Robustness

Vander Luis de Souza Freitas
vander.freitas@ufop.edu.br

Agenda

- Last class we discussed:
  - Degree correlations
  - Assortativity
  - Centrality measures

Agenda

- Today:
  - Discussion about the homework
  - Network Robustness
  - Cascading failures
  - Building robustness

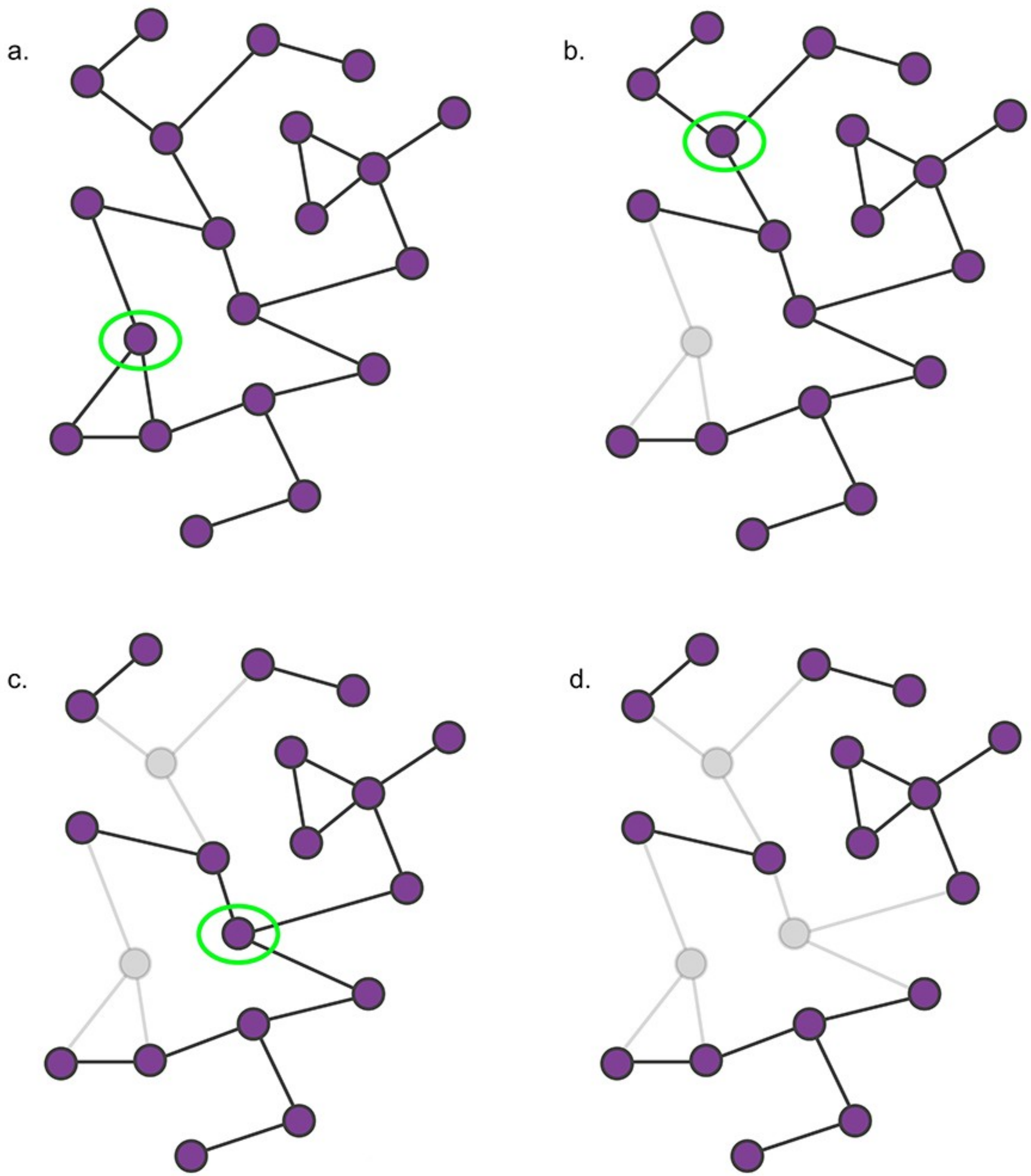
Discussion

Network robustness

"Robust" comes from the latin *Quercus Robur*, meaning oak, the symbol of strength and longevity in the ancient world.

http://networksciencebook.com/chapter/8

Network robustness



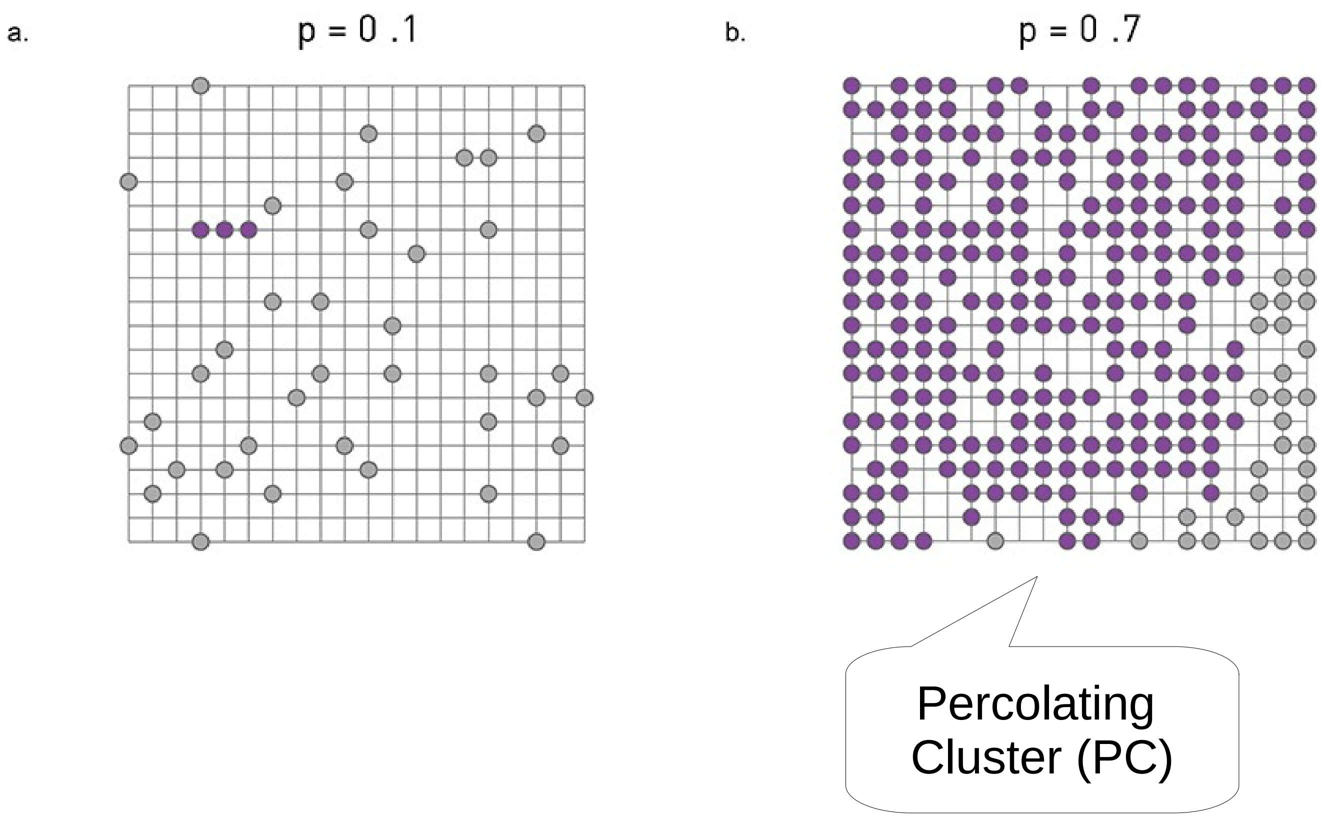
http://networksciencebook.com/chapter/8

Percolation theory

Percolation theory is a highly developed subfield of statistical physics and mathematics. Typical problem:

One places pebbles with probability *p* at each intersection:

- What is the expected size of the largest cluster?
- What is the average cluster size?



http://networksciencebook.com/chapter/8

Percolation theory

Average cluster size:

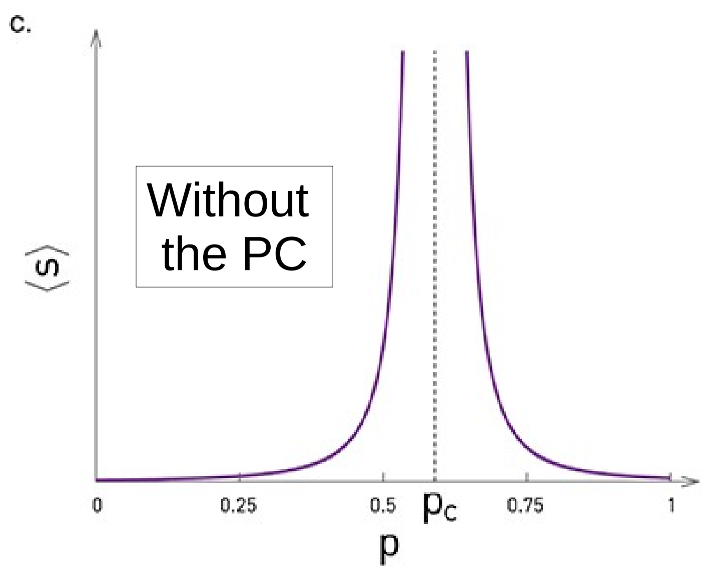
$$\langle s \rangle \sim |p - p_c|^{-\gamma_p}$$

