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

Section 1 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.

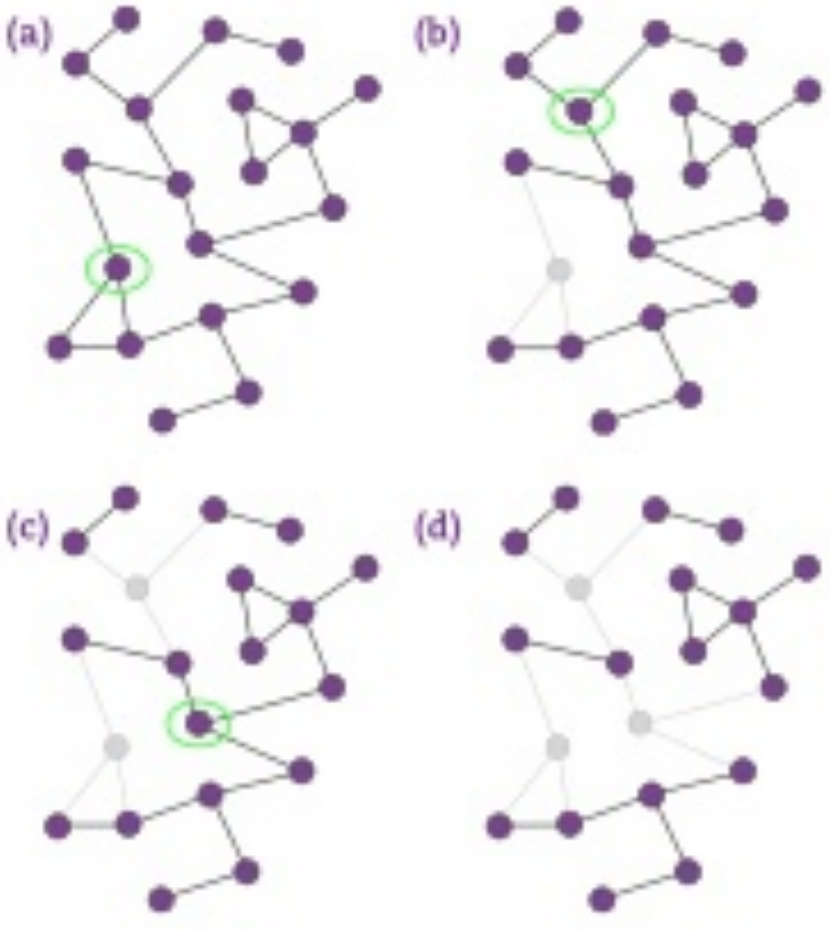
Where does robustness come from?

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



Section 2 Percolation Transition

Cluster size, S: average size of all finite clusters for a given p

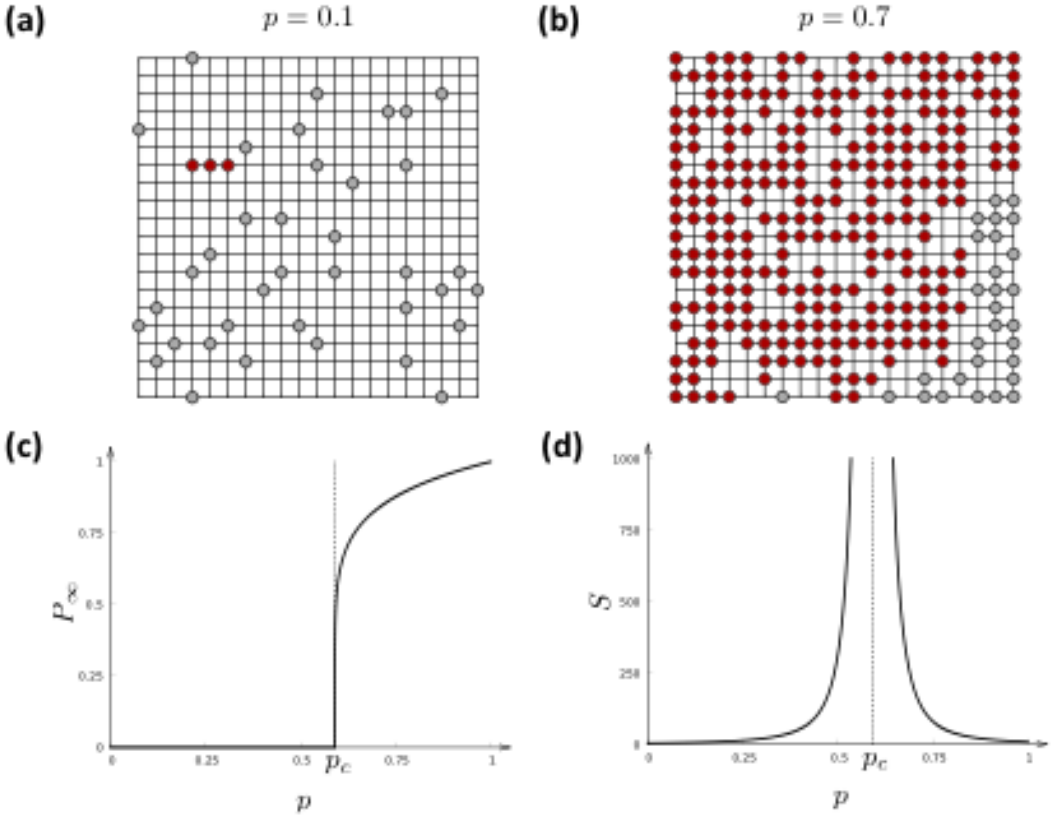
$$S \sim \left| p - p_c \right|^{-\gamma}$$

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.

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

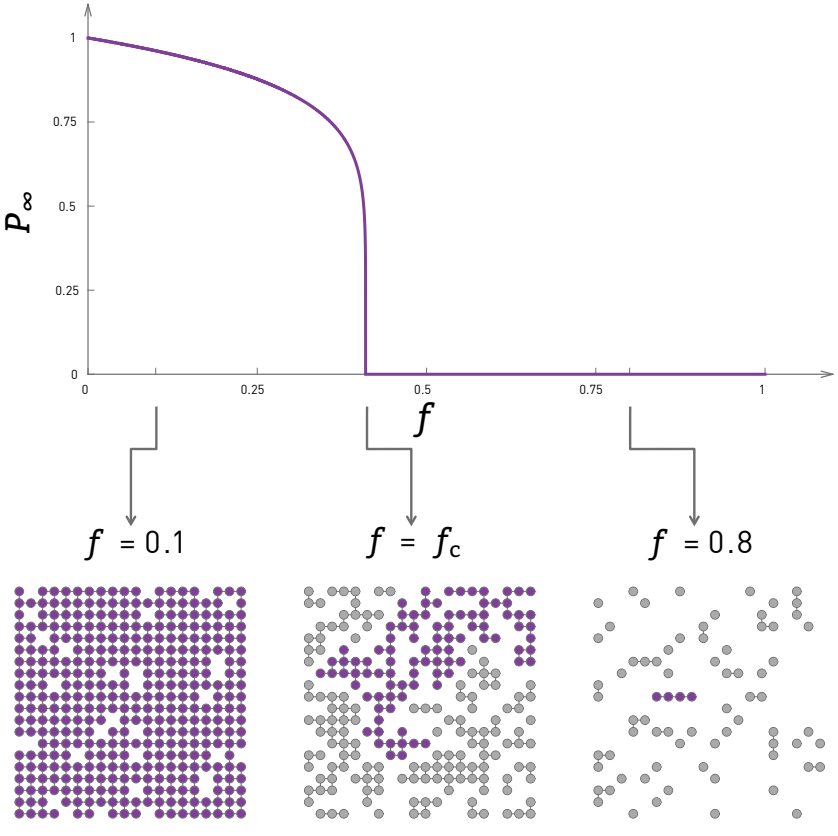


- The value of p_c depends on the lattice type, hence it is not universal. For example, for a two-dimensional square lattice (Figure 8.4) we have $p_c \approx 0.593$, while for a two-dimensional triangular lattice $p_c = 1/2$ (site percolation).

- 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.

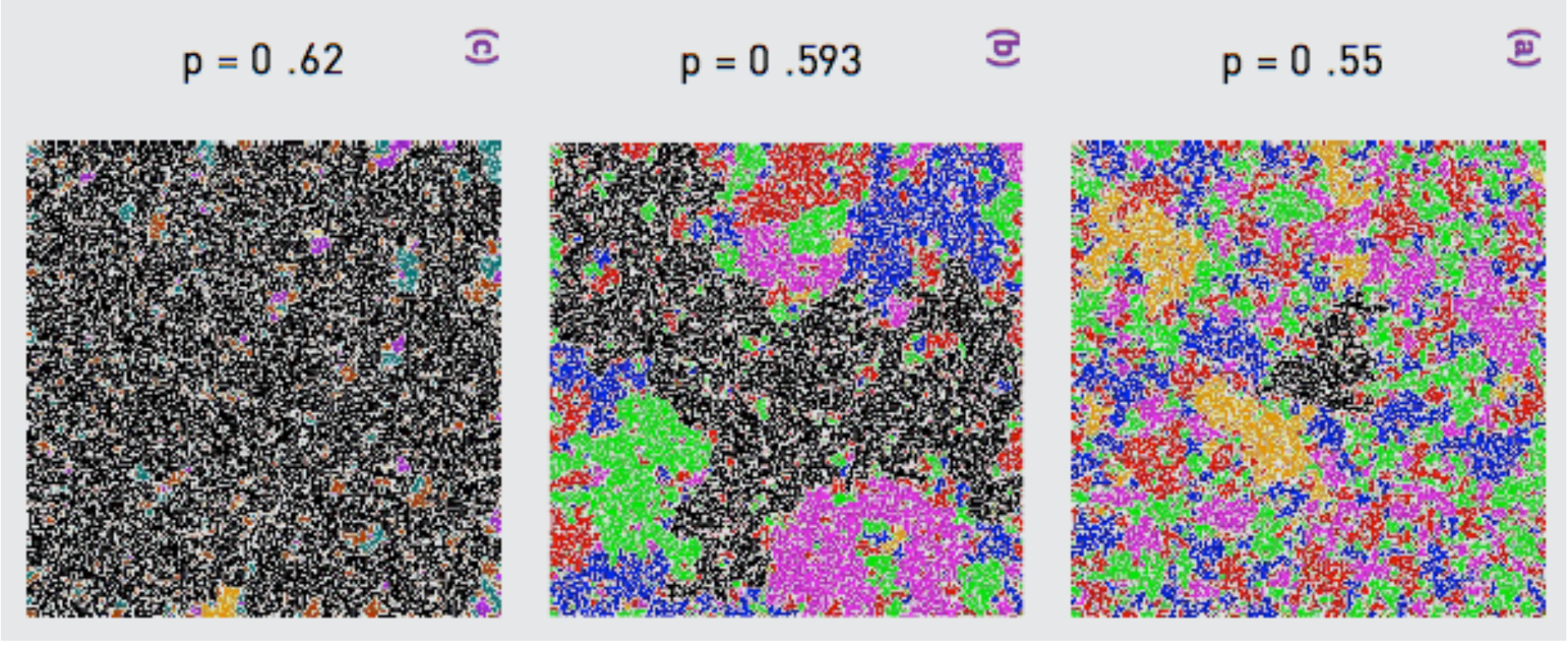
- In contrast with p_c, the critical exponents do not depend on the lattice type, but only on the lattice dimension. In two dimensions, the case shown in Figure 8.4, we have $\gamma_p = 43/18$, $\beta_c = 5/36$, and $\nu = 4/3$, for any lattice. In three dimensions $\gamma_p = 1.80$, $\beta_c = 0.41$, 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].

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.

