.

At what threshold f_c will the network fall apart (no giant component)?

Random node removal changes

the degree of individual nodes [k → k' ≤k)

the degree distribution [P(k) → P'(k')]

$$< k' >_f = (1-f) < k >$$

$$< k'^2 >_f = (1-f)^2 < k^2 > + f(1-f) < k >$$

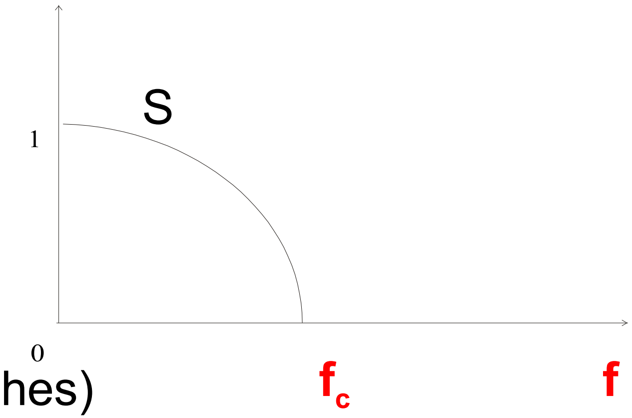
$$\kappa \equiv \frac{< k'^2 >_f}{< k' >_f} = 2$$

$\kappa>2$: a giant cluster exists

$\kappa<2$: many disconnected clusters

Breakdown threshold:

$$f_c = 1 - \frac{1}{\frac{\langle k^2 \rangle}{\langle k \rangle} - 1}$$



$f<f_c$: the network is still connected (there is a giant cluster)

$f>f_c$: the network becomes disconnected (giant cluster vanishes)

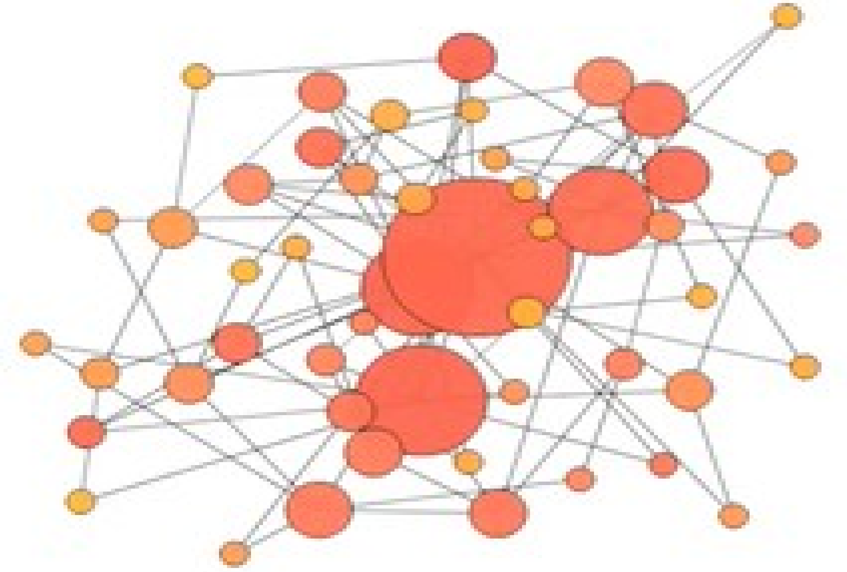
Cohen et al., Phys. Rev. Lett. 85, 4626 (2000).