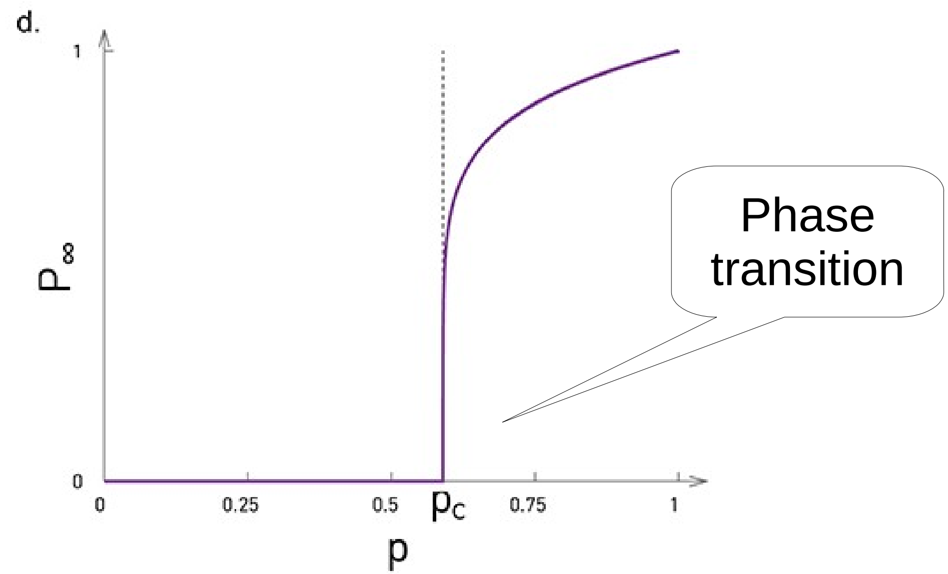
The average cluster size diverges as we approach p_c (PC not included).
The probability that a randomly chosen pebble belongs to the largest cluster is:

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

and drops to zero when p decreases towards p_c.
Correlation length ξ: the distance between two pebbles that belong to the same cluster is

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



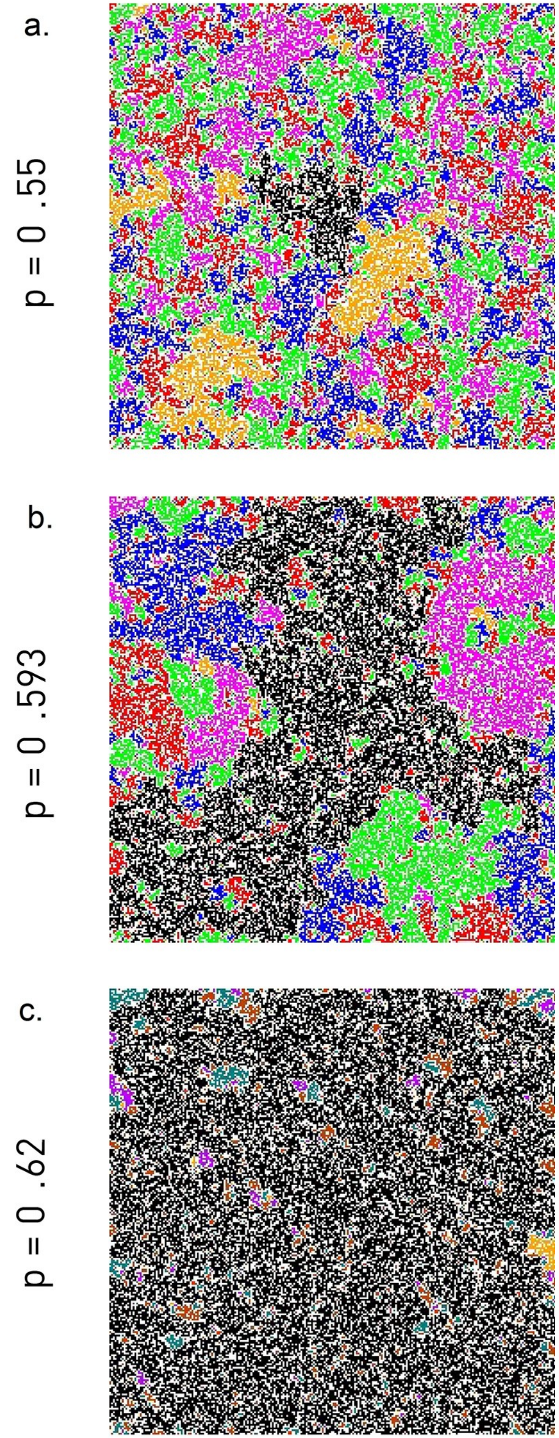


http://networksciencebook.com/chapter/8

Example - from forest fires to percolation theory:

Example - *from forest fires to percolation theory*:

- Each pebble is a tree.
- If the fire starts at a random tree, is it possible to burn the entire forest? It depends on *p*.



http://networksciencebook.com/chapter/8

Inverse percolation transition and robustness

Network Breakdown as *Inverse Percolation*:

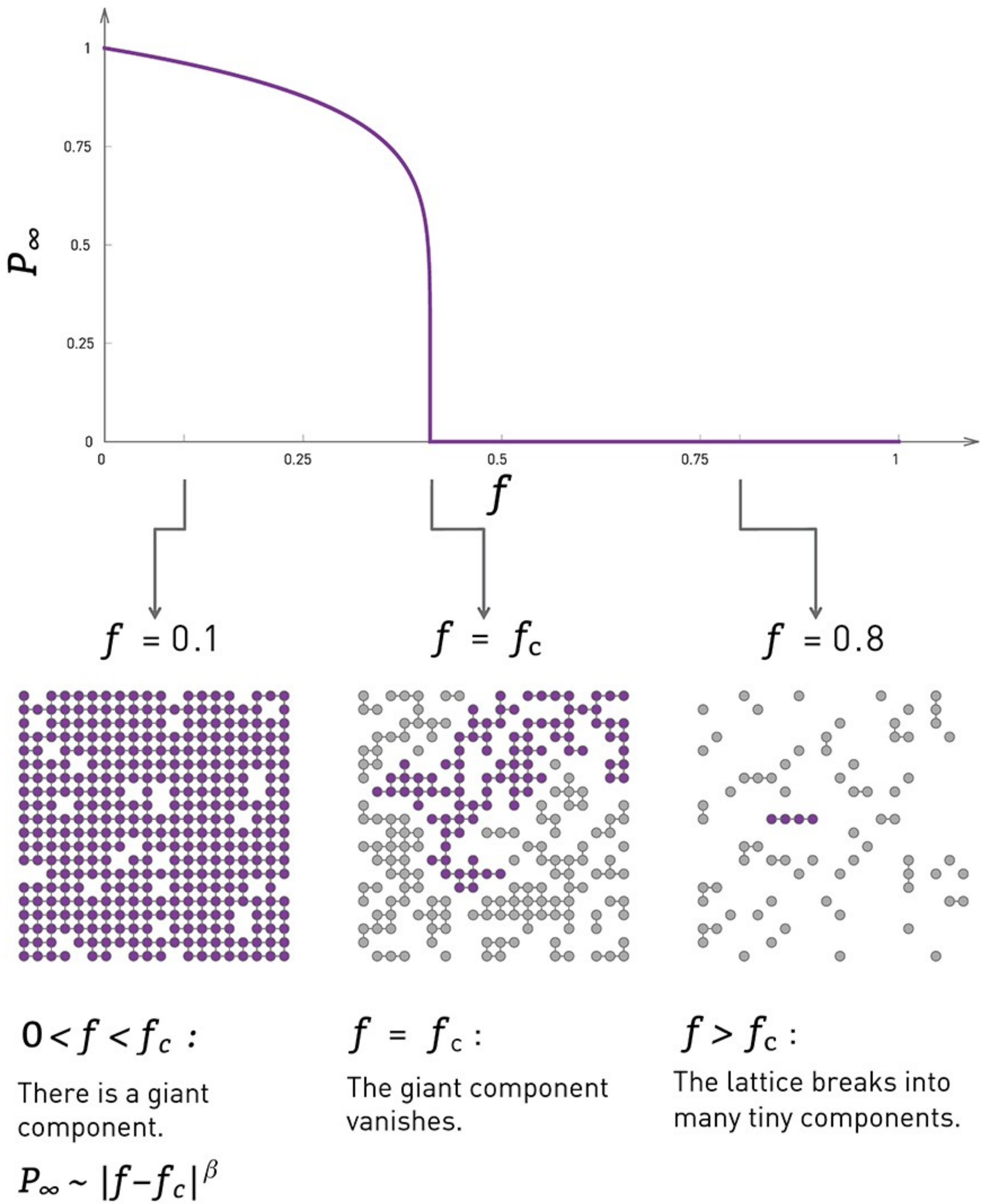
One starts with a square lattice and removes a fraction *f* of nodes. The size of the giant component *decreases* with increasing *f*, following:

$$f = 1 - p$$

This holds for random networks

P_∞ is the normalized size of the giant component and also the probability that a randomly chosen pebble belongs to it.