Section 8.2 Percolation, Forrest Fire



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*

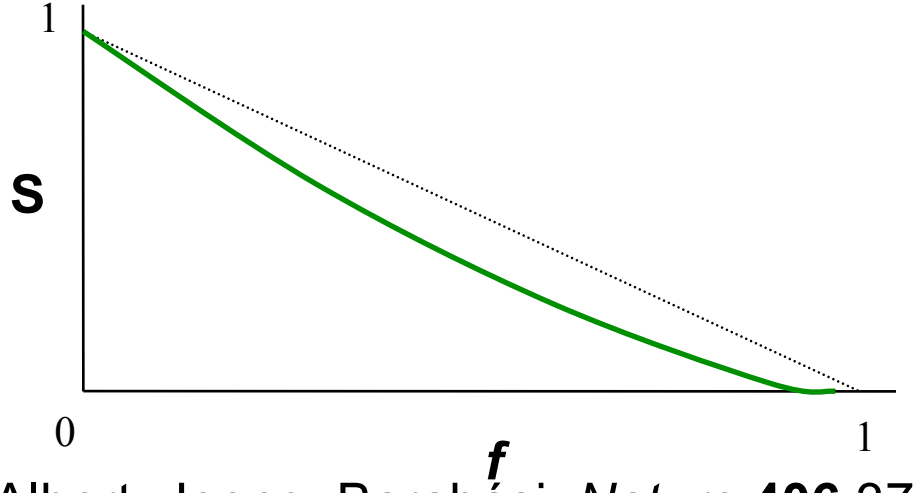
Albert, Jeong, Barabási, *Nature* **406** 378 (2000)

ROBUSTNESS OF SCALE-FREE NETWORKS

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

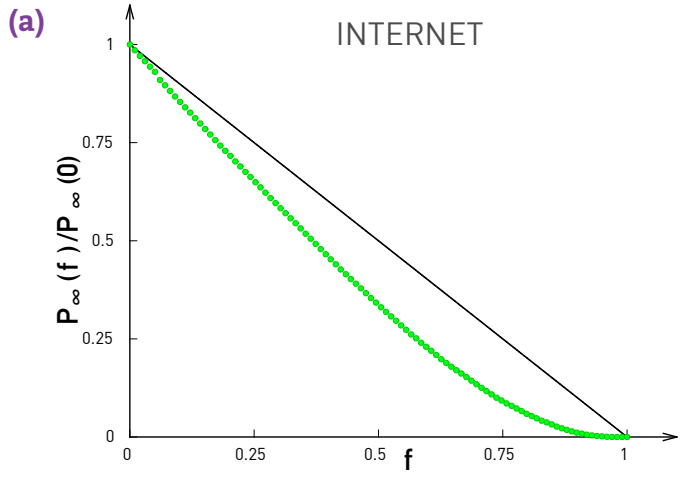
Reason: the hubs.

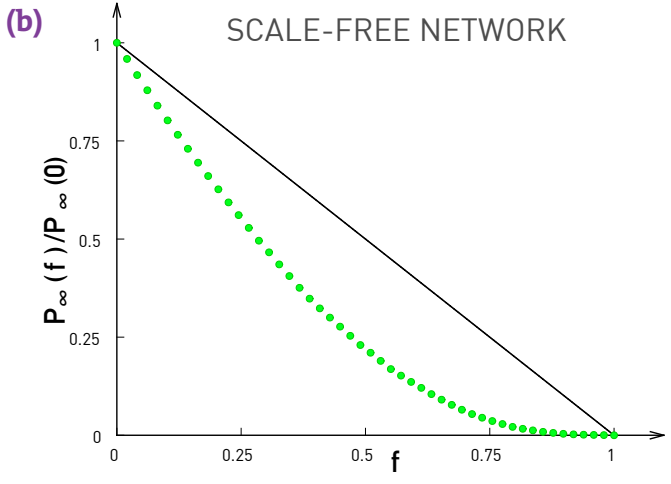
The likelihood of removing a hub is small.

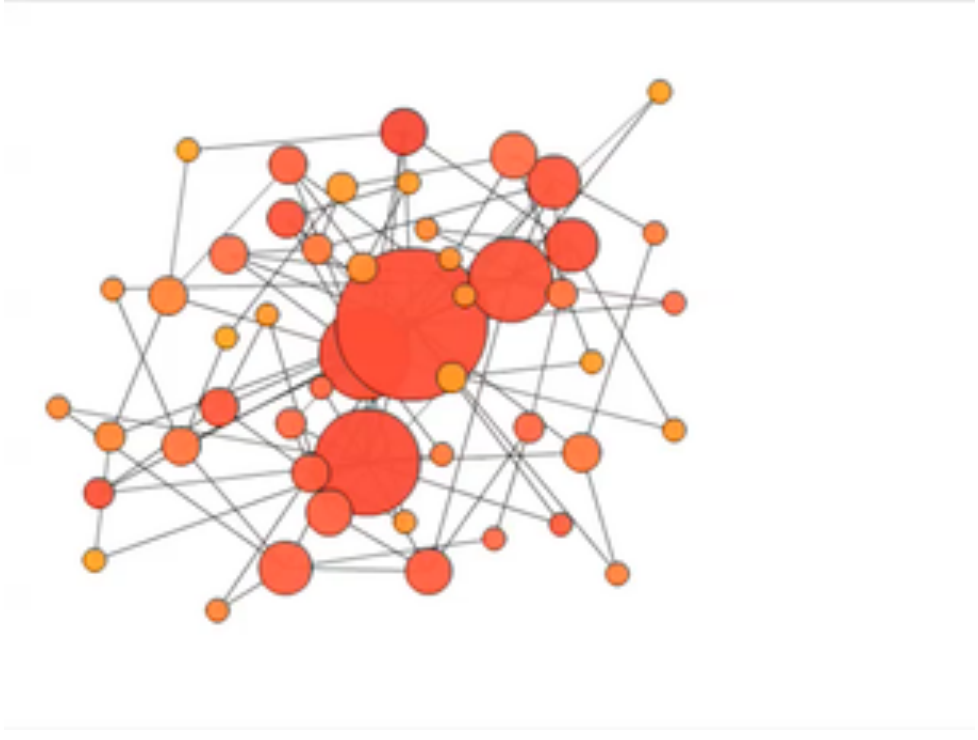


Albert, Jeong, Barabási, *Nature* **406** 378 (2000)

Section 8.3


(a)
INTERNET
1
0.75
0.5
0.25
0
P∞ (f)/P∞ (0)
0
0.25
0.5
f
0.75
1

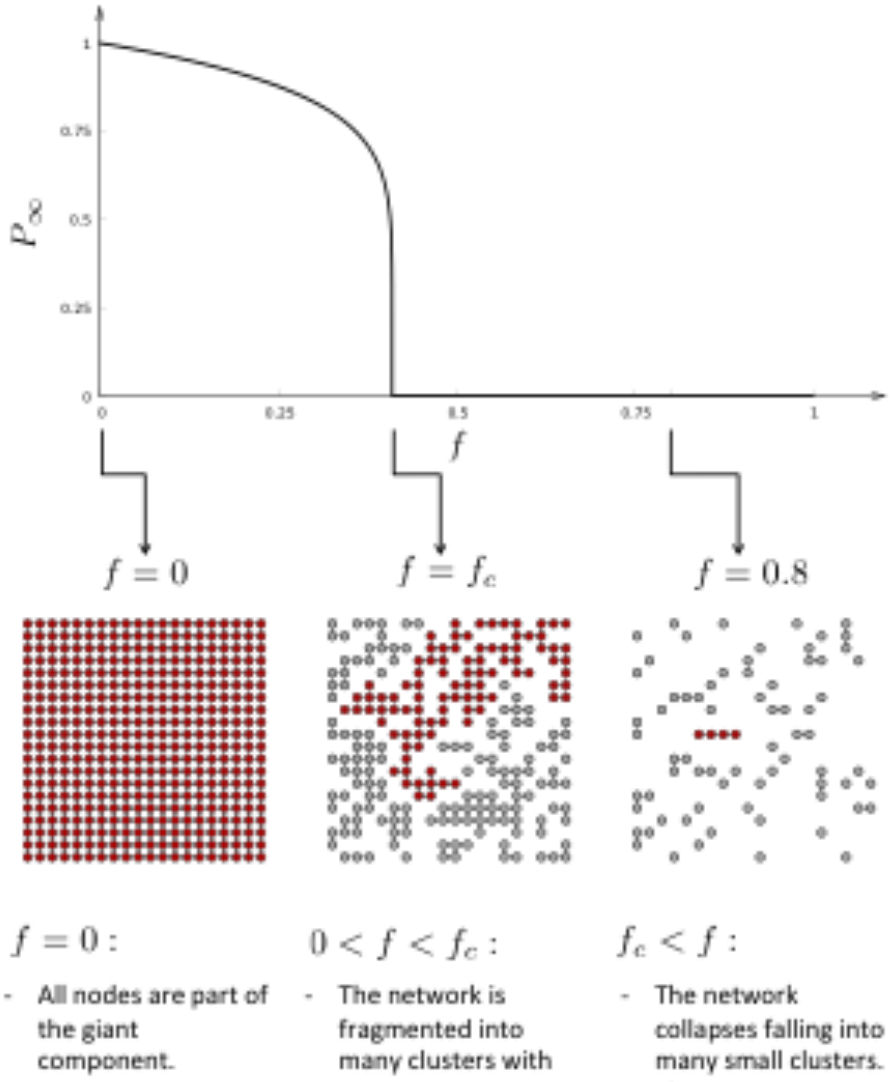

(b)
SCALE-FREE NETWORK
1
0.75
0.5
0.25
0
P∞ (f)/P∞ (0)
0
0.25
0.5
f
0.75
1



Network Breakdown: Inverse percolation

What it the value of fc?
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

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

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

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)?

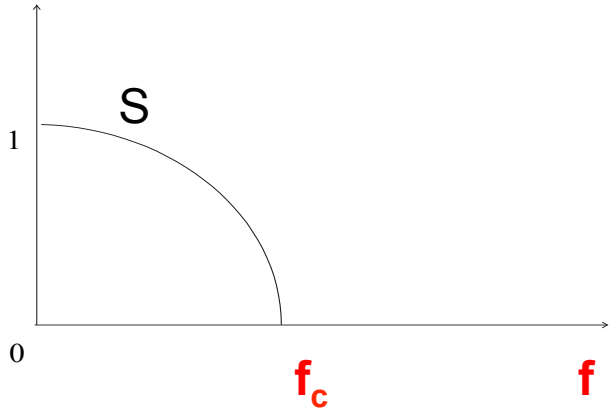
Random node removal changes

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:

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

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).

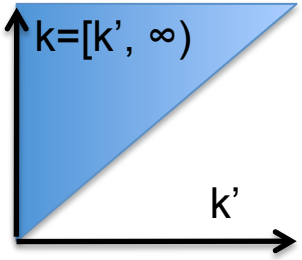
BREAKDOWN THRESHOLD FOR ARBITRARY P(K)

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

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



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

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

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

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

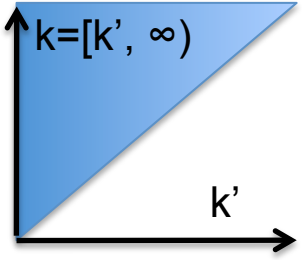
BREAKDOWN THRESHOLD FOR ARBITRARY P(K)

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

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



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

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

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

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

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 individuals nodes [k → k' ≤k)

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

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

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

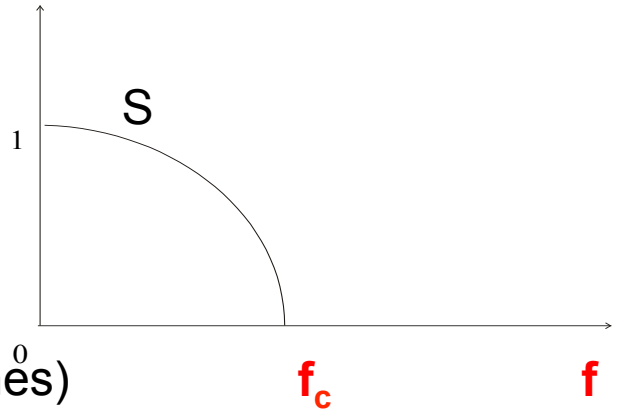
$$\kappa \equiv \frac{< k'^2 >_f}{< k' >_f} = 2$$

κ>2: a giant cluster exists

κ<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)

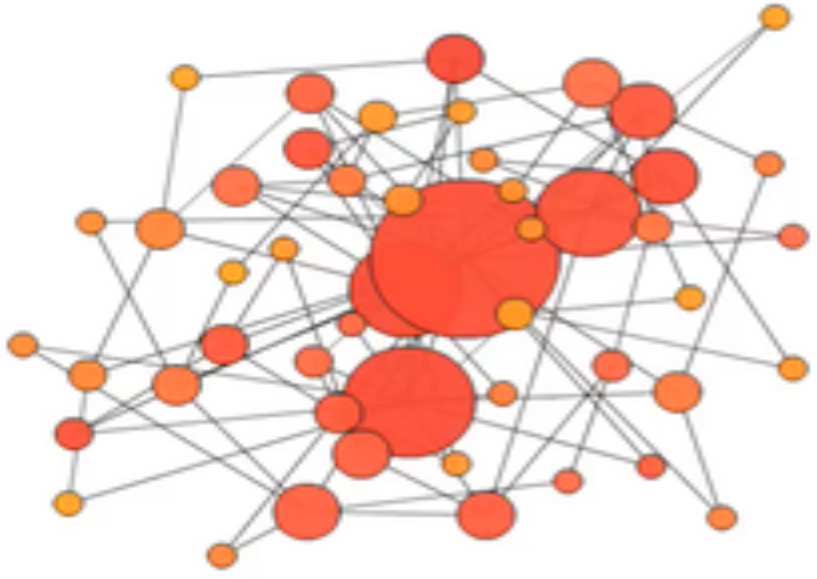
Cohen et al., Phys. Rev. Lett. 85, 4626 (2000).