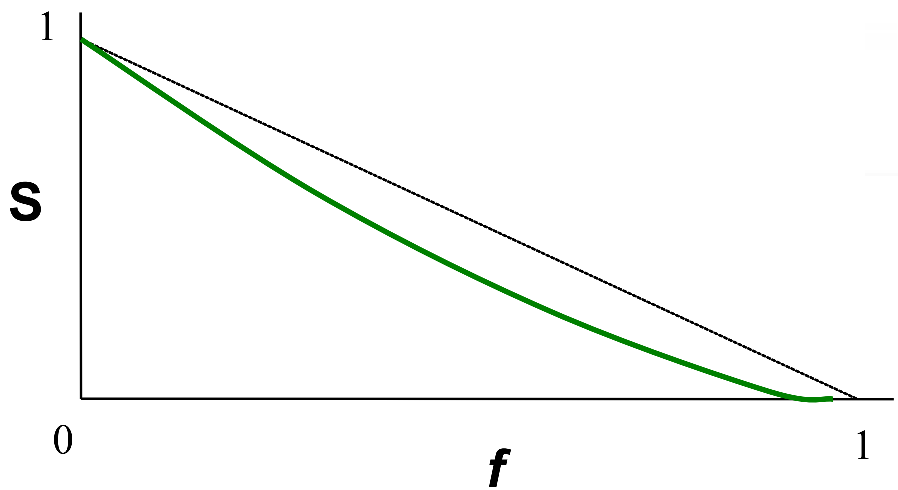
ROBUSTNESS OF SCALE-FREE NETWORKS

Scale-free networks do not appear to break apart under random failures.

Reason: the hubs.

The likelihood of removing a hub is small.





Albert, Jeong, Barabási, *Nature* **406** 378 (2000)

ROBUSTNESS OF SCALE-FREE NETWORKS

$$f_c = 1 - \frac{1}{\kappa - 1}$$

$$\kappa = \frac{<k^2>}{<k>} = \left|\frac{2-\gamma}{3-\gamma}\right| \begin{cases} K_{min} & \gamma > 3 \\ K_{max}{}^{3-\gamma} K_{min}^{\gamma-2} & 3 > \gamma > 2 \\ K_{max} & 2 > \gamma > 1 \end{cases}$$

$$K_{max} = K_{min} N^{\frac{1}{\gamma-1}}$$

γ>3: κ is finite, so the network will break apart at a finite f_c that depens on K_{min}

γ<3: κ diverges in the N→ ∞ limit, so f_c → 1 !!!

for an infinite system one needs to remove all the nodes to break the system.

For a finite system, there is a finite but large f_c that scales with the system size as: $\kappa \cong 1 - CN^{-\frac{3-\gamma}{\gamma-1}}$

Internet: Router level map, N=228,263; γ=2.1±0.1; κ=28 → f_c=0.962

ROBUSTNESS OF SCALE-FREE NETWORKS

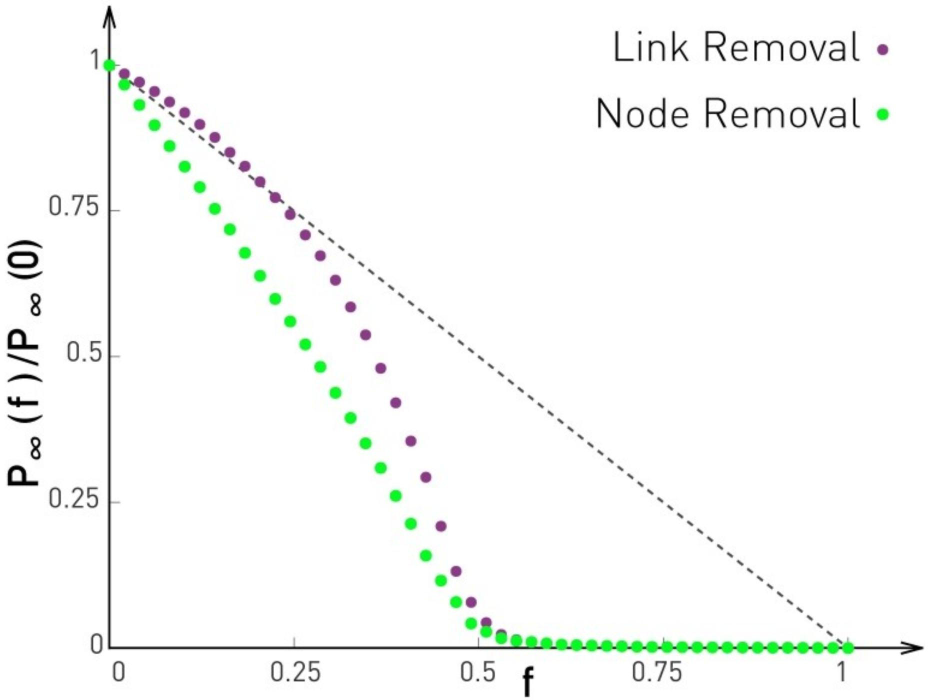
In general a network displays *enhanced robustness* if its breakdown threshold deviates from the random network prediction **(8.8)**, i.e. if

$$f_c > f_c^{ER}. \qquad \textbf{(8.11)}$$

$$f_c = 1 - \frac{1}{\frac{\langle k^2 \rangle}{\langle k \rangle} - 1} \cdot \qquad f_c^{ER} = 1 - \frac{1}{\langle k \rangle} \cdot$$