http://networksciencebook.com/chapter/8

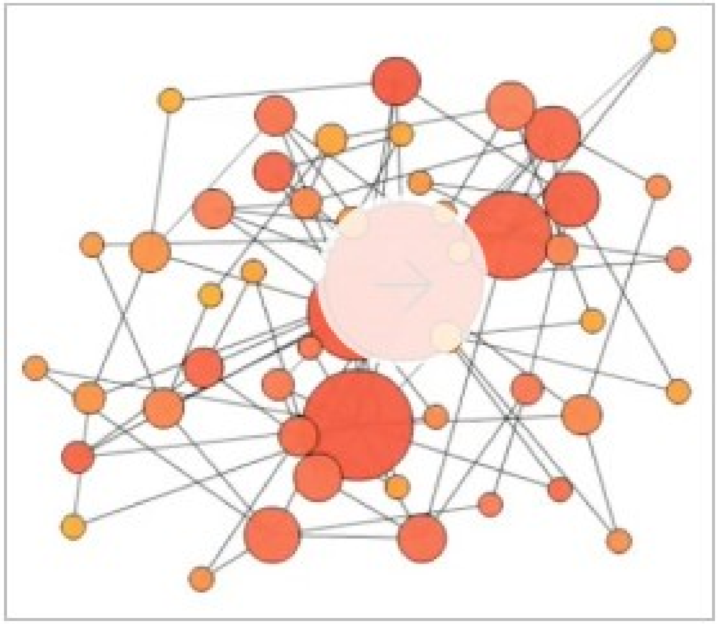


Robustness of scale-free networks

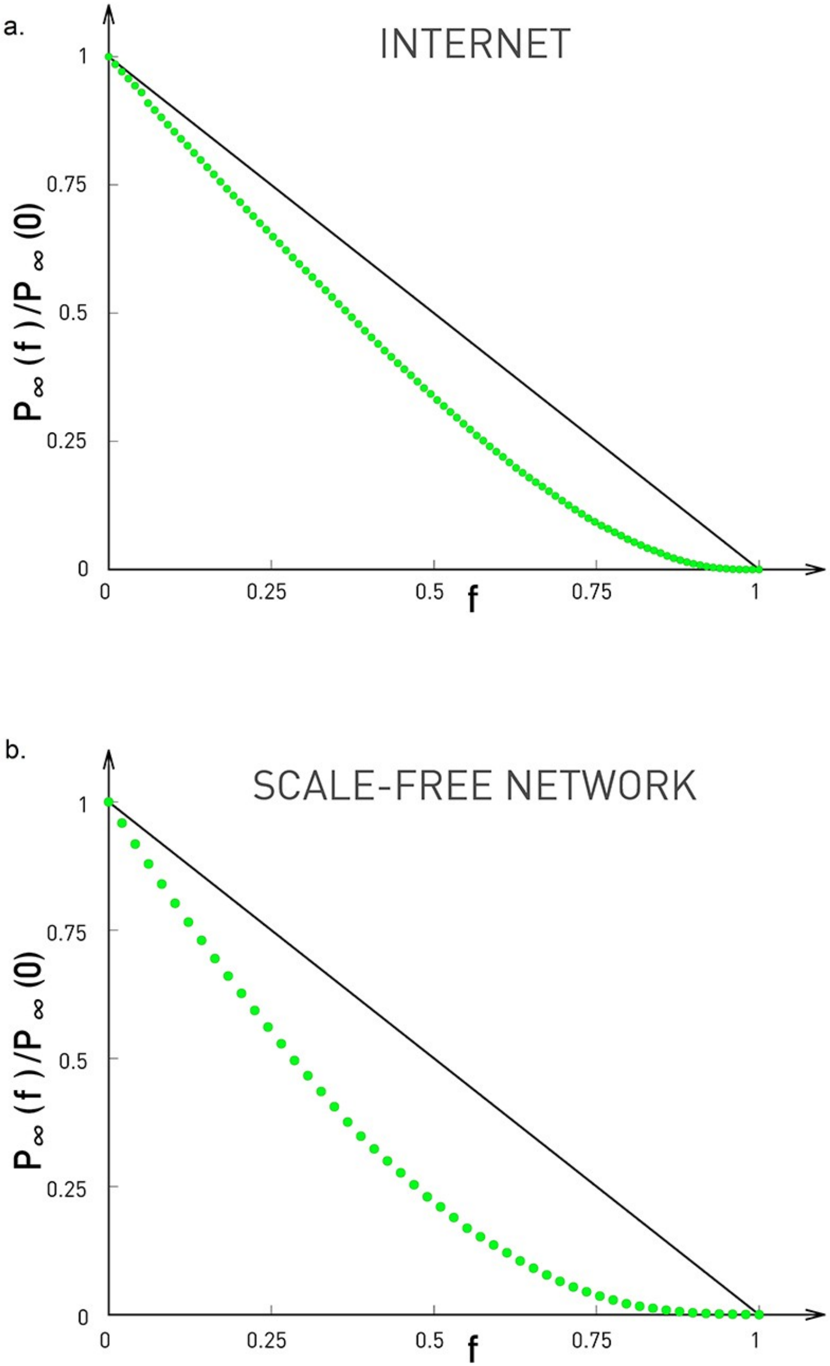
Unlike in random networks, the size of the giant component decreases gradually in scale-free networks, vanishing only in the vicinity of $f = 1$.

Video:

http://networksciencebook.com/images/ch-08/video-8-1.webm



http://networksciencebook.com/chapter/8



Molloy-Reed Criterion

A randomly wired network has a giant component if

This means that every node in the giant component must be connected to at least two other nodes

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

Valid for any degree distribution

Poisson Std. dev.

Binomial Std. dev.

$$\sqrt{\langle k \rangle} = \sqrt{\langle k^2 \rangle - \langle k \rangle^2}$$

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

Example with a random network:
In ER networks $\langle k^2 \rangle = \langle k \rangle (1 + \langle k \rangle)$. Thus

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

which agrees with the phase transition for the existence of a giant component in random networks.

http://networksciencebook.com/chapter/8

Critical Threshold f_c

The critical threshold for a network with arbitrary degree distribution depends only on $\langle k \rangle$ and $\langle k^2 \rangle$ as follows:

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

For an ER network:

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

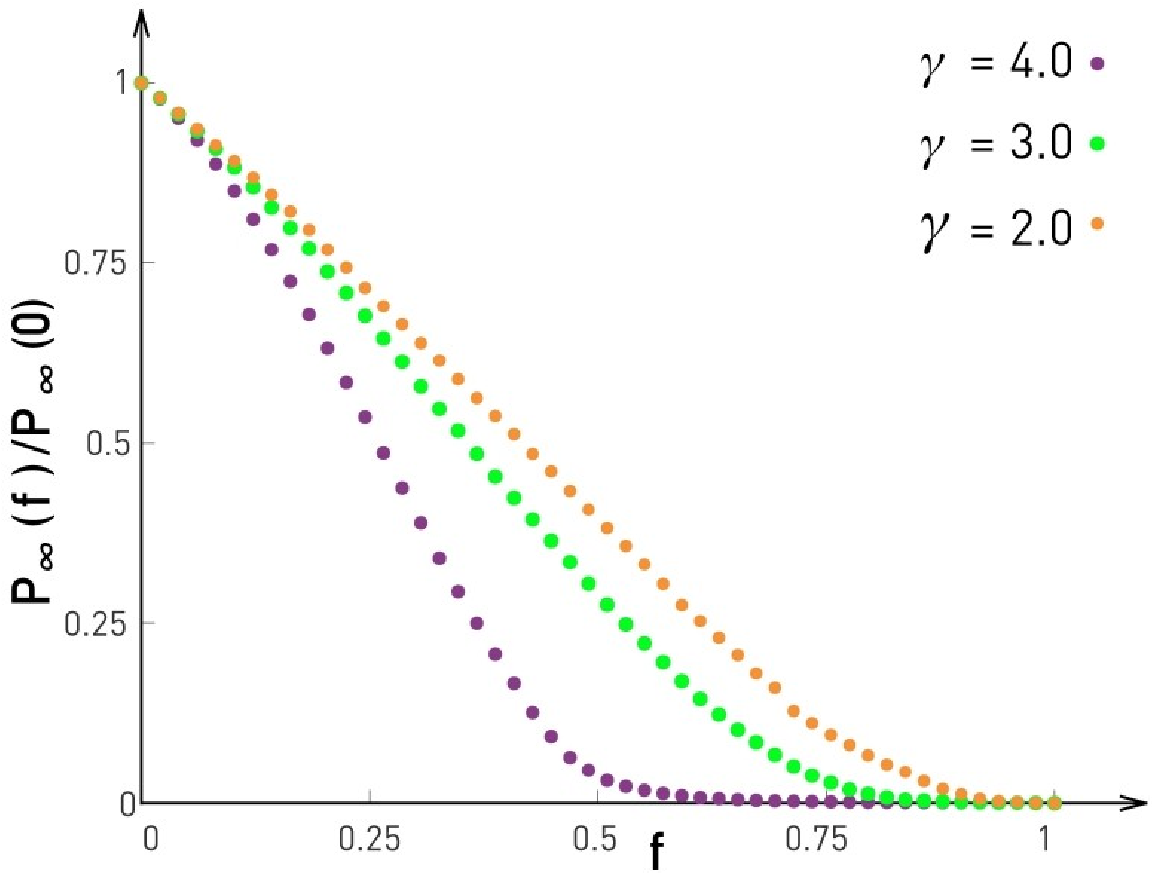
i.e. the denser the network the higher is its f_c.

http://networksciencebook.com/chapter/8

Robustness of scale-free networks

For scale-free networks with $\gamma < 3$, $\langle k^2 \rangle \to \infty$ therefore $f_c = 1$. In more details:

$$f_c = \begin{cases} 1 - \frac{1}{\frac{\gamma-2}{3-\gamma} k_{min}^{\gamma-2} k_{max}^{3-\gamma} - 1}, & 2 < \gamma < 3 \\ 1 - \frac{1}{\frac{\gamma-2}{\gamma-3} k_{min} - 1}, & \gamma > 3 \end{cases}$$



http://networksciencebook.com/chapter/8

Robustness of finite size networks

Most real networks have $f_c > f_c^{ER}$, since $\langle k^2 \rangle$ is usually higher than the random case: *enhanced robustness*.