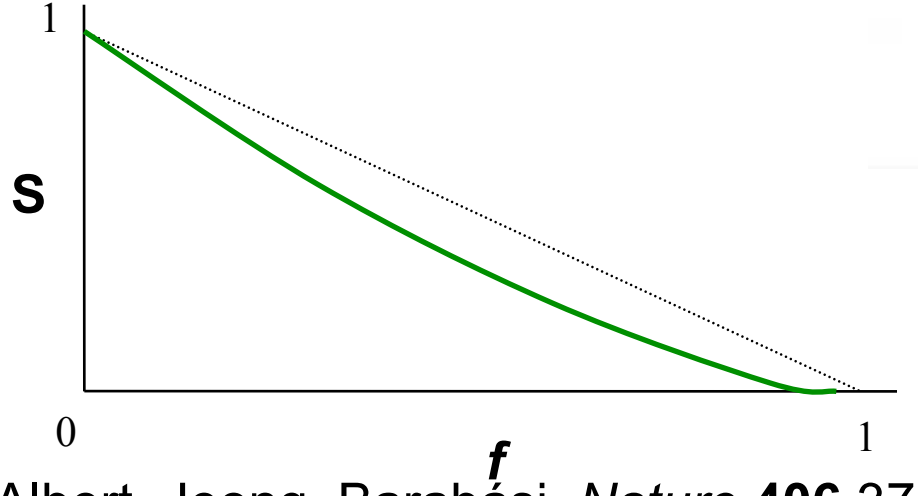
ROBUSTNESS OF SCALE-FREE NETWORKS

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

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

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

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

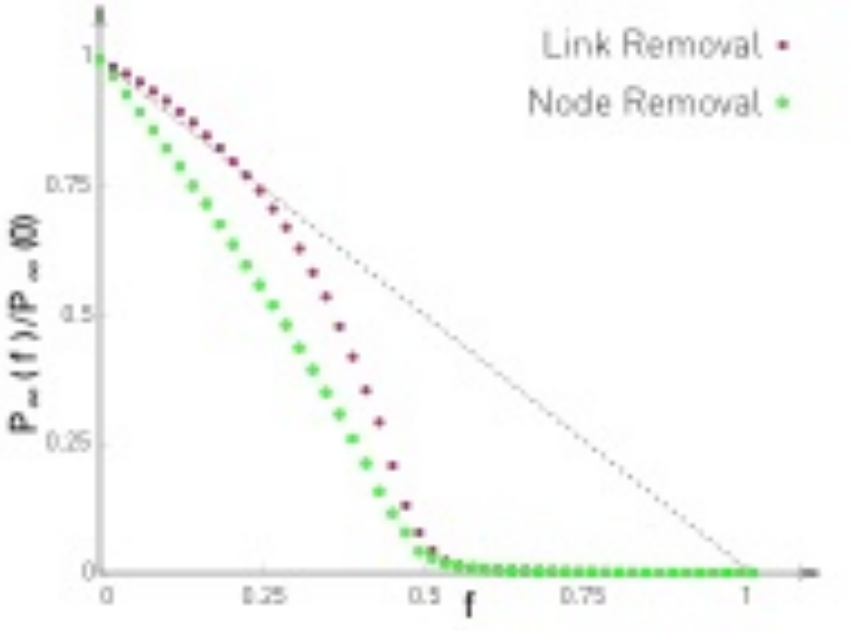
In general a network displays *enhanced robustness* if its breakdown threshold deviates from the random network prediction (8.8), i.e. if

$$f_c > f_c^{ER}. \tag{8.11}$$

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

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	0.89	0.66	0.06

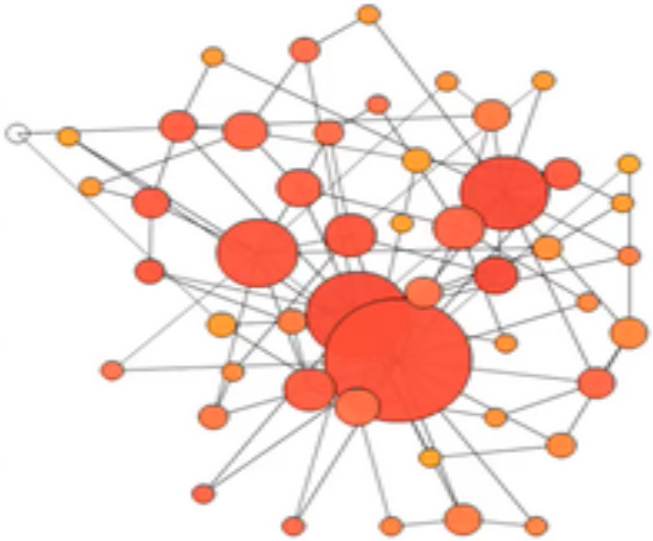
ROBUSTNESS and Link Removal

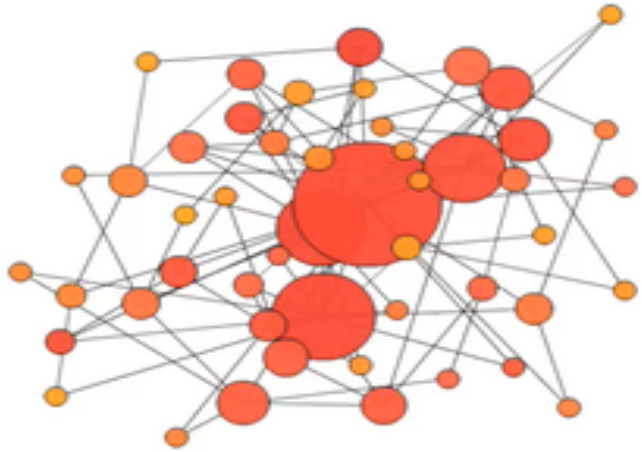


the critical threshold *fc* is the same for random link and node removal

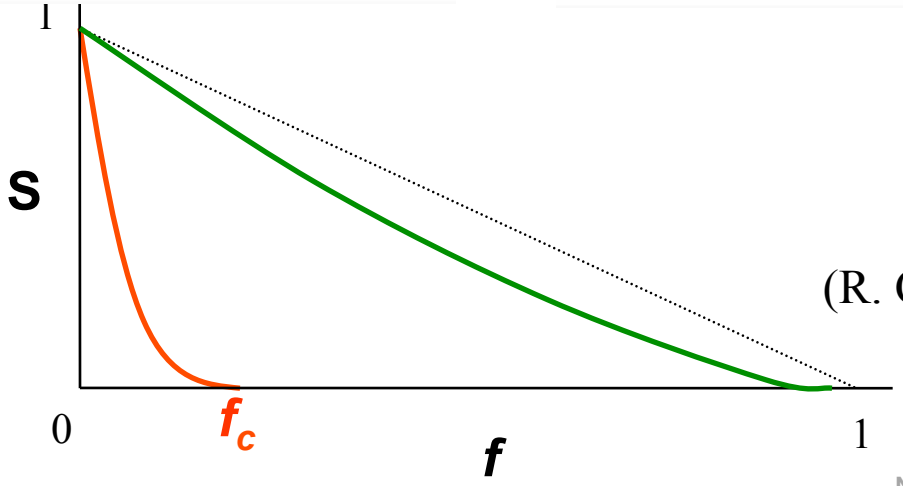
Attack tolerance

Achilles' Heel of scale-free networks





Attacks



Failures

$\gamma \leq 3 : f_c=1$

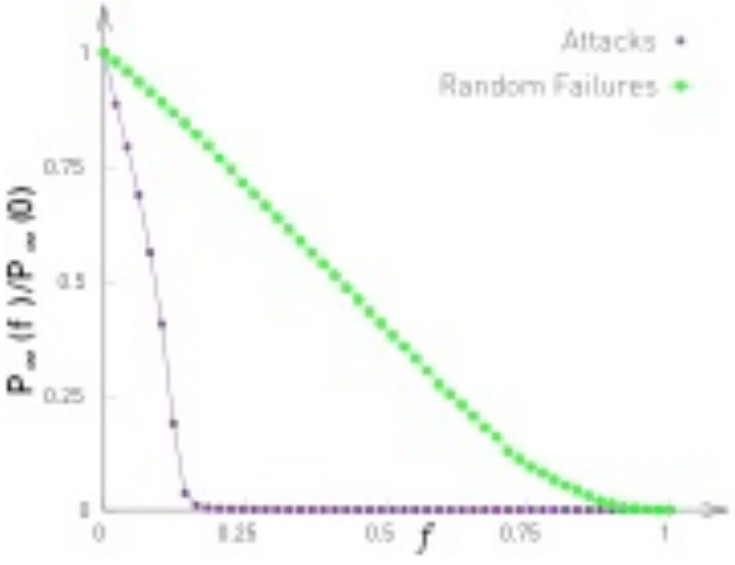
(R. Cohen et al PRL, 2000)

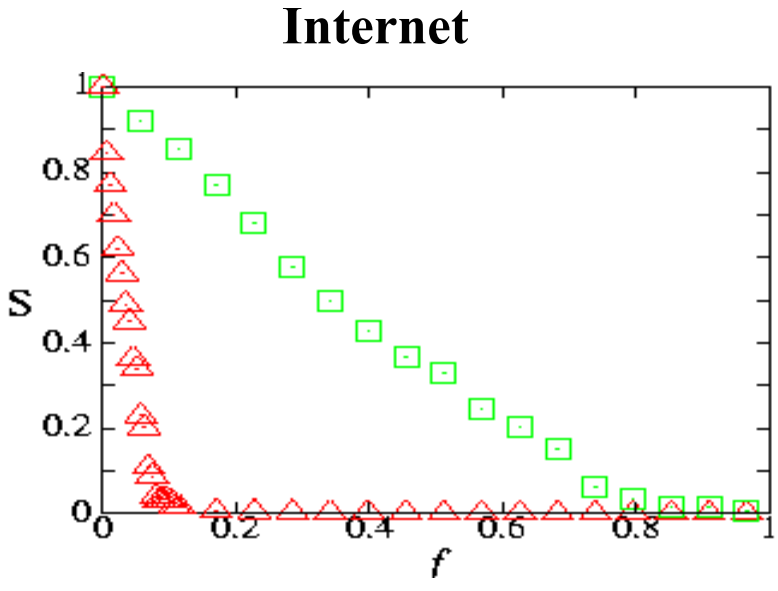
Albert, Jeong, Barabási, *Nature* **406** 378 (2000)

Achilles' Heel of complex networks

failure

attack





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 [$K_{max} \rightarrow K'_{max} \leq K_{max}$)

the degree distribution [$P(k) \rightarrow P'(k')$]

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 robusiness 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 [$K_{max} \rightarrow K'_{max} \leq K_{max}$) `

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 $K'_{max} \leq K_{max}$ we can ignore the K_{max} term

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

← 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 $K'_{max} \le K_{max}$

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

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

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

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

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

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

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

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'.