NETWORK	RANDOM FAILURES (REAL NETWORK)	RANDOM FAILURES (RANDOMIZED NETWORK)	ATTACK (REAL NETWORK)
Internet	0.92	0.84	0.16
WWW	0.88	0.85	0.12
Power Grid	0.61	0.63	0.20
Mobile-Phone Call	0.78	0.68	0.20
Email	0.92	0.69	0.04
Science Collaboration	0.92	0.88	0.27
Actor Network	0.98	0.99	0.55
Citation Network	0.96	0.95	0.76
E. Coli Metabolism	0.96	0.90	0.49
Yeast Protein Interactions	0.88	0.66	0.06

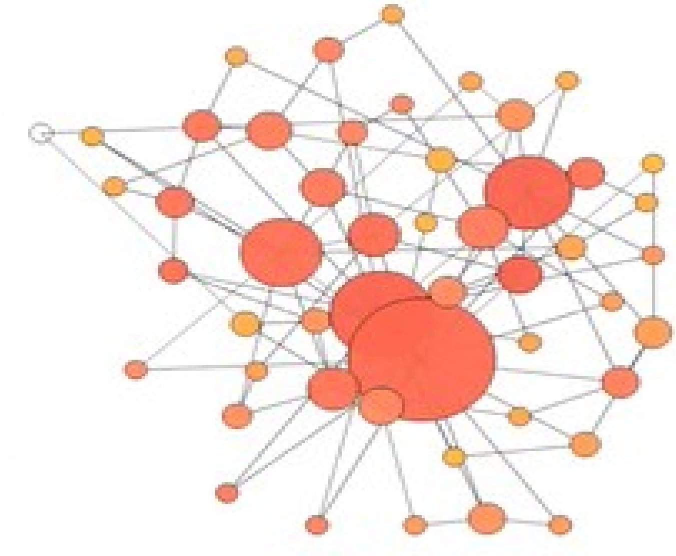
ROBUSTNESS and Link Removal

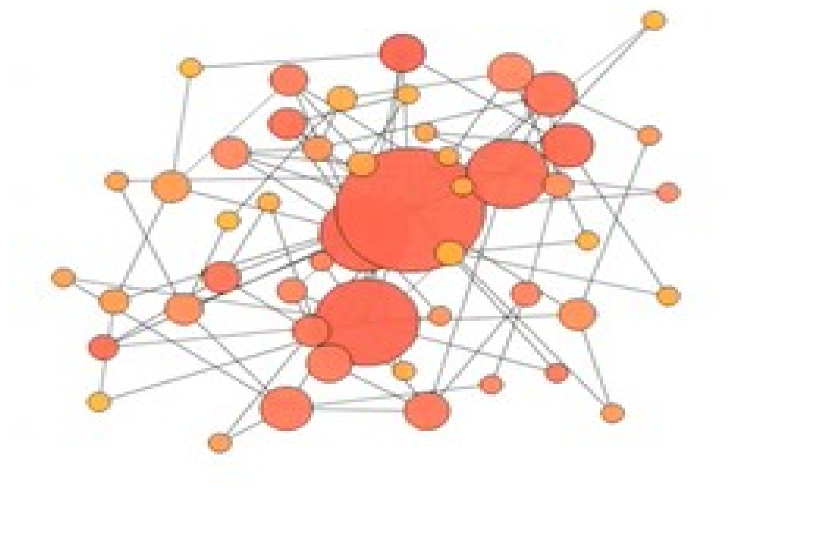


the critical threshold *fc* is the same for random link and node removal