Exp. degree distrib.

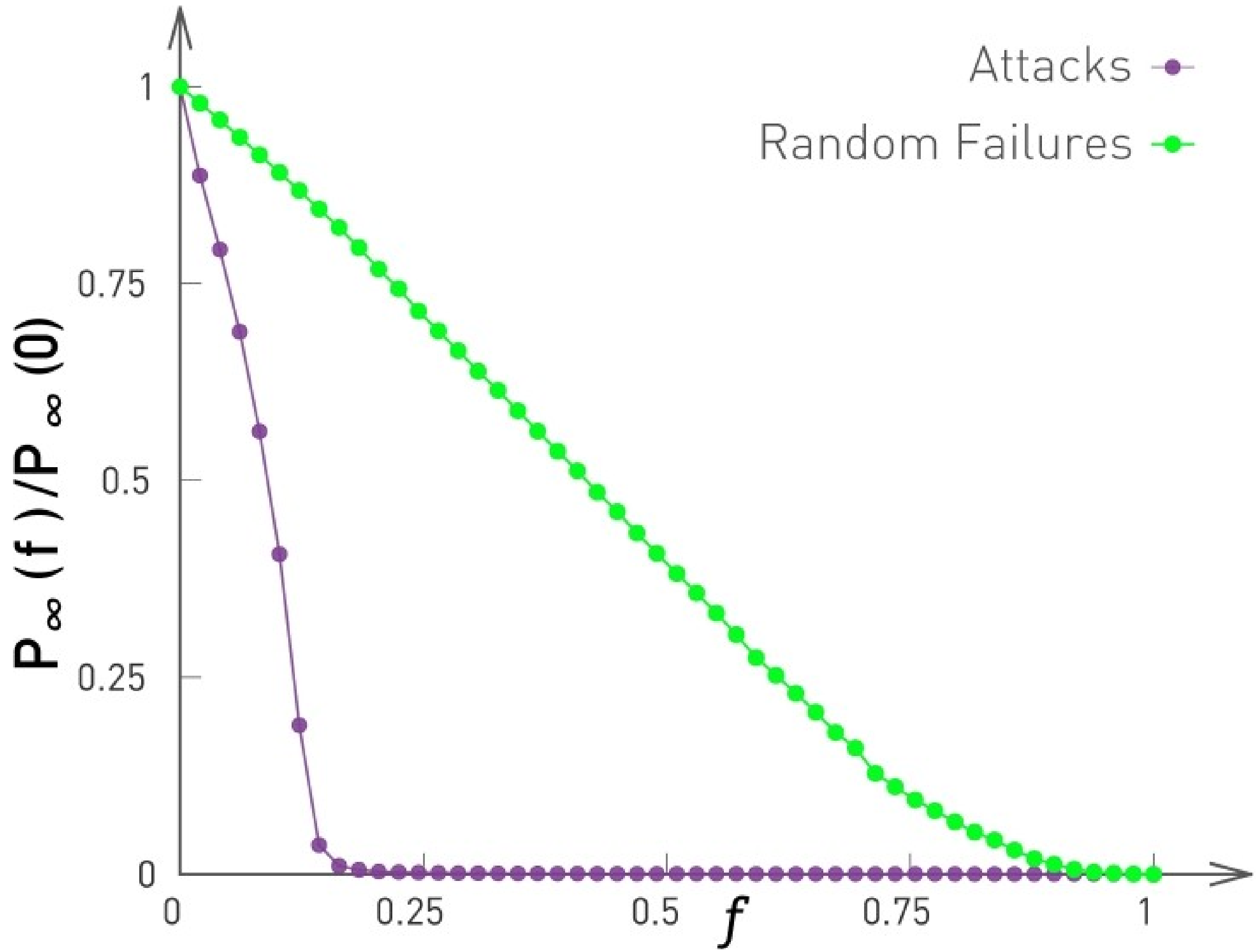
High $\langle k \rangle$

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 Calls	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
Protein Interactions	0.88	0.66	0.06

http://networksciencebook.com/chapter/8

Attack tolerance

What if we do not remove the nodes randomly, but go after the hubs?



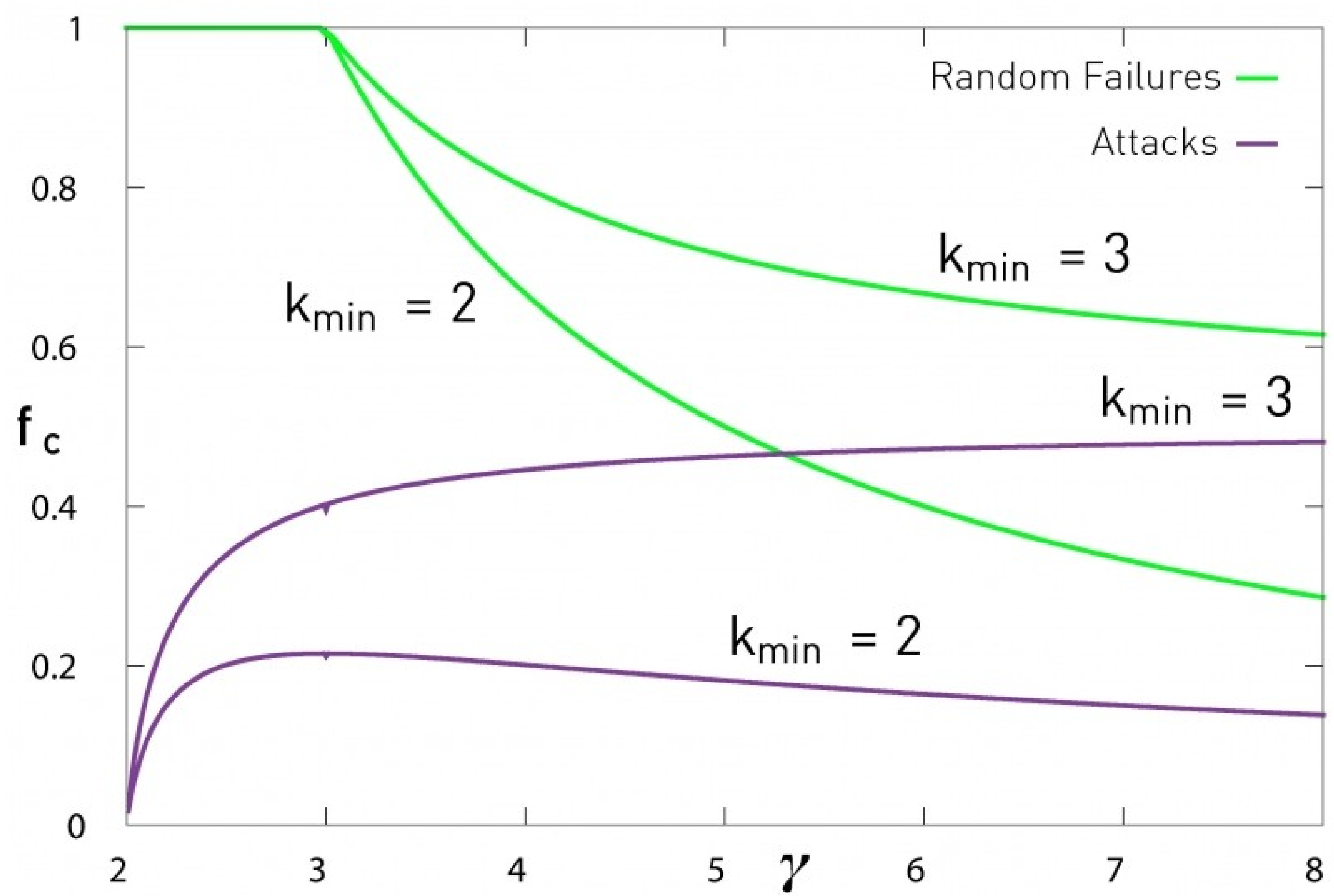
Video: http://networksciencebook.com/images/ch-08/video-8-2.webm

http://networksciencebook.com/chapter/8

Attack tolerance

The critical threshold for attacks on a scale-free network is the solution of

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



Interesting ref: https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.86.3682

http://networksciencebook.com/chapter/8

Attack tolerance

Preliminary conclusions:

- Attacking airports at random would not destroy the existing flight mesh; Attacking the most connected airports like GRU would lead to chaos.
- Attacking a random router would not break the Internet; Attacking the most connected ones would cause serious problems.