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

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

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

Attack threshold for arbitrary P(k)

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

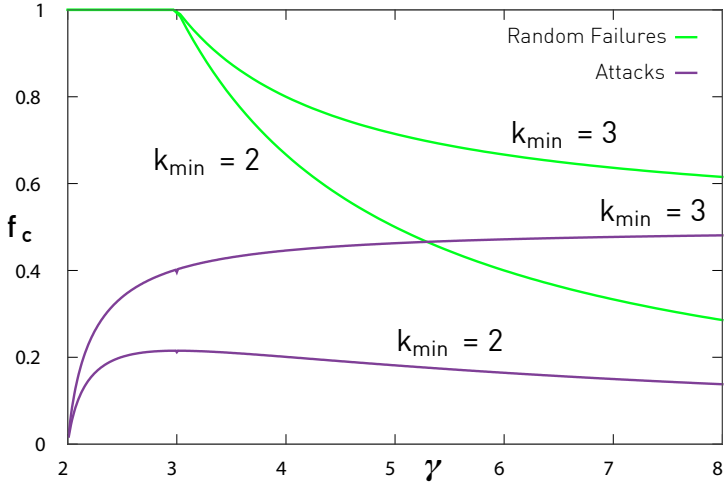
- While f_c for failures decreases monotonically with γ, f_c for attacks can have a non-monotonic behavior: it increases for small γ and decreses for large γ.

- 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.

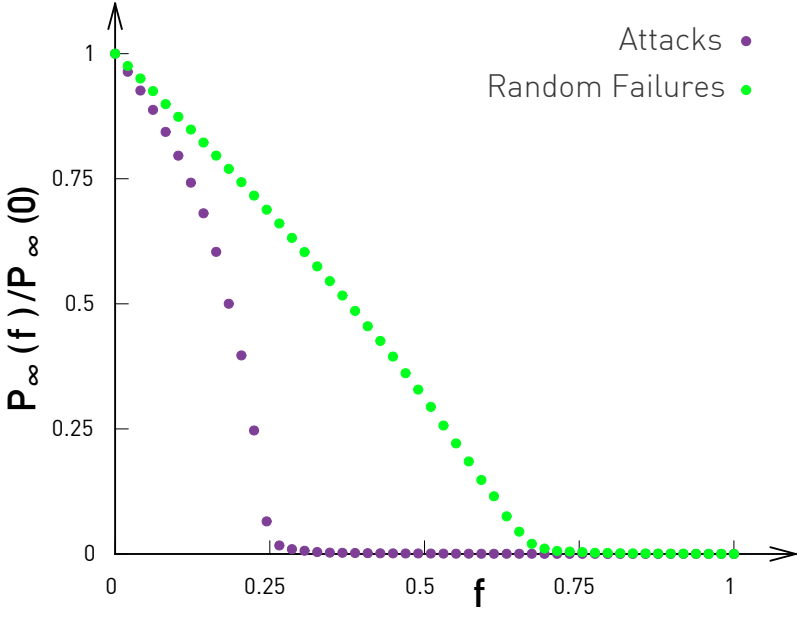


Erdos-Renyi networks

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

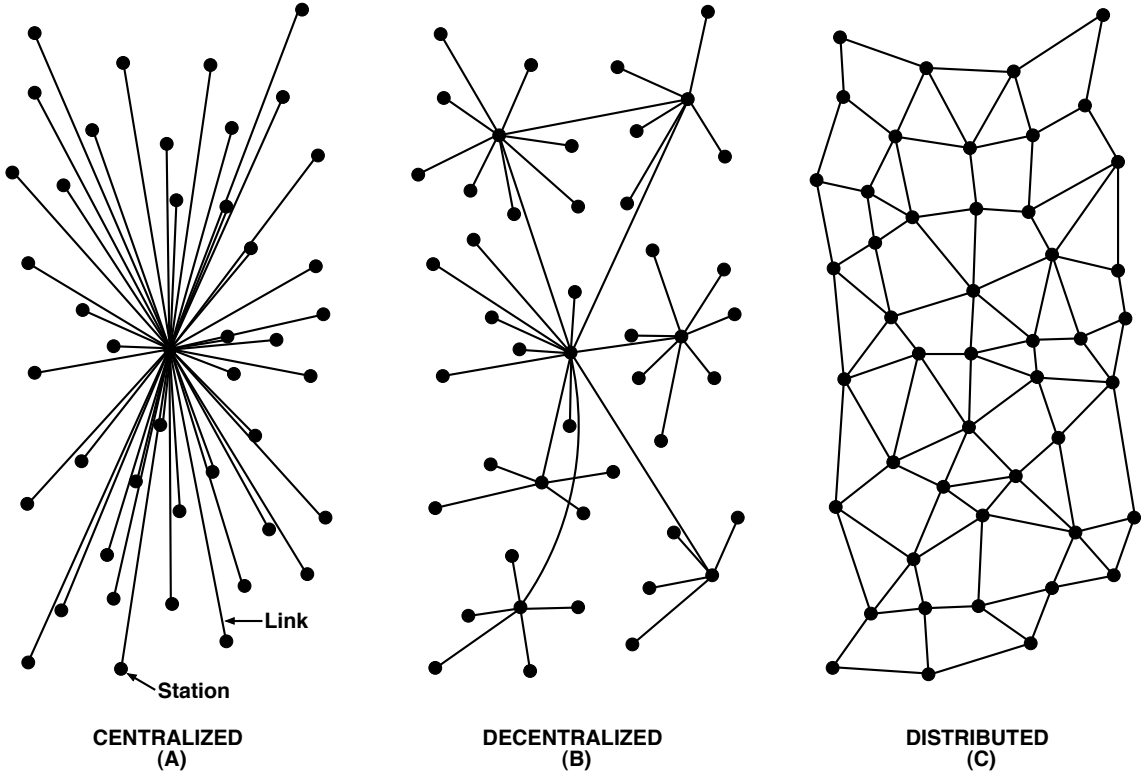
Find the critical fraction of removed nodes such that the giant connected component is destroyed.

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



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

Historical Detour: Paul Baran and Internet



1958

Cascading failures: Empirical Results

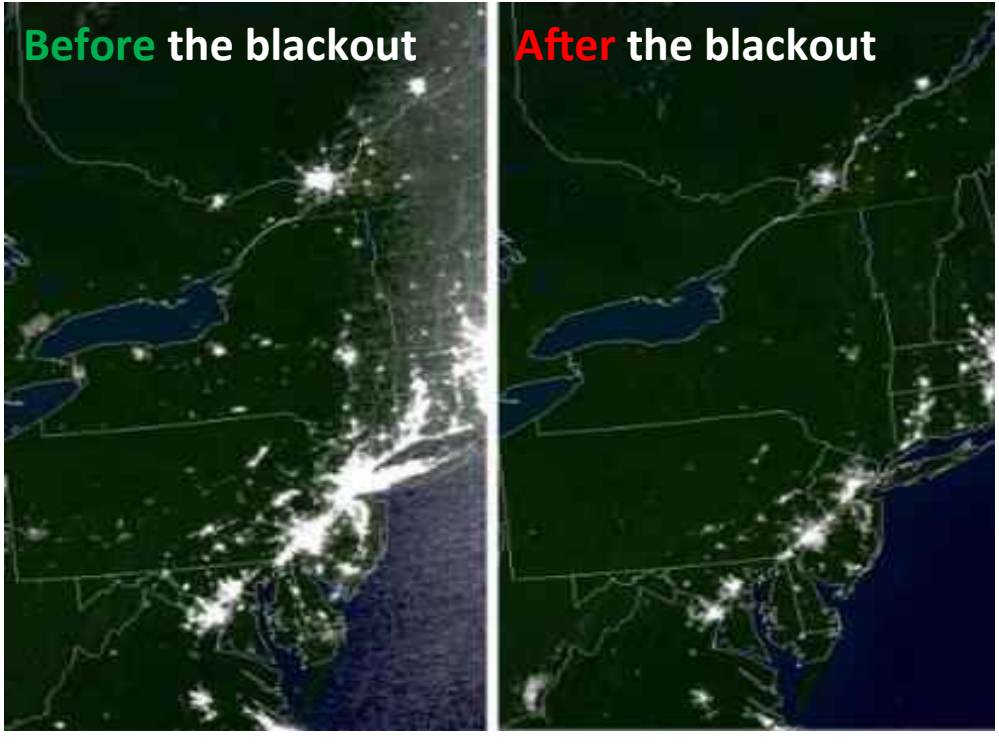
Cascades: The Domino Effect

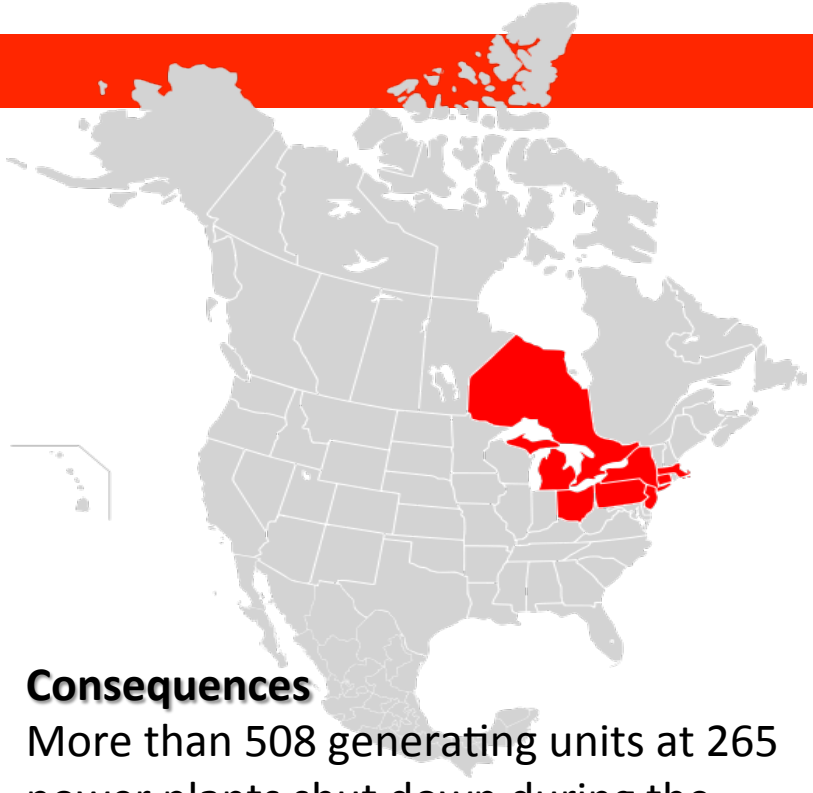
Large events triggered by small initial shocks

Northeast Blackout of 2003

Origin

A 3,500 MW power surge (towards Ontario) affected the transmission grid at 4:10:39 p.m. EDT. (Aug-14-2003)





Consequences

More than 508 generating units at 265 power plants shut down during the outage. In the minutes before the event, the NYISO-managed power system was carrying 28,700 MW of load. At the height of the outage, the load had dropped to 5,716 MW, a loss of 80%.

- **Denial of Service Attacks (Internet)**
  If a router fails to transmit the packets received by it, the Internet protocols will alert the neighboring routers to avoid the troubled equipment by re-routing the packets using alternative routes. Consequently a failed router increases traffic on other routers, potentially inducing a series of denial of service attacks throughout the Internet [13].

- **Financial Crises**
  Cascading failures are common in economic systems. For example, the drop in the house prices in 2008 in the U.S. has spread along the links of the financial network, inducing a cascade of failed banks, companies and even nations [14, 15, 16]. It eventually caused the worst global financial meltdown since the 1930s Great Depression.