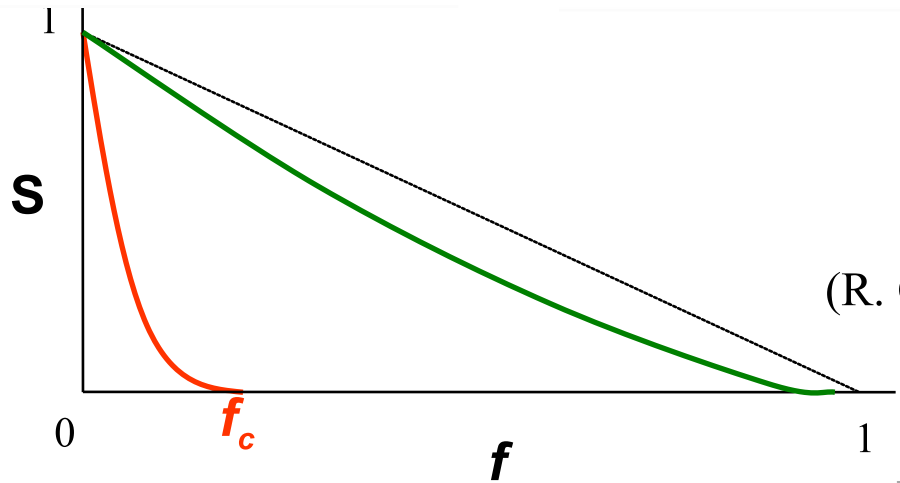
Attack tolerance

Achilles' Heel of scale-free networks





Attacks



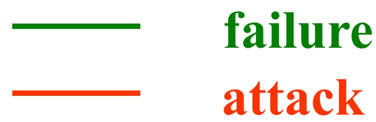
Failures

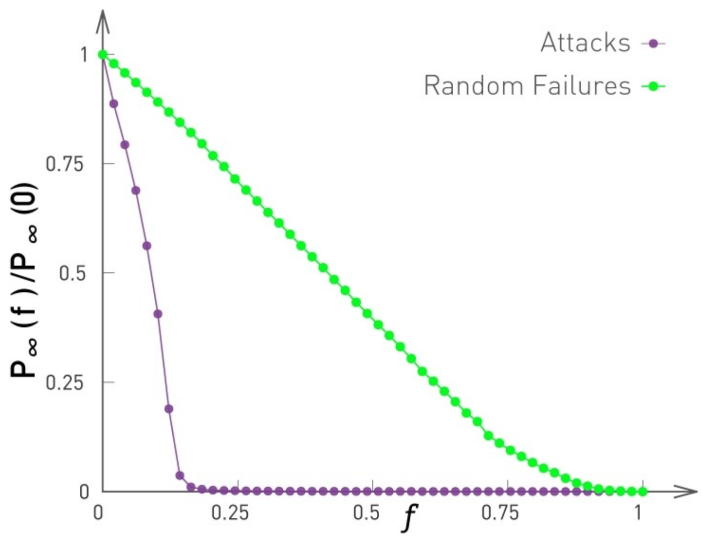
$\gamma \leq 3$: f_c=1

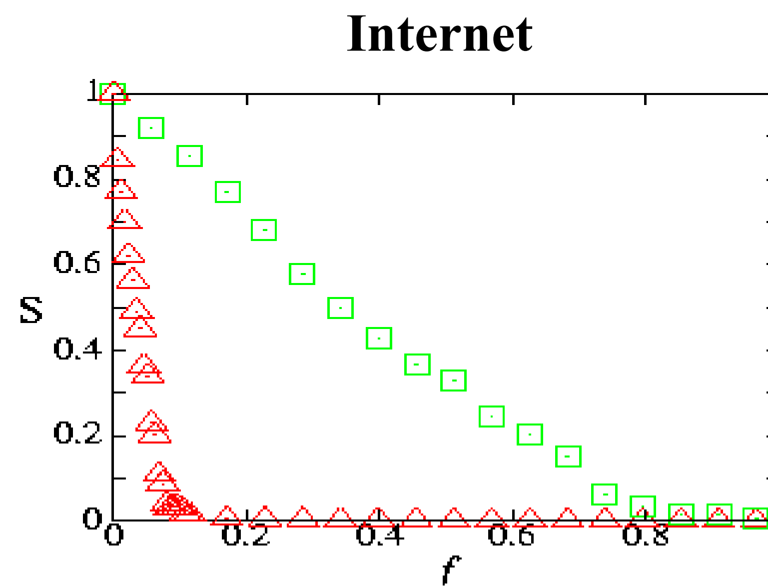
(R. Cohen et al PRL, 2000)

Albert, Jeong, Barabási, *Nature* **406** 378 (2000)

Achilles' Heel of complex networks







R. Albert, H. Jeong, A.L. Barabasi, *Nature* **406** 378 (2000)

Attack threshold for arbitrary P(k)

Attack problem: we remove a fraction *f* of the hubs.