Therefore, random failures and targeted attacks usually produce different critical thresholds f_c .

http://networksciencebook.com/chapter/8

Cascading failures

The failure of a node can induce the failure of the nodes connected to it:

- Blackouts (Power Grid)
- Denial of Service Attacks (Internet): a failed router increases traffic on other routers.
- Financial crises

The failure starts somewhere in the network, and spreads along the links, inducing additional failures.

http://networksciencebook.com/chapter/8

Cascading failures

Blackouts: The probability distribution of energy **un**served in all North America blackouts between 1984 and 1998 are usually approximated by Electrical engineers with the power law

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

Different events with similar exponents

in which α is the **avalanche exponent**.

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

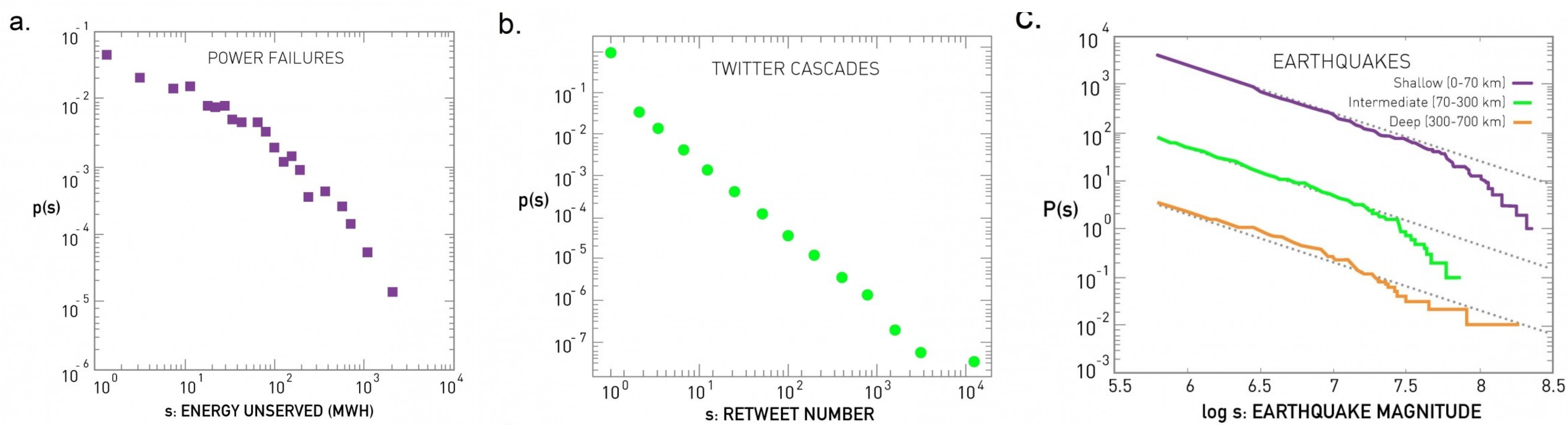
http://networksciencebook.com/chapter/8

Cascading failures

Blackouts: The probability distribution of energy **un**served in all North America blackouts between 1984 and 1998 are usually approximated by Electrical engineers with the power law

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

in which α is the **avalanche exponent**.



$\alpha \approx 1.75$ $\alpha \approx 1.67$

http://networksciencebook.com/chapter/8

Cascading failures

U.S. Northeast blackout of 2003: 10 million people without electricity in Ontario (CA) and 45 million in eight U.S. states.

http://networksciencebook.com/chapter/8

Cascading failures

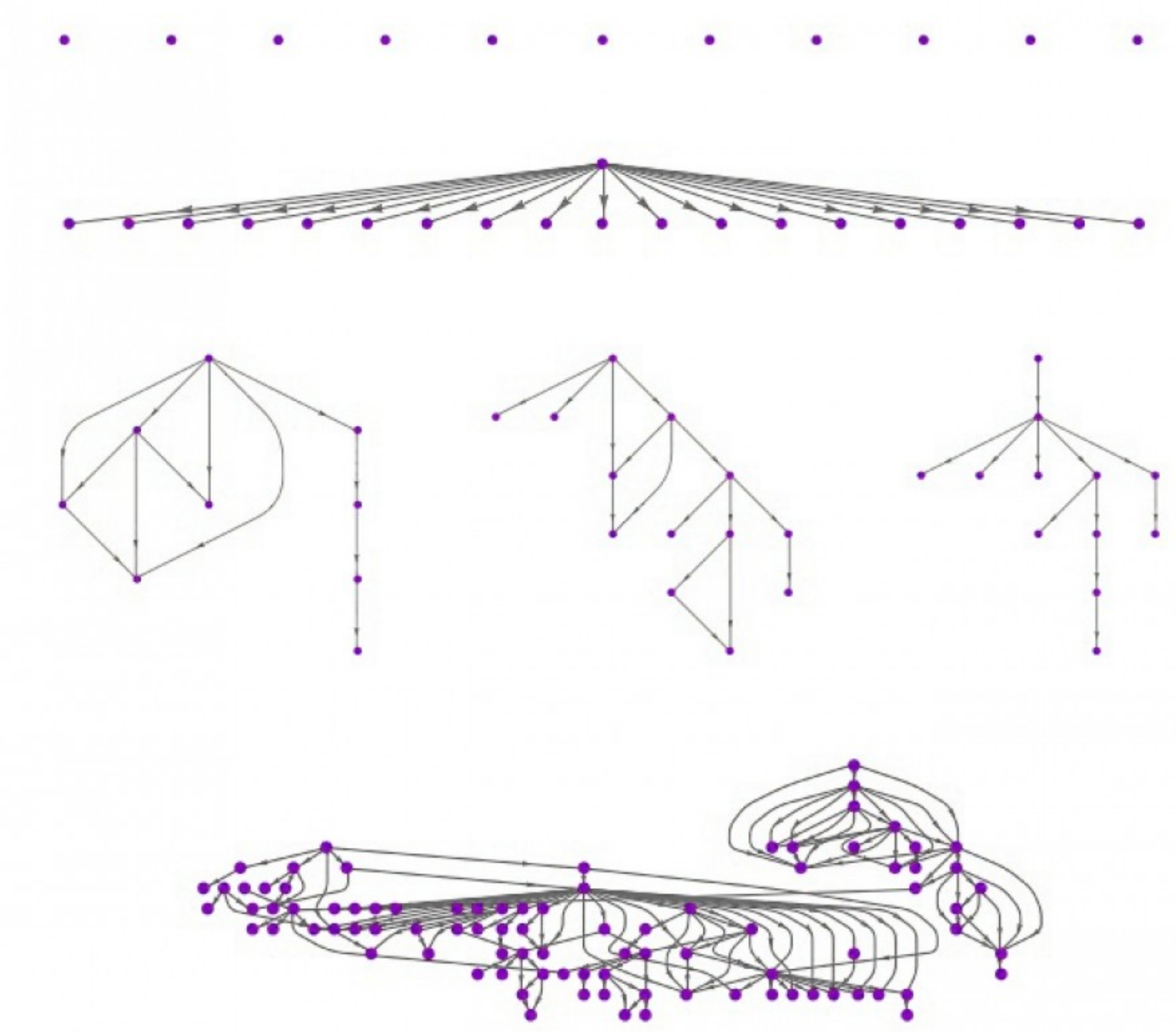
Information cascades:
Example with retweets

Avalanche exponent:

$$\alpha \approx 1.75$$

Average cascade size:

$$\langle s \rangle = 1.14$$



http://networksciencebook.com/chapter/8

Cascading failures

Other examples:

- Bad weather or mechanical failures can cascade through airline schedules;
- The disappearance of a species can cascade through the food web of an ecosystem;
- The shortage of a particular component can cripple supply chains.

Cascading sizes are well approximated with a power law, implying that most cascades are too small to be noticed, and a few are huge.