VOLUME 279
NUMBER 73
Suggested retail price
$1.00
$1.50 outside of
Metro Boston

The Boston Globe

MONDAY, MARCH 14, 2011

A NEW WEAK

TODAY: *Partly sunny and colder. H*
37-42. Low 27-32.
TOMORROW: *Mostly sunny, milde*
High 42-47. Low 32-37.
HIGH TIDE: *6:42 a.m., 7:25 p.m.*
SUNRISE: *6:59* SUNSET: *6:49*
FULL REPORT: PAGE B13

Cascading disaster in Japan

Blast shakes a second reactor death toll soar

By Martin Fackler and Mark McDonald
NEW YORK TIMES

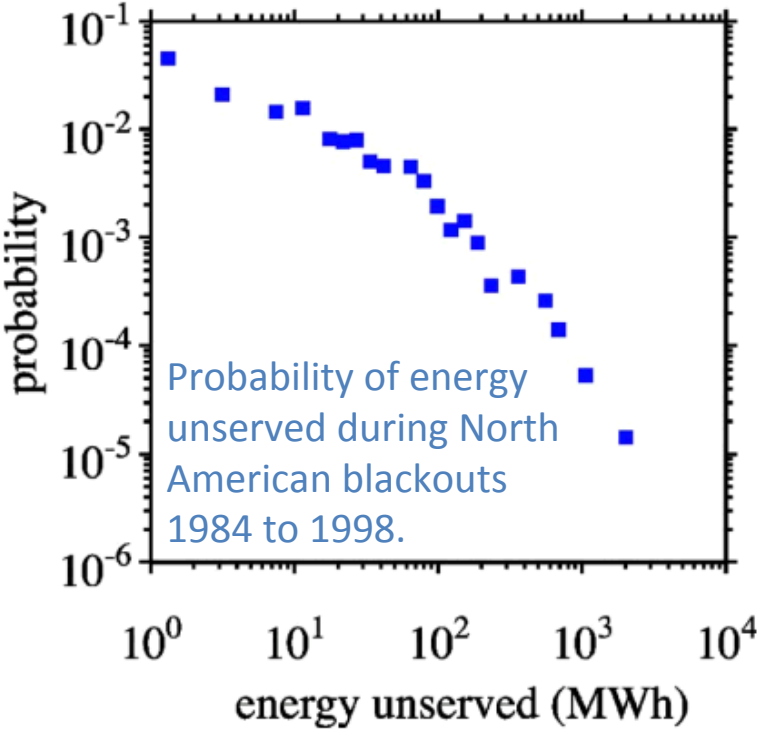
SENDAI, Japan — Japan reel from a rapidly unfolding disaster epic scale yesterday, pummeled by t death toll, destruction, and homele ness caused by the earthquake a tsunami and new hazards from da aged nuclear reactors. The prime m ister called it Japan's worst crisis sin World War II.

Japan's $5 trillion economy, t world's third largest, was threaten with severe disruptions and partial p ralysis as many industries shut do temporarily. The armed forces and v unteers mobilized for the far more gent crisis of finding survivors, eva ating residents near the strick power plants and caring for the v tims of the record 8.9 magnitu quake that struck on Friday.

The disaster has left more th 10,000 dead, many thousands hon less, and millions without water, po er, heat, or transportation.

Cascades Size Distribution of Blackouts

Unserved energy/power magnitude (*S*) distribution



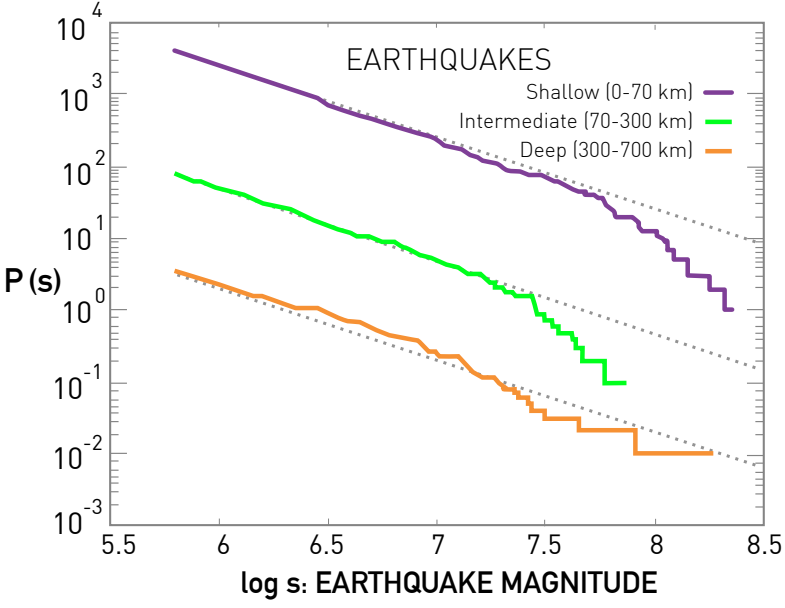
$$P(S) \sim S^{-\alpha},\ 1 < \alpha < 2$$

Source	Exponent	Quantity
North America	2.0	Power
Sweden	1.6	Energy
Norway	1.7	Power
New Zealand	1.6	Energy
China	1.8	Energy

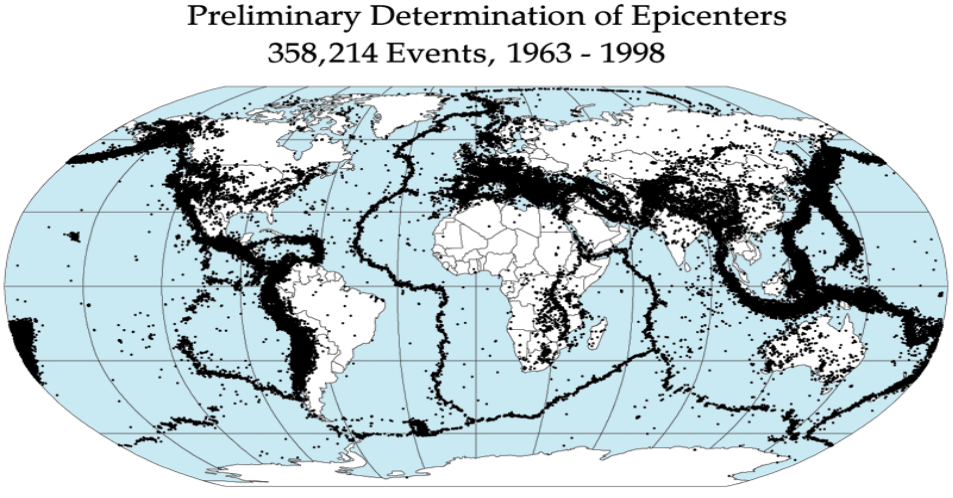
I. Dobson, B. A. Carreras, V. E. Lynch, D. E. Newman, *CHAOS* 17, 026103 (2007)

Cascades Size Distribution of Earthquakes

(c)



Earthquakes during 1977–2000.

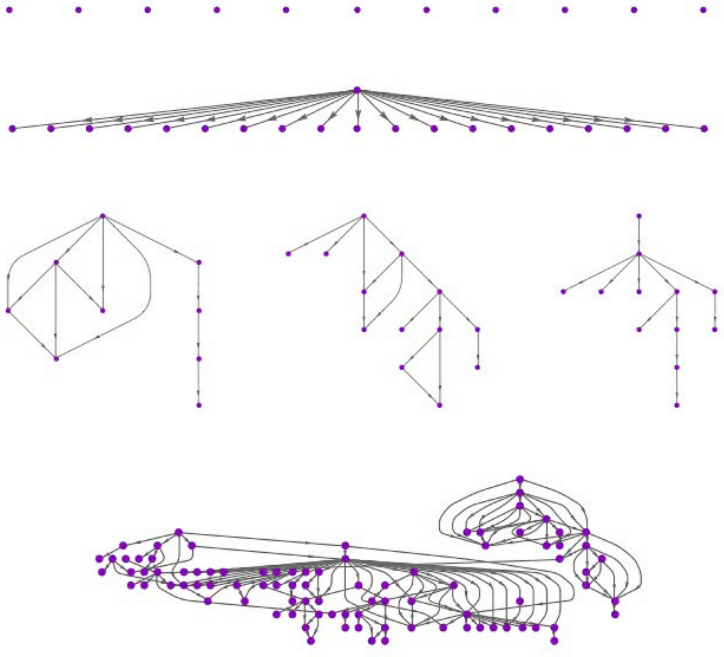


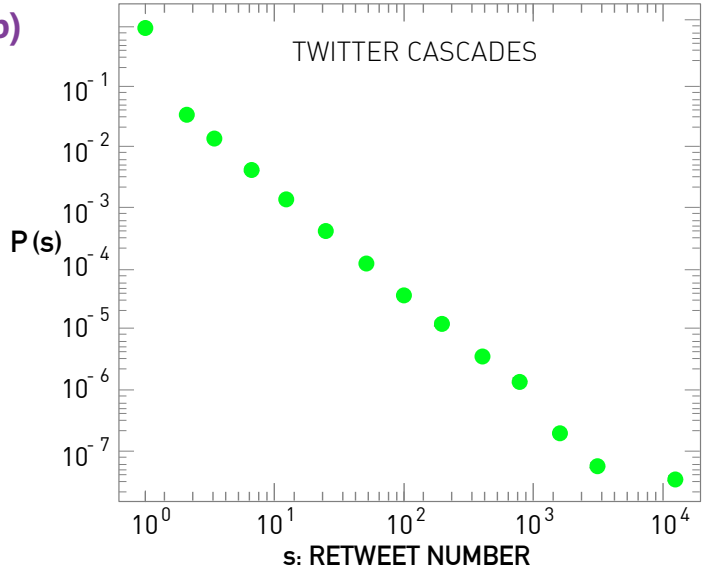
Earthquake size *S* distribution

$$P(S) \sim S^{-\alpha}, \alpha \approx 1.67$$

Y. Y. Kagan, *Phys. Earth Planet. Inter.* 135 (2–3), 173–209 (2003)

Information Cascades





$$p(s) \sim s^{-\alpha},$$

$\alpha \simeq 1.75$

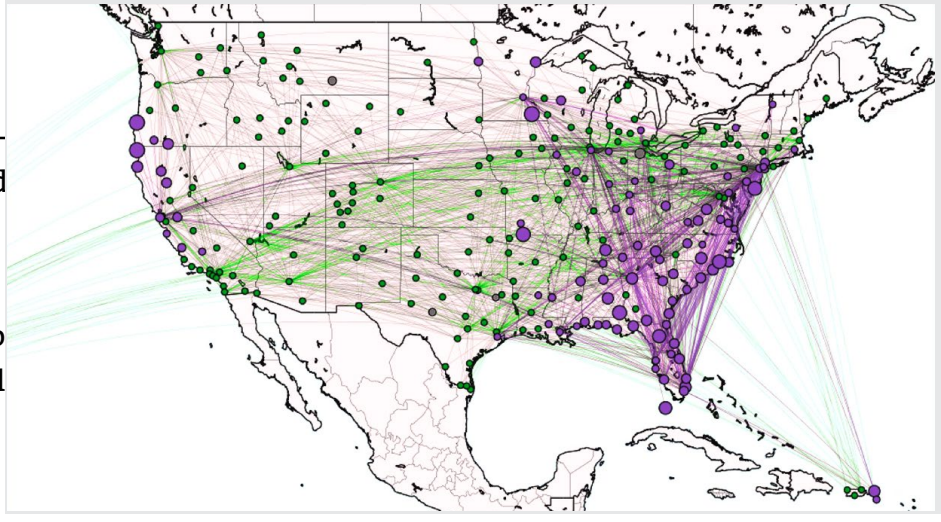
Section 8.5 Empirical Results

Cascading failures are documented in many other environments:

- The consequences of bad weather or mechanical failures can cascade through airline schedules, delaying multiple flights and stranding thousands of passengers (BOX 8.3) [22].

- The disappearance of a species can cascade through the food web of an ecosystem, inducing the extinction of numerous species and altering the habitat of others [23, 24, 25, 26].

- The shortage of a particular component can cripple supply chains. For example, the 2011 floods in Thailand have resulted in a chronic shortage of car components that disrupted the production chain of more than 1,000 automotive factories worldwide. Therefore the damage was not limited to the flooded factories, but resulted in worldwide insurance claims reaching $20 billion [27].



U.S. aviation map showing congested airports as purple nodes, while those with normal traffic as green nodes. The lines correspond to the direct flights between them on March 12, 2010. The clustering of the congested airports indicate that the dealys are not independent of each other, but cascade through the airport network. After [22].

Section 8.5 Empirical Results: Summary

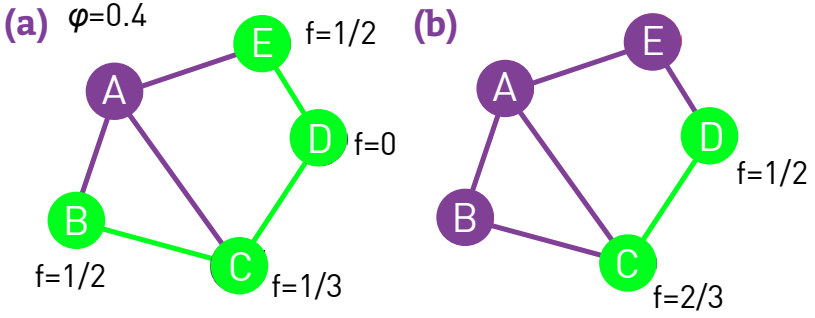
SOURCE	EXPONENT	CASCADE
Power grid (North America)	2.0	Power
Power grid (Sweden)	1.6	Energy
Power grid (Norway)	1.7	Power
Power grid (New Zealand)	1.6	Energy
Power grid (China)	1.8	Energy
Twitter Cascades	1.75	Retweets
Earthquakes	1.67	Seismic Wave

Modeling Cascading failures

(i) The system is characterized by some flow over a network, like the flow of electric current in the power grid or the flow of information in communication systems.