At what threshold f_c will the network fall apart (no giant component)?

Hub removal changes

the maximum degree of the network [K_{max} → $K'_{max} \leq K_{max}$)

the degree distribution [P(k) → P'(k')]

A node with degree k will loose some links because some of its neighbors will vanish.

Claim: once we correct for the changes in K_{max} and P(k),we are back to the robustness problem.

That is, attack is nothing but a robustness of the network with a new K_{max} and P(k).

f_c f

Cohen et al., Phys. Rev. Lett. 85, 4626 (2000).

Attack threshold for arbitrary P(k)

Attack problem: we remove a fraction *f* of the hubs.

the maximum degree of the network [K_{max} → K'_{max} ≤K_{max}) `

If we remove an *f* fraction of hubs, the maximum degree changes:

$$\int_{K'_{max}}^{K_{max}} P(k)dk = f$$

$$\int_{K'_{max}}^{K_{max}} P(k)dk = (\gamma - 1)K_{min}^{\gamma-1} \int_{K'_{max}}^{K_{max}} k^{-\gamma} dk = \frac{\gamma - 1}{1 - \gamma} K_{min}^{\gamma-1} (K_{max}^{1-\gamma} - K'^{1-\gamma}_{max})$$

As K'_{max} ≤K_{max} we can ignore the K_{max} term

$$\left(\frac{K_{min}}{K'_{max}}\right)^{\gamma-1} = f$$

$$K'_{max} = K_{min} f^{\frac{1}{1-\gamma}}$$

← The new maximum degree after removing f fraction of the hubs.

Cohen et al., Phys. Rev. Lett. 85, 4626 (2000).

Attack threshold for arbitrary P(k)

Attack problem: we remove a fraction *f* of the hubs.

the degree distribution changes [P(k) → P'(k')]

A node with degree *k* will loose some links because some of its neighbors will vanish.

Let us calculate the fraction of links removed 'randomly' , f', as a consequence of removing f fraction of hubs.

$$\int_0^{K_{max}} kP(k)dk$$

as K'$_{max}$ ≤K$_{max}$

$$f' = \frac{\int_{K'_{max}}^{K_{max}} kP(k)dk}{<k>} = \frac{1}{<k>}(\gamma-1)K_{min}^{\gamma-1}\int_{K'_{max}}^{K_{max}} k^{1-\gamma}dk = \frac{1}{<k>}\frac{\gamma-1}{2-\gamma}K_{min}^{\gamma-1}(K_{max}^{2-\gamma} - K'^{2-\gamma}_{max}) = -\frac{1}{<k>}\frac{\gamma-1}{2-\gamma}K_{min}^{\gamma-1}K'^{2-\gamma}_{max}$$

$$f' = -\frac{1}{<k>}\frac{\gamma-1}{2-\gamma}K_{min}^{\gamma-1}K_{min}^{2-\gamma}f^{\frac{2-\gamma}{1-\gamma}} = -\frac{1}{<k>}\frac{\gamma-1}{2-\gamma}K_{min}f^{\frac{2-\gamma}{1-\gamma}}$$

$$<k^m> = -\frac{(\gamma-1)}{(m-\gamma+1)}K_{min}^m$$

$$f' = f^{\frac{2-\gamma}{1-\gamma}}$$

For γ→2, f'→1, which means that even the removal of a tiny fraction of hubs will destroy the network. The reason is that for γ=2 hubs dominate the network

$$<k> = -\frac{(\gamma-1)}{(2-\gamma)}K_{min}$$

Cohen et al., Phys. Rev. Lett. 85, 4626 (2000).

Attack threshold for arbitrary P(k)

Attack problem: we remove a fraction *f* of the hubs.

At what threshold f_c will the network fall apart (no giant component)?

Hub removal changes

the maximum degree of the network [K_{max} → $K'_{max} \leq K_{max}$) $K'_{max} = K_{min} f^{\frac{1}{1-\gamma}}$

the degree distribution [P(k) → P'(k')]

A node with degree k will loose some links because some of its neighbors will vanish. $f' = f^{\frac{2-\gamma}{1-\gamma}}$

Claim: once we correct for the changes in K_{max} and P(k), we are back to the robustness problem.