Modeling cascading failures

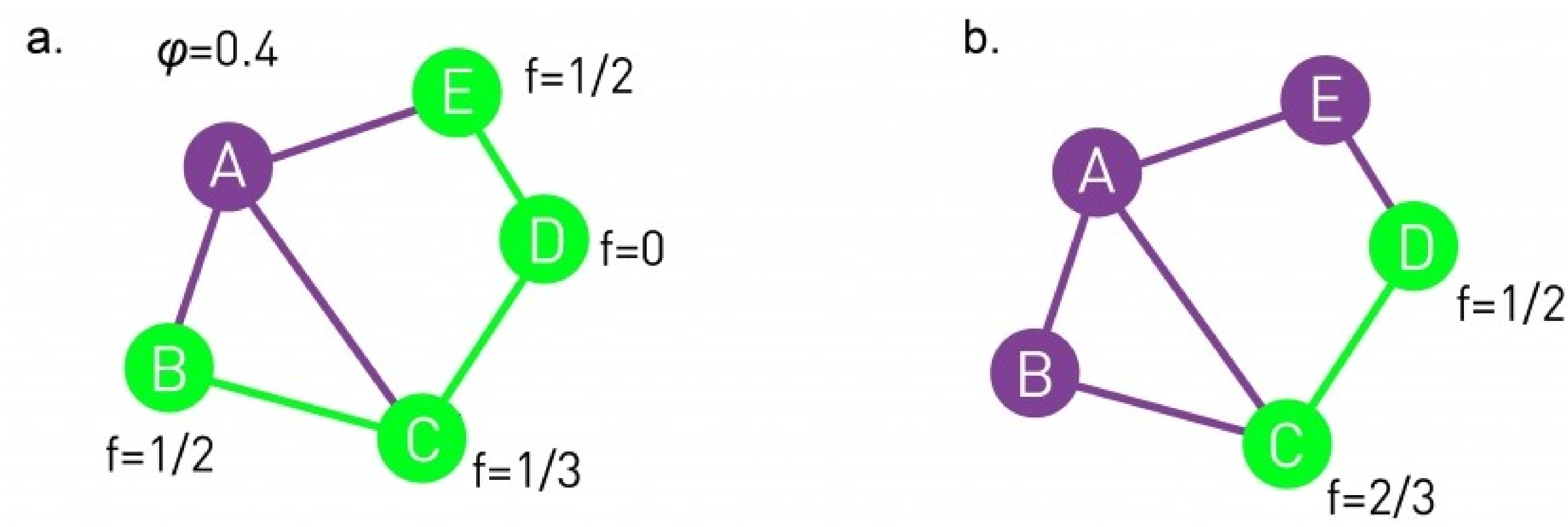
Three key ingredients:

- There is some flow over the network (current, information, etc).
- Each component has a local breakdown rule that determines when it contributes to a cascade.
- Each system has a mechanism to redistribute the traffic to other nodes upon the failure or the activation of a component.

Modeling cascading failures

Failure propagation model

- Nodes have state 0 (active or healthy) or 1 (inactive or failed), and the network has a breakdown threshold φ.
- One node starts with state 1 and the others with 0.
- A node *i* is randomly selected. If at least a fraction φ of its k_i neighbors are in state 1, it flips to 1 as well.



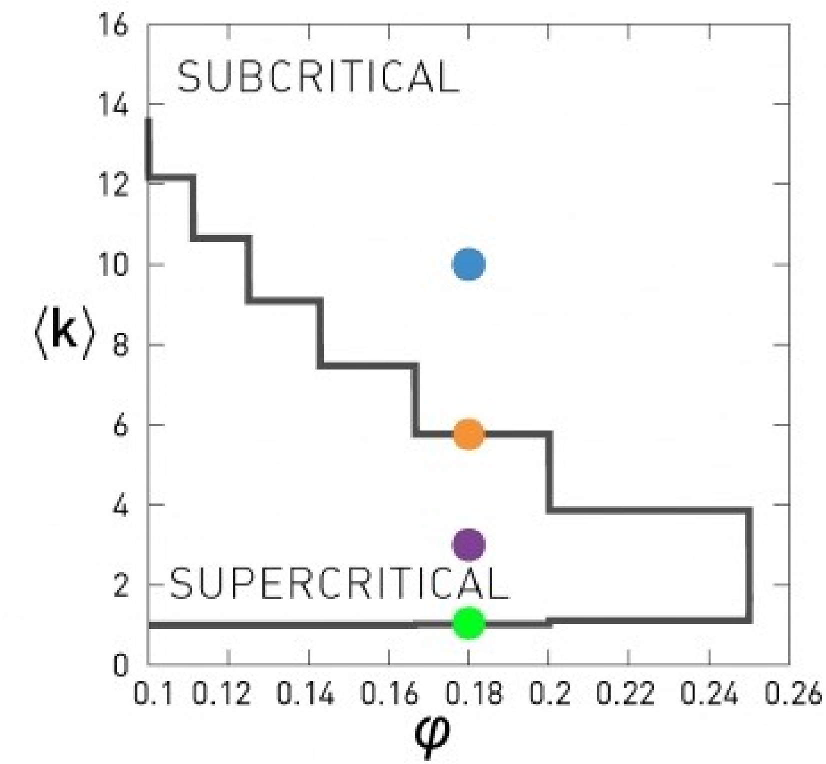
What happens if the failure started at B instead?

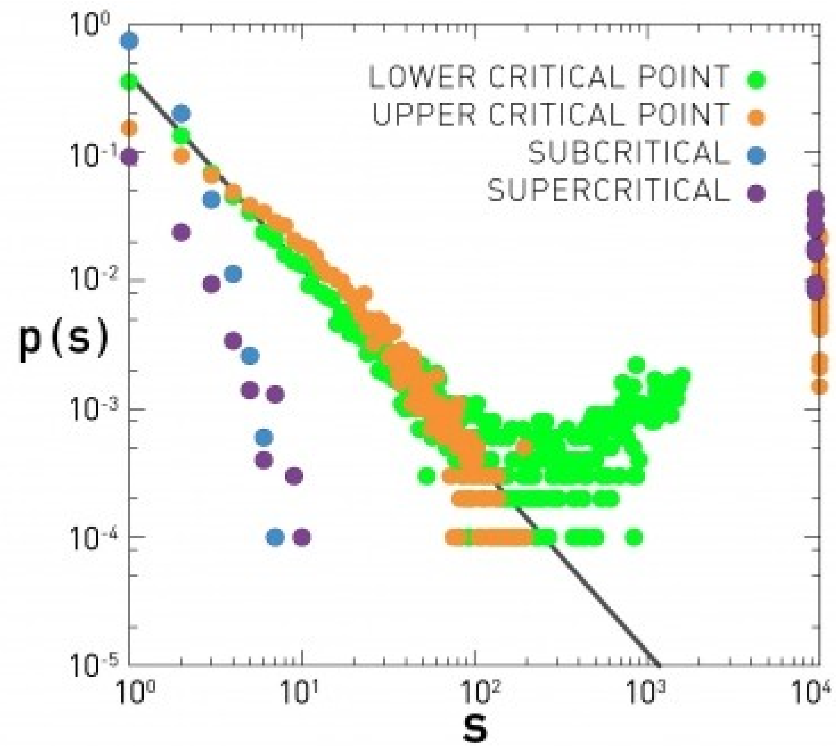
http://networksciencebook.com/chapter/8

Modeling cascading failures

Failure propagation model

- Subcritical regime (high $\langle k \rangle$): cascades die out quickly.
- Supercritical regime (small $\langle k \rangle$): cascades reach a global scale.
- Critical regime: avalanche sizes *s* follow a power law with $\alpha = 3/2$.





Random network:
$N = 10,000, \varphi = 0.18$

Green: $\langle k \rangle = 1.05$
Orange: $\langle k \rangle = 5.76$

Purple: $\langle k \rangle = 3$
Blue: $\langle k \rangle = 10$

http://networksciencebook.com/chapter/8

Modeling cascading failures

Branching model

- The cascading starts at the *root of the tree*.
- Each node produces k offsprings, where k is selected from a p_k distribution.
- If the node selects $k = 0$, that branch dies out.
- If it selects $k > 0$, the node will have k new active sites.
- The size of an avalanche corresponds to the size of the tree when all active sites died out.