(ii) Each component has a local breakdown rule that determines when it contributes to a cascade, either by failing (power grid, earthquakes) or by choosing to pass on a piece of information (Twitter).

(iii) Each system has a mechanism to redistribute the traffic to other nodes upon the failure or the activation of a component.



(a,b) The development of a cascade in a small network in which each node has the same breakdown threshold $\varphi = 0.4$. Initially all nodes are in state 0, shown as green circles. After node A changes its state to 1 (purple), its neighbors *B* and *E* will have a fraction $f = 1/2 > 0.4$ of their neighbors in state 1. Consequently they also fail, changing their state to 1, as shown in (b). In the next time step *C* and *D* will also fail, as both have $f > 0.4$. Consequently the cascade sweeps the whole network, reaching a size $s = 5$. One can check that if we initially flip node *B*, it will not induce an avalanche.

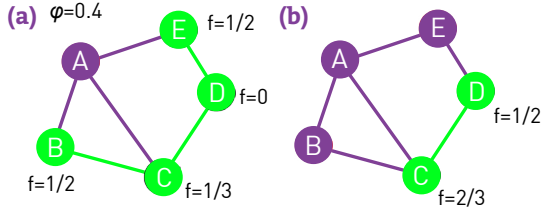
Initial Setup

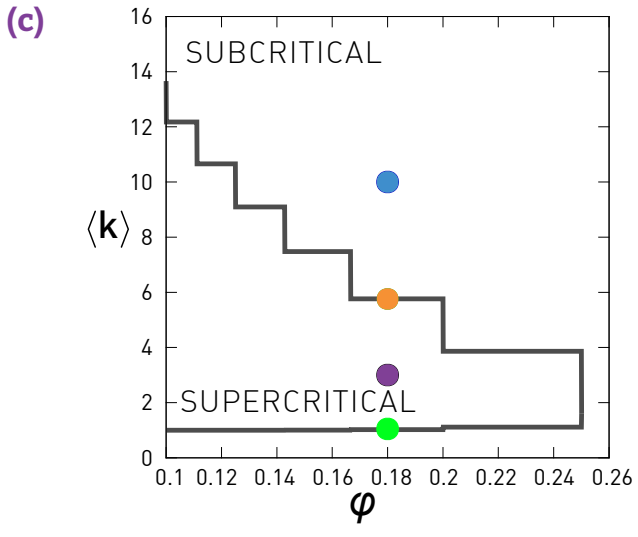
- Random graph with *N* nodes
- Initially each node is functional.

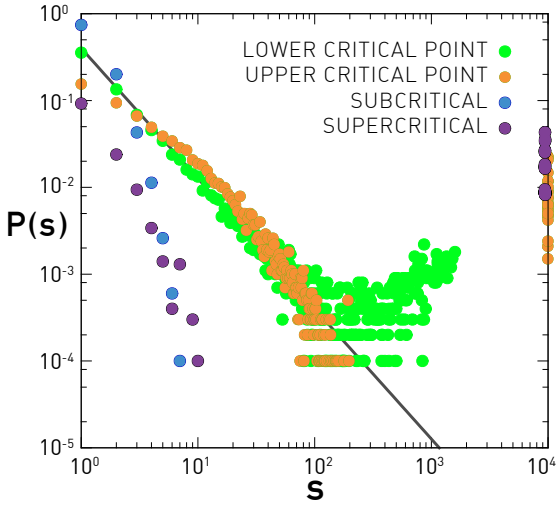
Cascade

- Initiated by the failure of one node.
- f_i : fraction of failed neighbors of node *i*. Node *i* fails if f_i is greater than a global threshold ϕ.

D. Watts, *PNAS* 99, 5766-5771 (2002)





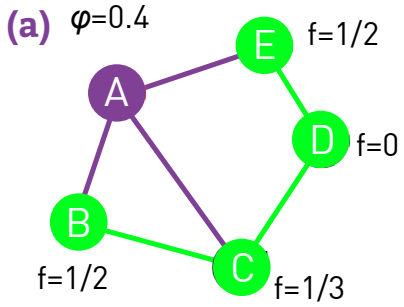


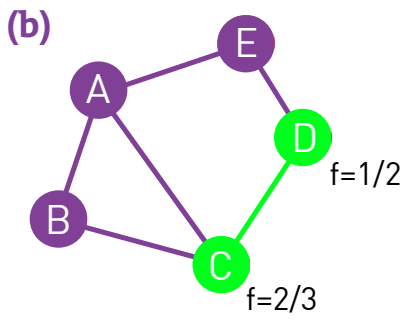
Erdos-Renyi network

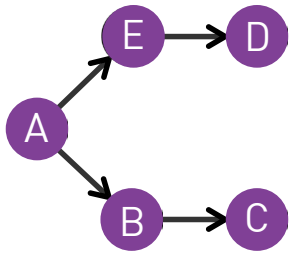
$$P(S) \sim S^{-3/2}$$

D. Watts, *PNAS* 99, 5766-5771 (2002)

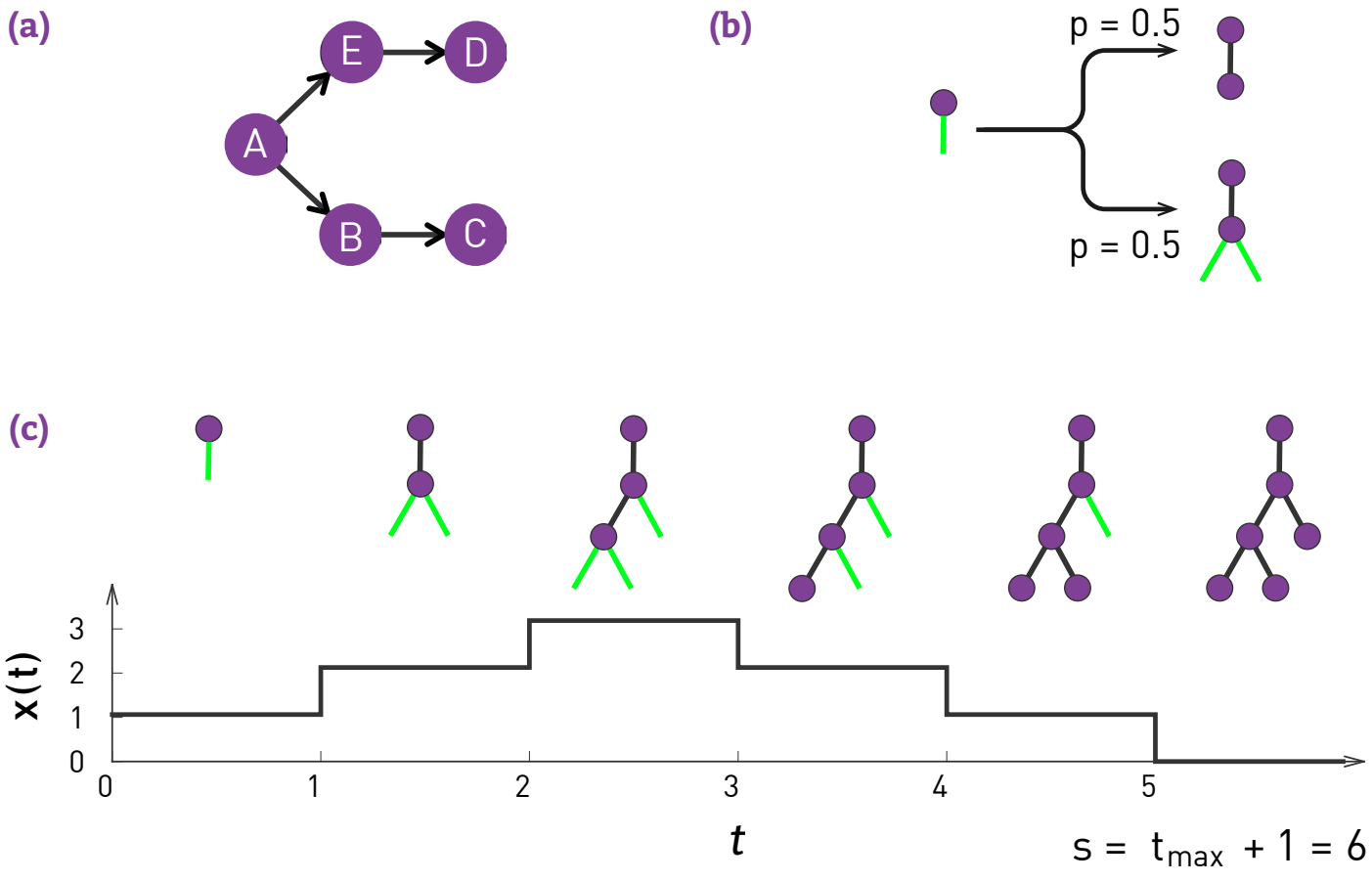
Section 8.6 Branching Model





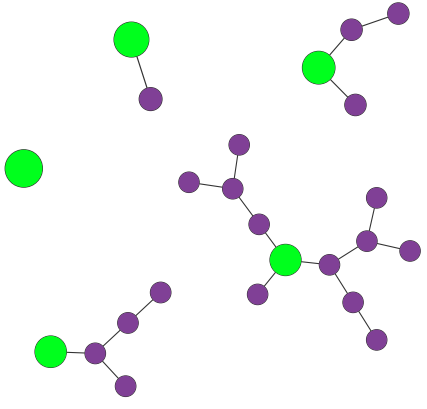


Section 8.6 Branching Model



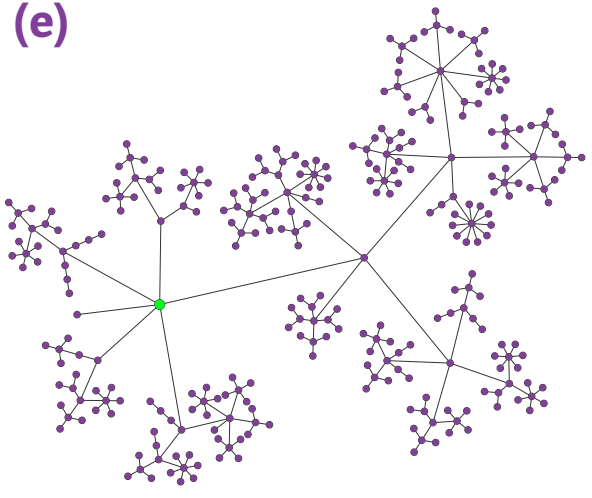
SUBCRITICAL

(d)



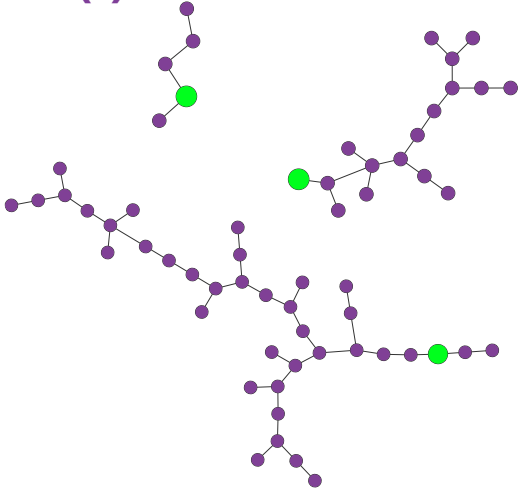
SUPERCRITICAL

(e)