That is, attack is nothing but a robustness of the network with a new K'_{max} and f'.

$$f' = 1 - \frac{1}{\kappa' - 1}$$

$$\kappa' = \frac{<k'^2>}{<k'>} = \frac{<k^2>}{(1-f_c)<k>} = \frac{\kappa}{1-f_c}$$

$$\kappa = \left|\frac{2-\gamma}{3-\gamma}\right| \begin{cases} K_{min} & \gamma > 3 \\ K_{max}^{3-\gamma} K_{min}^{\gamma-2} & 3 > \gamma > 2 \\ K_{max} & 2 > \gamma > 1 \end{cases}$$

$$f_c^{\frac{2-\gamma}{1-\gamma}} = 2 + \frac{2-\gamma}{3-\gamma} K_{min} \left(f_c^{\frac{3-\gamma}{1-\gamma}} - 1 \right)$$

Cohen et al., Phys. Rev. Lett. 85, 4626 (2000).

Attack threshold for arbitrary P(k)

$$f_c^{\frac{2-\gamma}{1-\gamma}} = 2 + \frac{2-\gamma}{3-\gamma} K_{\min}\left(f_c^{\frac{3-\gamma}{1-\gamma}} - 1 \right)$$

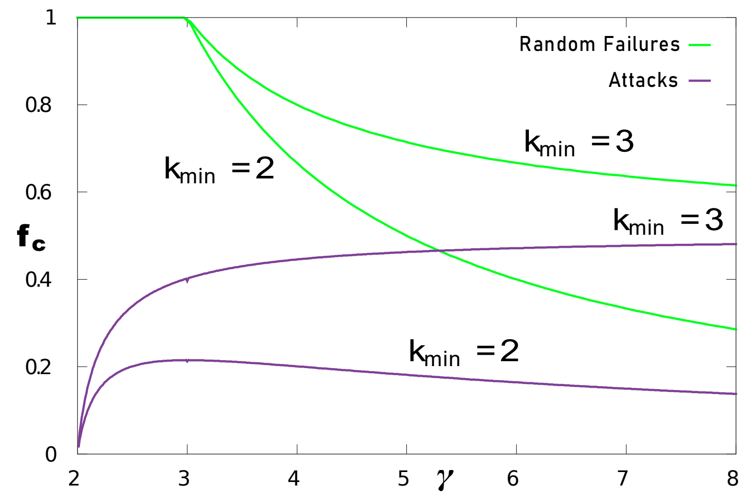
- While f_c for failures decreases monotonically with γ, f_c for attacks can have a non-monotonic behavior: it increases for small γ and decreses for large γ.

- f_c for attacks is always smaller than f_c for random failures.

- For large γ a scale-free network behaves like a random network. As a random network lacks hubs, the impact of an attack is similar to the impact of random node removal. Consequently the failure and the attack thresholds converge to each other for large γ. Indeed, if $\gamma \to \infty$ then $p_k \to \delta(k - k_{min})$, meaning that all nodes have the same degree k_{min}. Therefore random failures and targeted attacks become indistinguishable in the $\gamma \to \infty$ limit, obtaining

$$f_c \to 1 - \frac{1}{(k_{min} - 1)}. \qquad (8.13)$$

- As Figure 8.13 shows, a random network has a finite percolation threshold under both random failures and attacks, as predicted by Figure 8.12 and (8.13) for large γ.