http://networksciencebook.com/chapter/8

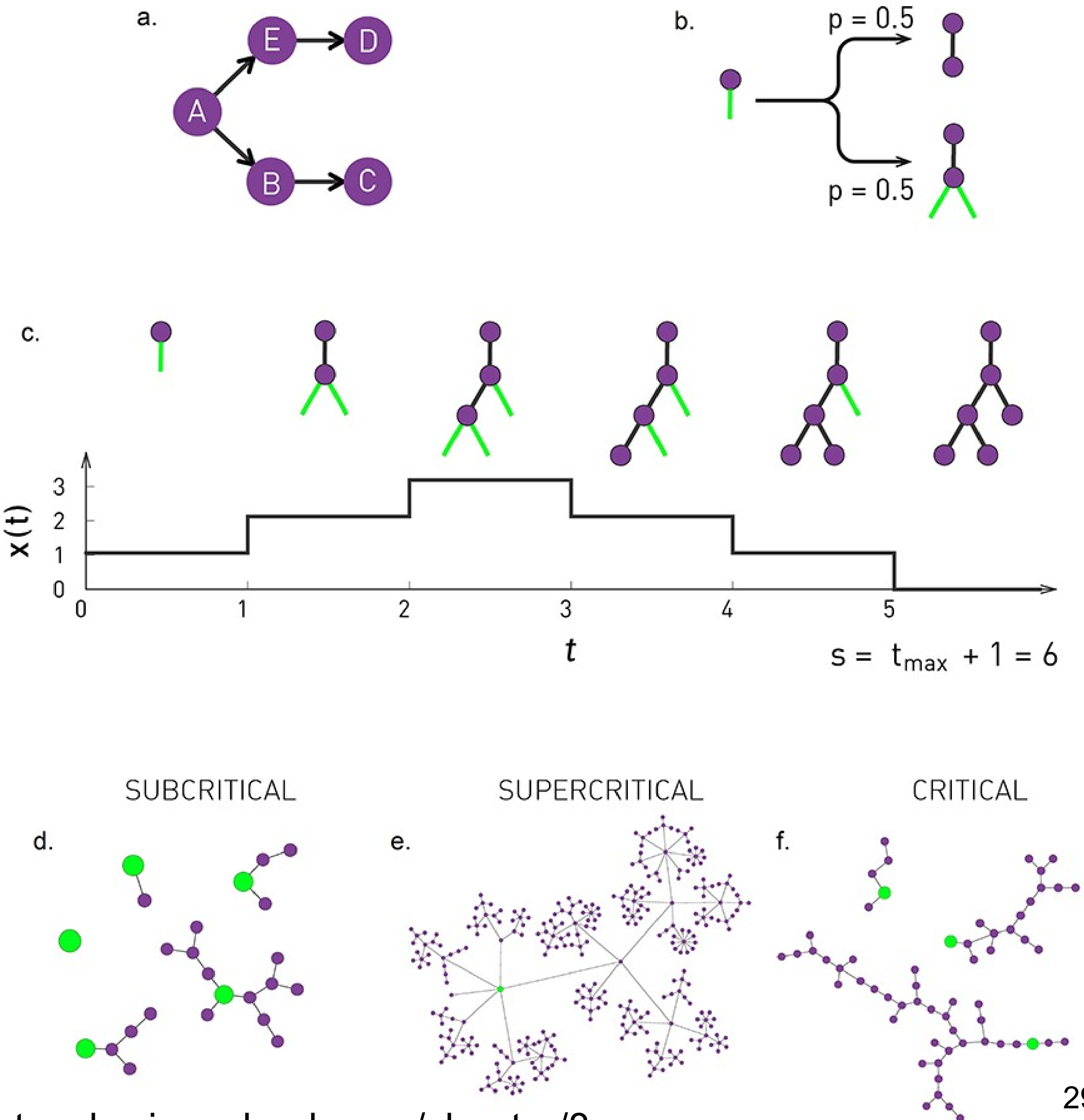
Modeling cascading failures

Branching model

Subcritical regime
$\langle k \rangle < 1$

Supercritical regime
$\langle k \rangle > 1$

Critical regime
$\langle k \rangle = 1$



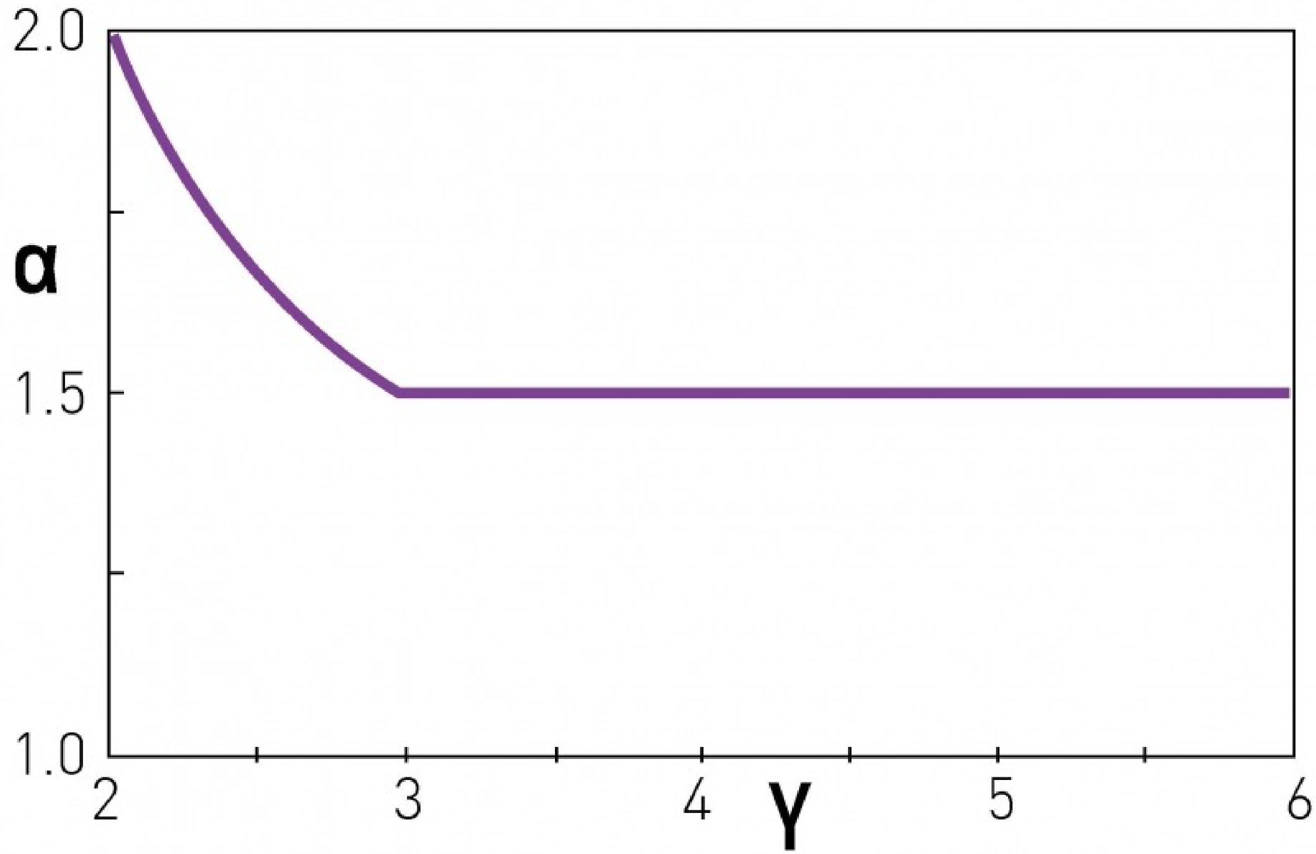
http://networksciencebook.com/chapter/8

Modeling cascading failures

Branching model

Avalanche exponent wrt the exponent of a scale-free network:

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



http://networksciencebook.com/chapter/8

Building robustness

How to enhance a network's robustness?

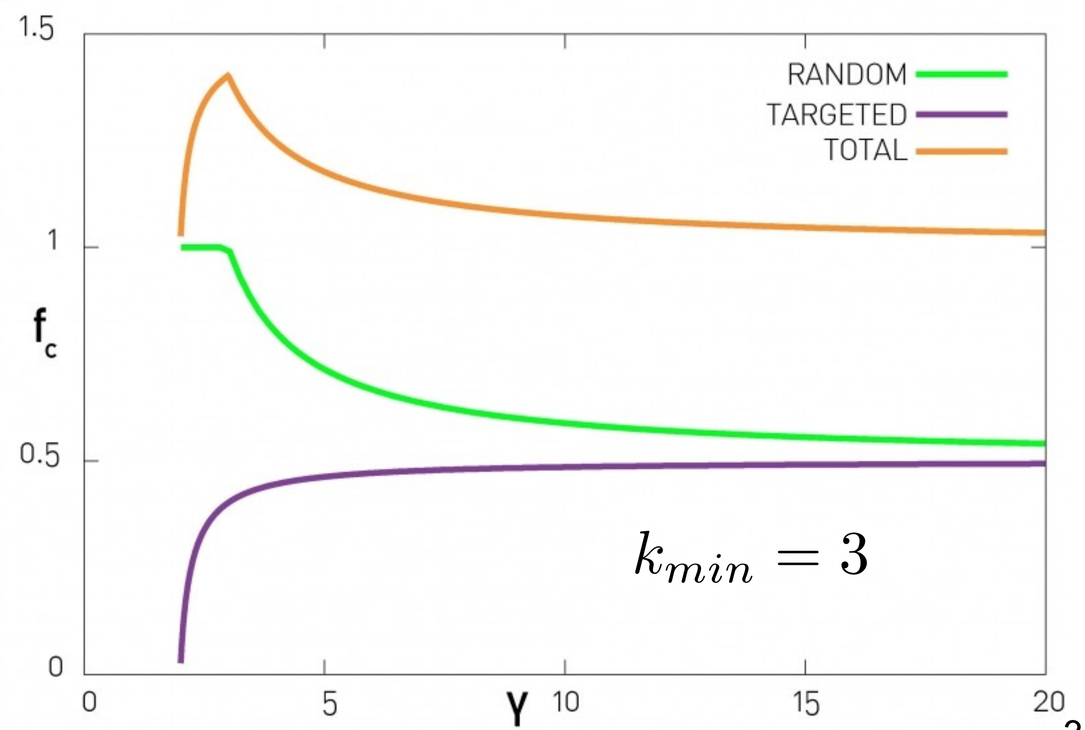
Maximizing the sum $f_c^{tot} = f_c^{rand} + f_c^{targ}$

with a bimodal degree distribution, corresponding to a network with only two kinds of nodes, with degrees k_{min} and k_{max}:

Dirac delta function

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

that describes a network in which an r fraction of nodes have degree k_{max} and the remaining $(1-r)$ fraction have degree k_{min}.