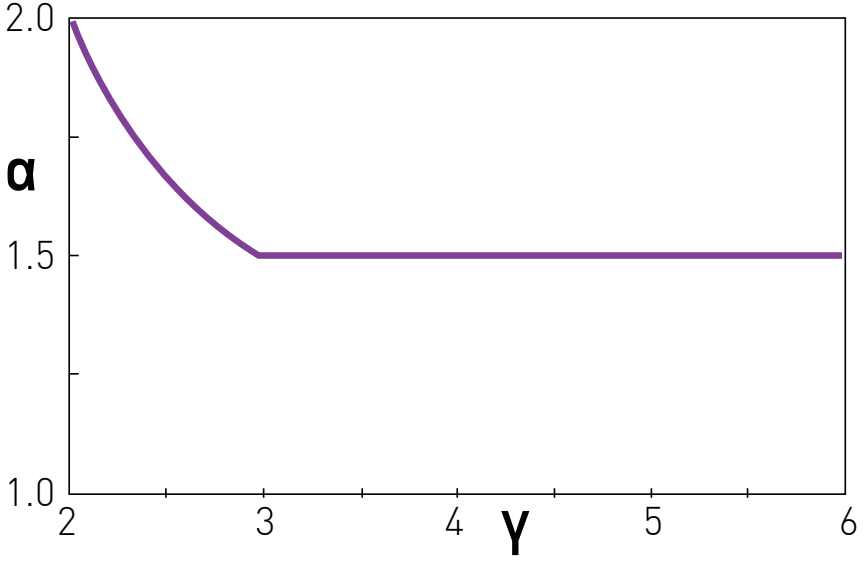


CRITICAL

(f)

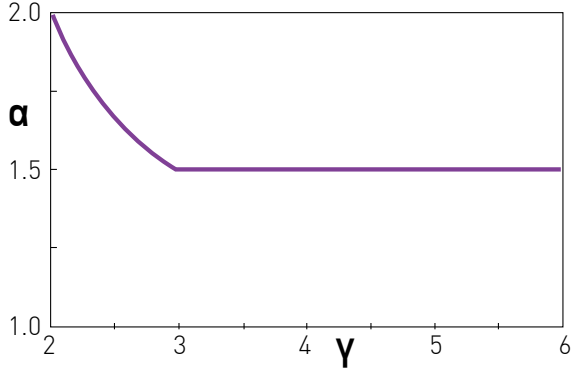


$$\alpha = \begin{cases} 3/2, & \gamma \geq 3 \\ \gamma/(\gamma-1), & 2 < \gamma < 3 \end{cases} .$$



Section 8.6 Branching Model

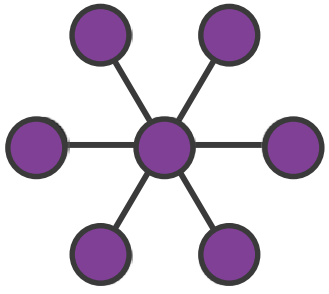
SOURCE	EXPONENT	CASCADE
Power grid (North America)	2.0	Power
Power grid (Sweden)	1.6	Energy
Power grid (Norway)	1.7	Power
Power grid (New Zealand)	1.6	Energy
Power grid (China)	1.8	Energy
Twitter Cascades	1.75	Retweets
Earthquakes	1.67	Seismic Wave



$$\alpha = \begin{cases} 3/2, & \gamma \geq 3 \\ \gamma/(\gamma-1), & 2 < \gamma < 3 \end{cases}.$$

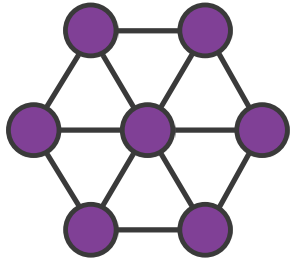
Building Robustness

(a)



$\langle k \rangle = 12/7$

(b)



$\langle k \rangle = 24/7$

Can we maximize the robustness of a network to both random failures and targeted attacks without changing the cost?

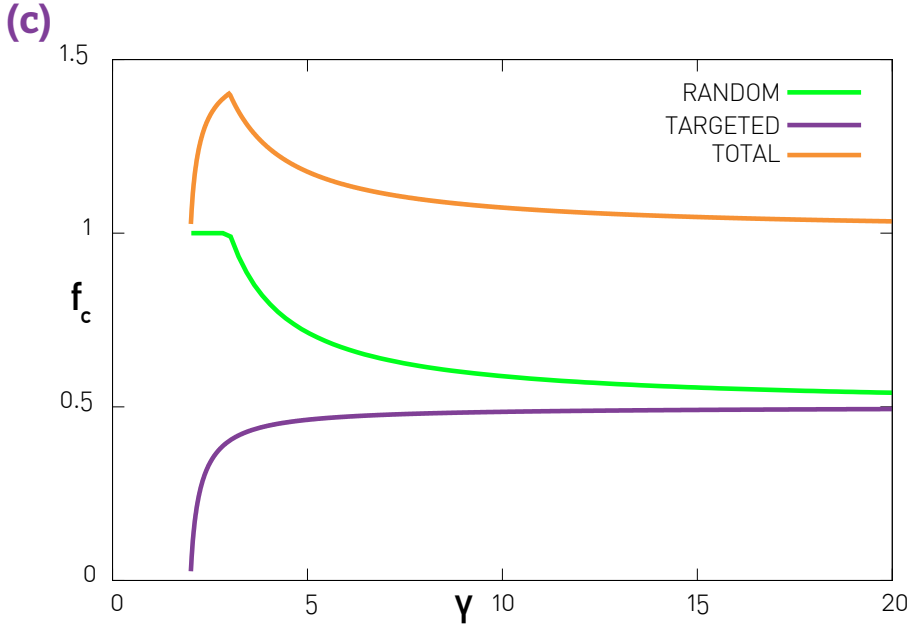
A network's robustness against random failures is captured by its percolation threshold f_c, which is the fraction of the nodes we must remove for the network to fall apart. To enhance a network's robustness we must increase f_c. According to (8.7) f_c depends only on $\langle k \rangle$ and $\langle k^2 \rangle$. Consequently the degree distribution which maximizes f_c needs to maximize $\langle k^2 \rangle$ if we wish to keep the cost $\langle k \rangle$ fixed. This is achieved by a bimodal distribution, corresponding to a network with only two kinds of nodes, with degrees k_{min} and k_{max} (Figure 8.23a,b).

$$f_c^{tot} = f_c^{rand} + f_c^{targ} .$$

$$f_c^{tot} = f_c^{rand} + f_c^{targ} .$$

$$p_k \equiv (1-r)\delta(k-k_{\min}) + r\delta(k-k_{\max}),$$

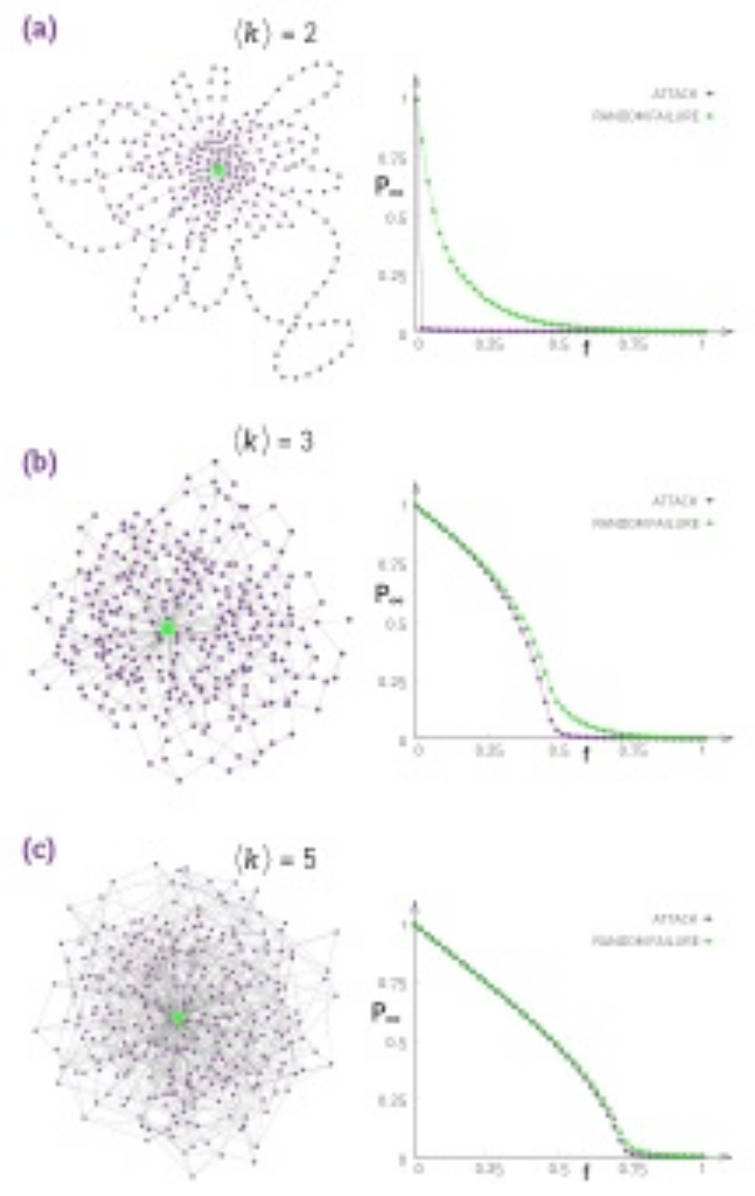
$$k_{\max} = AN^{2/3}.$$



$$f_c^{tot} = f_c^{rand} + f_c^{targ} .$$

$$p_k \equiv (1-r)\delta(k-k_{\min}) + r\delta(k-k_{\max}),$$

$$k_{\max} = AN^{2/3}.$$



Section 8.7 Halting Cascading Failures

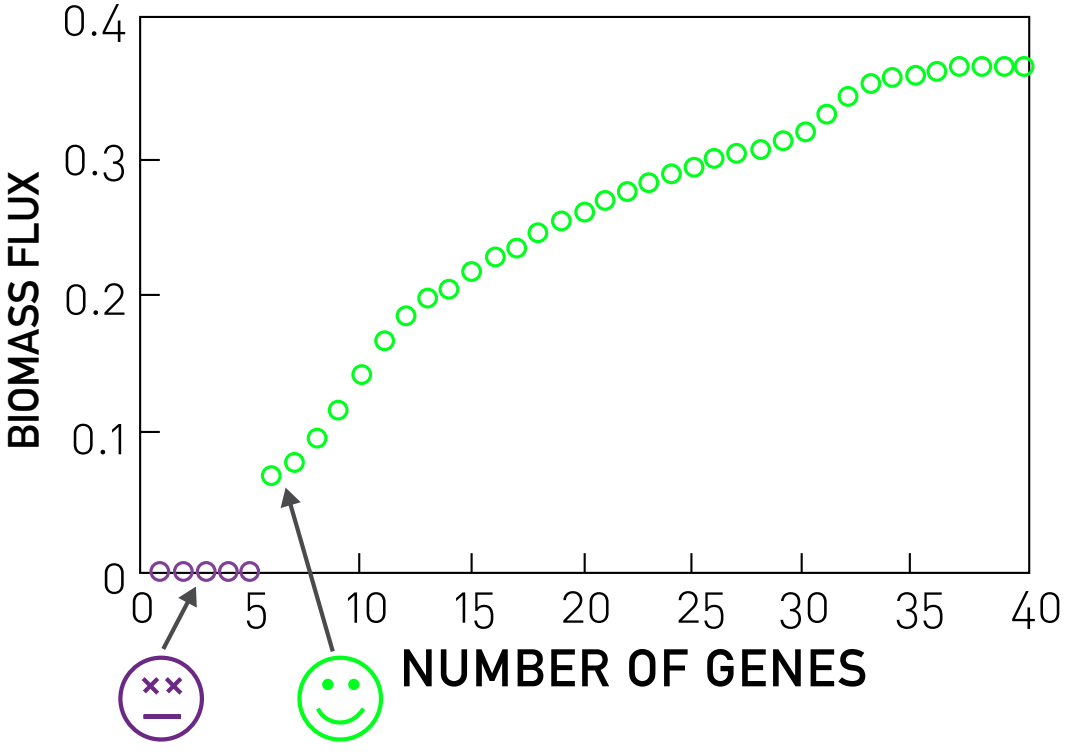
(i) *Initial failure* is the breakdown of the first node or link, representing the source of the subsequent cascade.

(ii) *Propagation* is when the initial failure induces the failure of additional nodes and starts cascading through the network.

Simulations indicate that to limit the size of the cascades we must remove nodes with small loads and links with large excess load in the vicinity of the initial failure. The mechanism is similar to the method used by firefighters, who set a controlled fire in the fire- line to consume the fuel in the path of a wildfire.