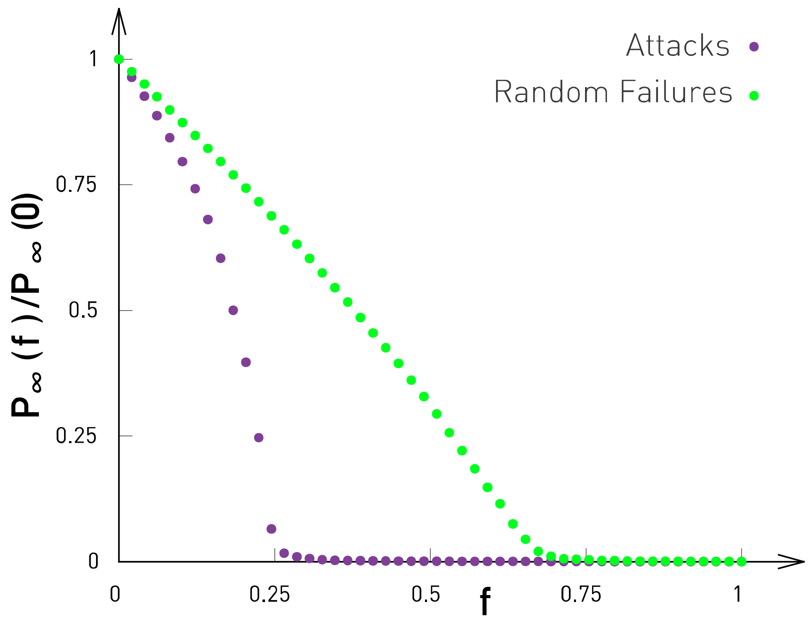


Erdos-Renyi networks

Consider a random graph with connection probability *p* such that at least a giant connected component is present in the graph.

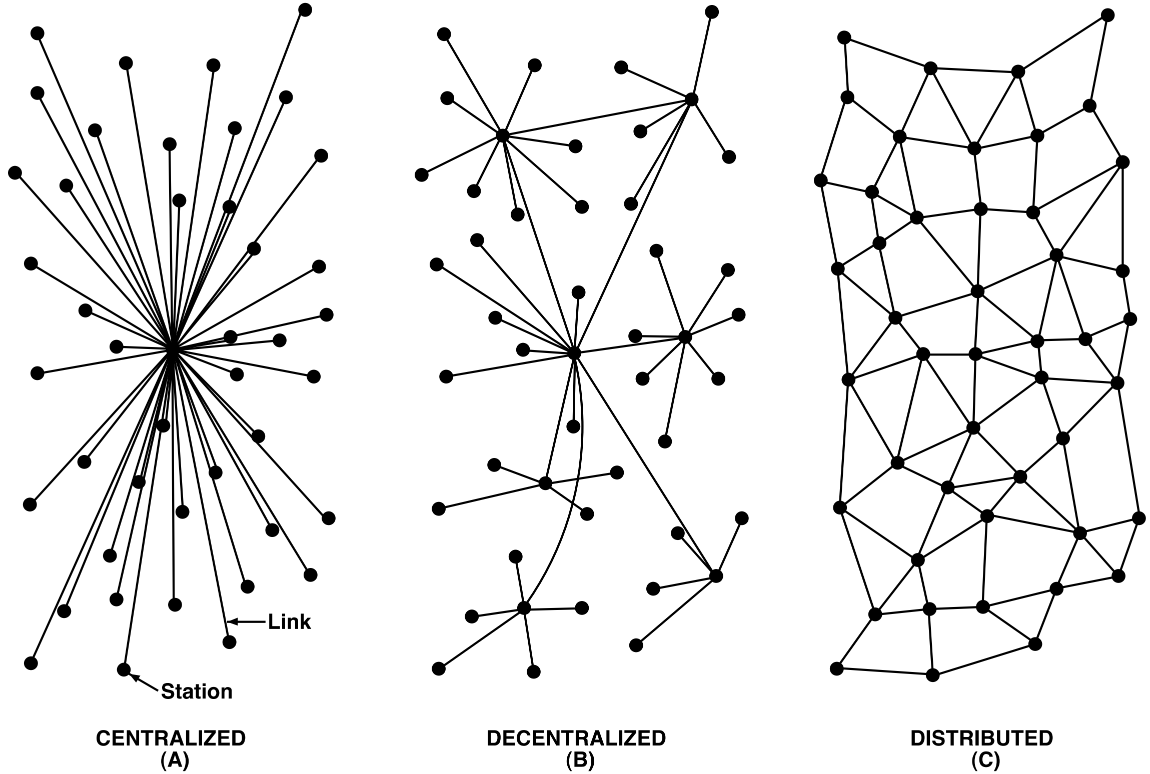
Find the critical fraction of removed nodes such that the giant connected component is destroyed.

$$f_c = 1 - \frac{1}{\frac{\langle k_0^2 \rangle}{\langle k_0 \rangle} - 1} = 1 - \frac{1}{pN} = 1 - \frac{1}{\langle k_0 \rangle}$$



The higher the average degree, the larger damage the network can survive.

Historical Detour: Paul Baran and Internet



1958