http://networksciencebook.com/chapter/8

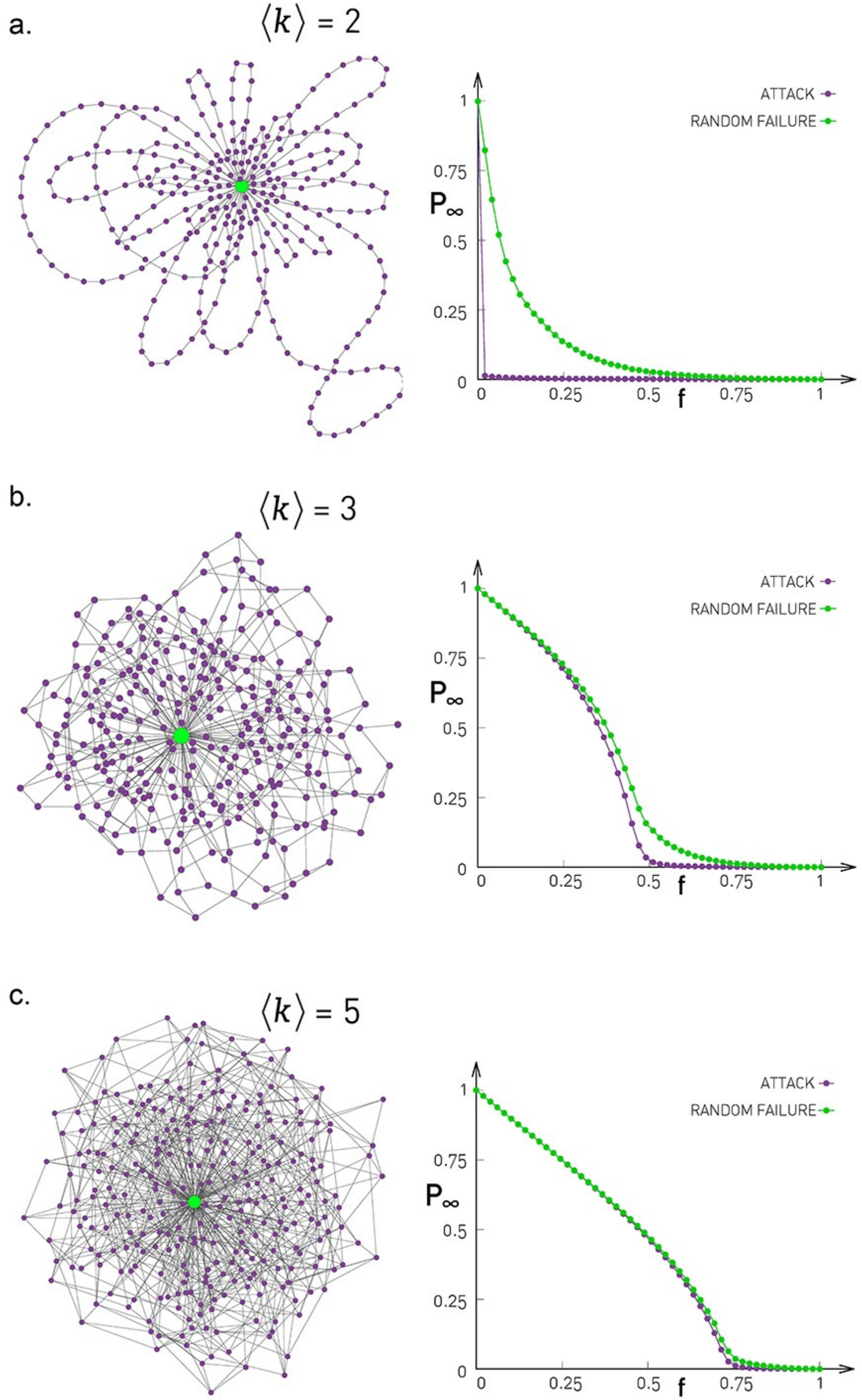
Building robustness

The optimal f_c^{tot} is obtained when $r = 1/N$, which gives a single node with degree k_{max}, and the remaining with degree k_{min}, with

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

Although it has a single hub, it is not vulnerable to attacks if $k_{min} > 1$,since these nodes form a giant component on their own.

A *is defined in (8.67) – Book.*



http://networksciencebook.com/chapter/8

Building robustness

Halting cascading failures

Can we avoid cascading failures?
In most real systems the time needed to establish a new link is much larger than the timescale of a cascading failure.
Example: Adding a new link to a transmission line on the power grid can take up to two decades. In contrast a cascading failure can sweep the power grid in a few seconds.

The time between the initial failure and its propagation is usually short.

One approach is to remove nodes with small loads and links with large excess load in the vicinity of the initial failure.

Case Study: Estimating Robustness

European power grid:

- More than 20 national power grids
- Over 3,000 generators and substations (nodes)
- 200,000 km of transmission lines

Degree distribution is approximated with

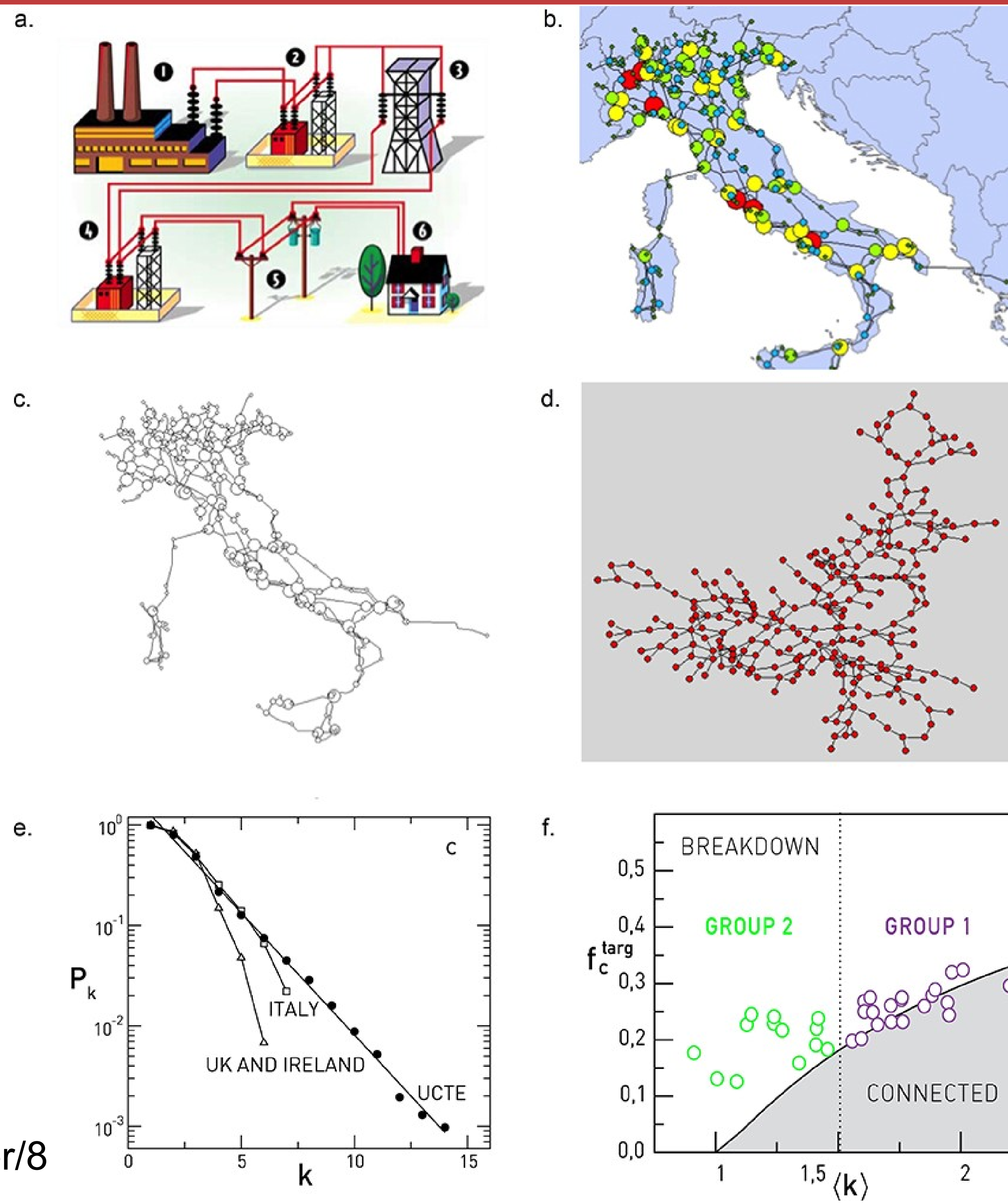
$$p_k = \frac{e^{-k/\langle k \rangle}}{\langle k \rangle}$$

(it lacks preferential attachment)

http://networksciencebook.com/chapter/8

Case Study: Estimating Robustness

(a) Infrastructure.
(b,c,d) Italian power grid.
(e) Degree distribution for the full network (UCTE) and others.
(f) Phase space $(\langle k \rangle, f_c^{targ})$.
Group 1 agrees with analytical predictions. Group 2 shows enhanced robustness.



http://networksciencebook.com/chapter/8

Take home message

Network topology, robustness, and fragility cannot be separated from each other. Rather, each complex system has its own Achilles' Heel: the networks behind them are simultaneously robust to random failures but vulnerable to attacks.

- **Robustness**: a system is robust if it is able to maintain its basic functions in the presence of errors;
- **Resilience:** dynamical property;
- **Redundancy:** parallel components and functions.

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:

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

Cascading failures:

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

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

http://networksciencebook.com/chapter/8