Section 8.7

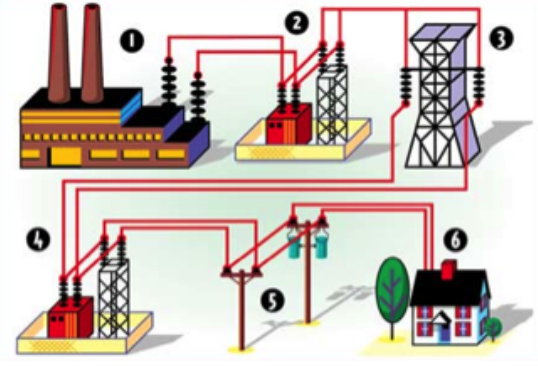
Lazarus Effect



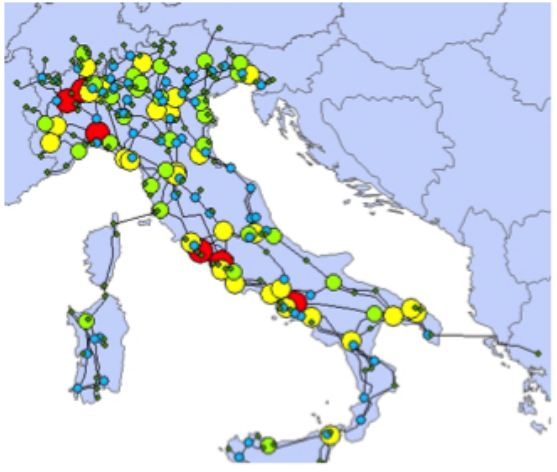
Section 8.7

Case Study: Power Grid

(a)

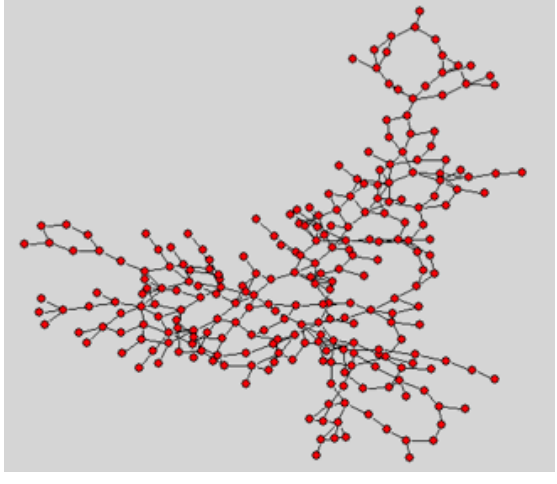


(b)

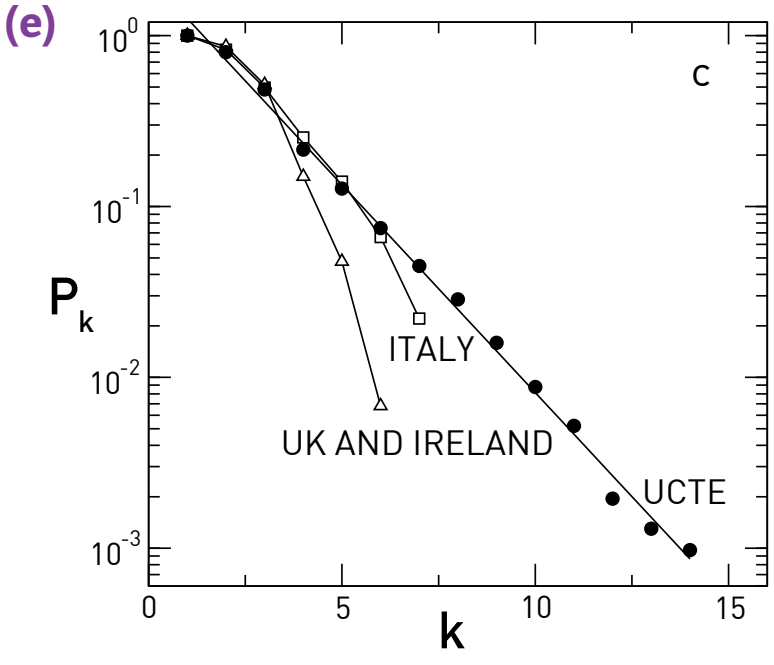


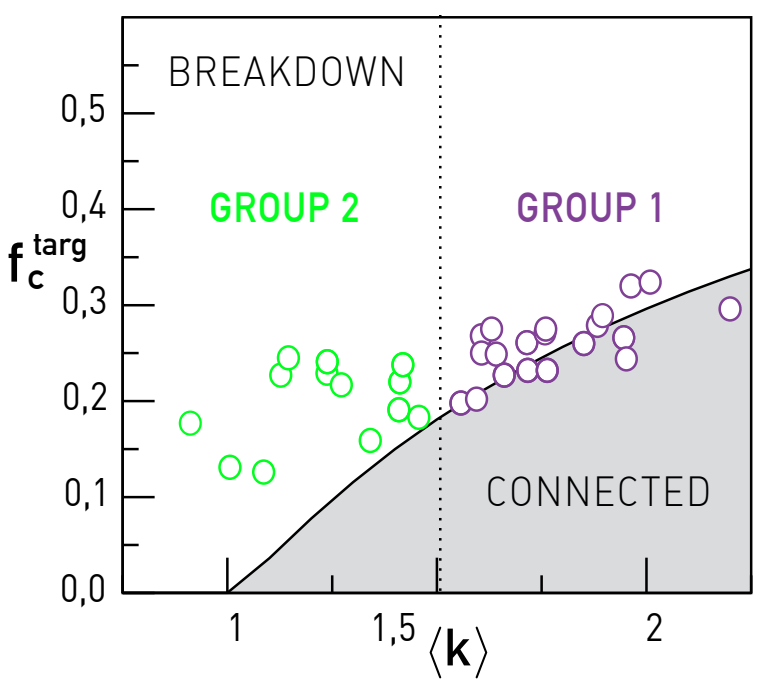
(c)

(d)



Case Study: Power Grid

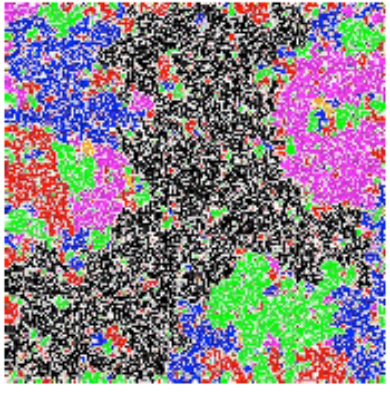




$$p_k = \frac{e^{-k/\langle k \rangle}}{\langle k \rangle}$$

Group 2: these networks are more robust to attacks than expected based on their degree distribution.

Section 8.8 Summary



PERCOLATION

ACHILLES' HEEL

SHLOMO HAVLIN

Mathematicians **Simon Broadbent** and **John Hammersley** introduce percolation and formalize many of its mathematical concepts [5]. The theory rose to prominence in the 1960s and 70s, finding applications from oil exploration to superconductivity.

Paul Baran explores the vulnerability of communication networks to Soviet nuclear attacks, concluding that they are too centralized to be viable under attack. Proposes instead a mesh-like network architecture (BOX 8.2).

Albert, Jeong and **Barabási** study the error and attack tolerance of complex networks, discovering their joint robustness to failures and fragility to attacks.

Shlomo Havlin and his collaborators establish a formal link between network robustness and percolation theory, showing that the percolation threshold of a scale-free network is determined by the first two moments of the degree distribution.

Section 8.8

Summary

AT A GLANCE: NETWORK ROBUSTNESS

Malloy-Reed criteria:

A giant component exists if

$$\frac{\langle k^2 \rangle}{\langle k \rangle} > 2$$

Random failures:

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

Random Network: $f_c^{ER} = 1 - \frac{1}{\langle k \rangle}$

Enhanced robustness: $f_c > f_c^{ER}$

Attacks:

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

Cascading failures:

$$p(s) \sim s^{-\alpha}$$

$$\alpha = \begin{cases} 3/2 & \gamma > 3 \\ \frac{\gamma}{\gamma - 1} & 2 < \gamma < 3 \end{cases}$$

Robustness

A system is robust if it can maintain its basic functions in the presence of internal and external errors. In a network context robustness refers to the system's ability to carry out its basic functions even when some of its nodes and links may be missing.

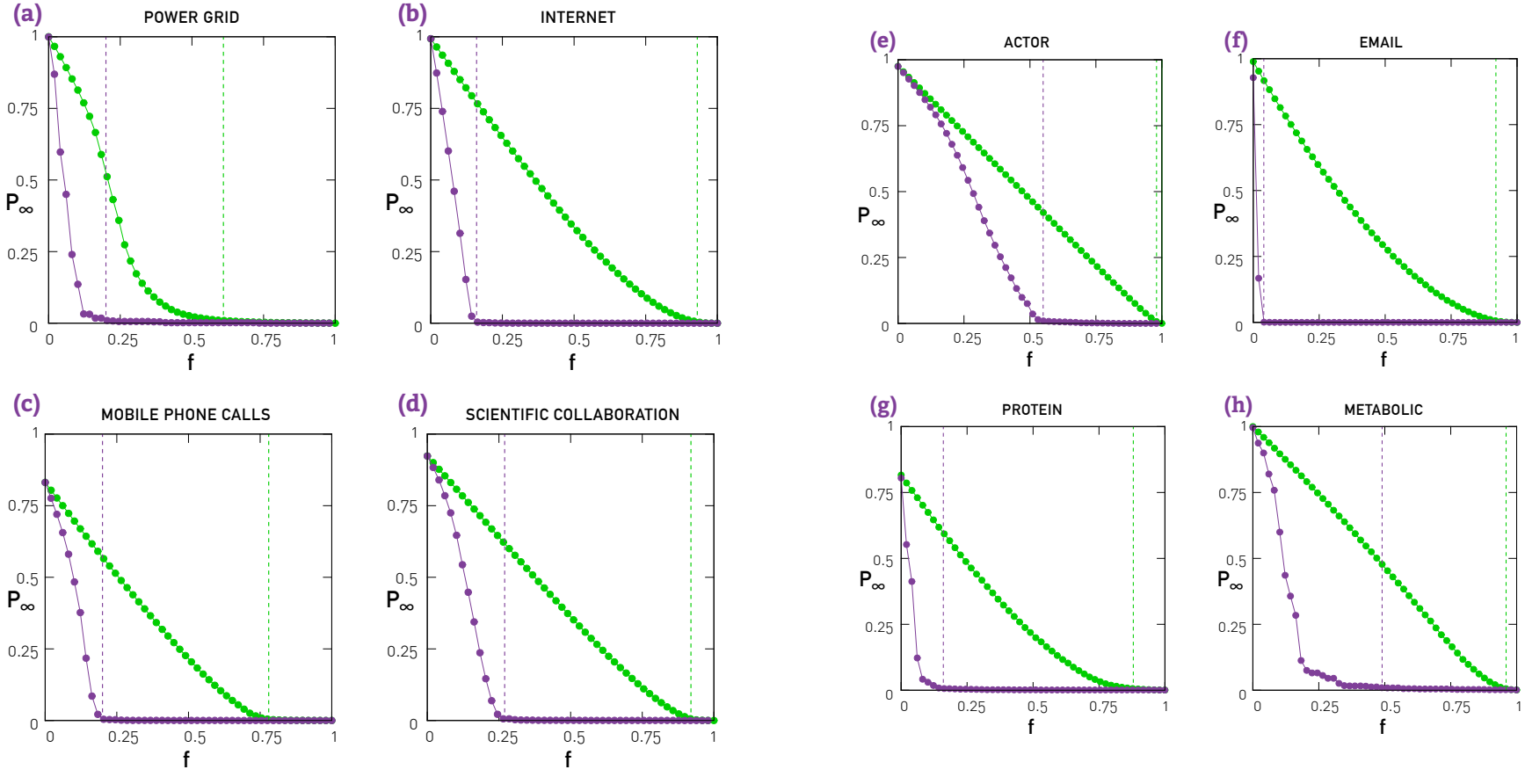
Resilience

A system is resilient if it can adapt to internal and external errors by changing its mode of operation, without losing its ability to function. Hence resilience is a dynamical property that requires a shift in the system's core activities.

Redundancy

Redundancy implies the presence of parallel components and functions that, if needed, can replace a missing component or funciton. Networks show considerable redundancy in their ability to navigate information between two nodes, thanks to the multiple independent paths between most node pairs.

Section 8.8 Achilles' Heel



The end