School of Information
University of Michigan

Network resilience

Lecture 20

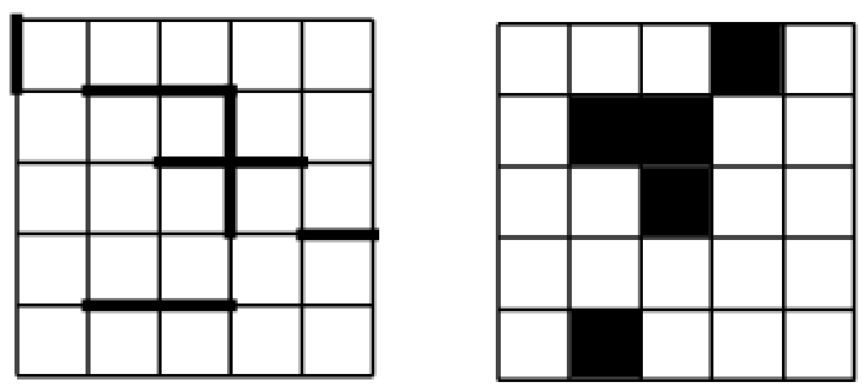
Outline

- network resilience
  - effects of node and edge removal
  - example: power grid
- discussion of insights from projects
- p* (exponential graph) models
  - (time permitting, or next Monday)

Network robustness and resillience

- Q: If a given fraction of nodes or edges are removed…
  - how large are the connected components?
  - what is the average distance between nodes in the components

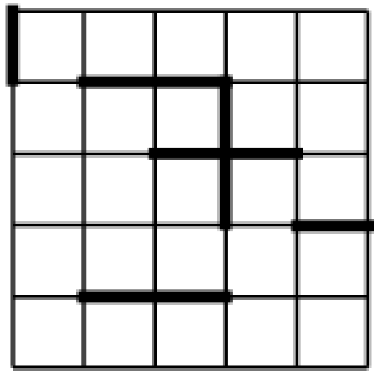
- Related to percolation (previously studied on lattices):



bond percolation *site percolation*

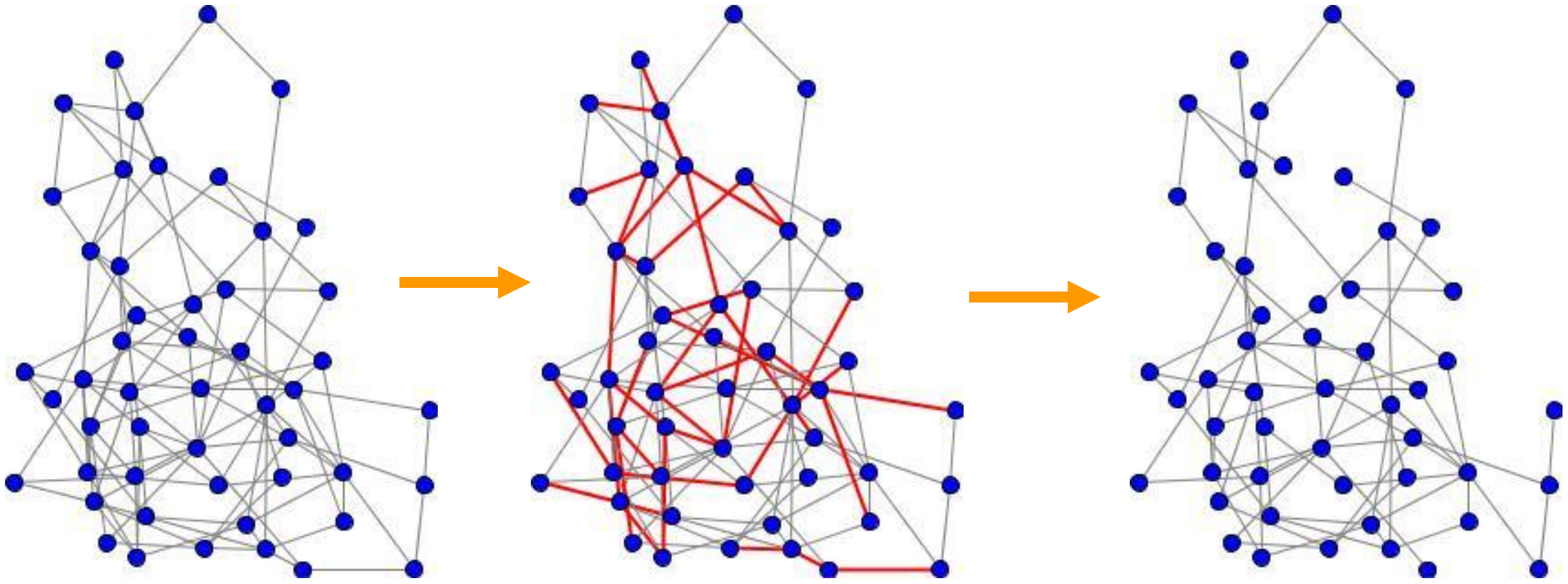
Bond percolation in Networks

- Edge removal
  - bond percolation: each edge is removed with probability (1-p)
    - corresponds to random failure of links
  - targeted attack: causing the most damage to the network with the removal of the fewest edges
    - strategies: remove edges that are most likely to break apart the network or lengthen the average shortest path
    - e.g. usually edges with high betweenness



bond percolation

Edge percolation

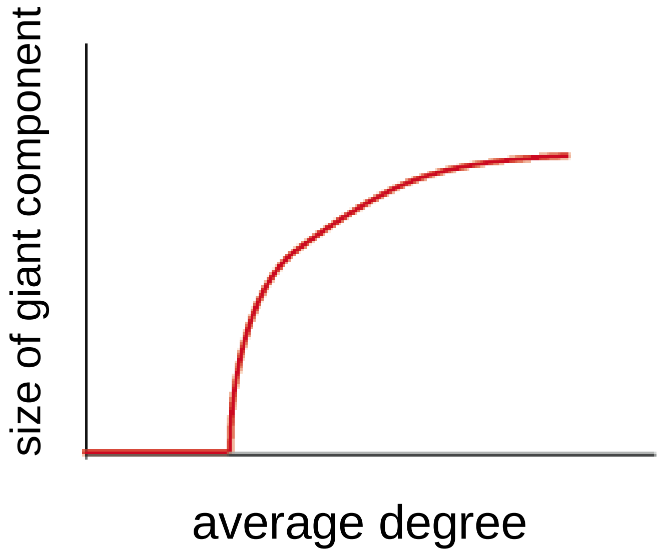


50 nodes, 116 edges, average degree 4.64

after 25 % edge removal

76 edges, average degree 3.04 – still well above percolation threshold

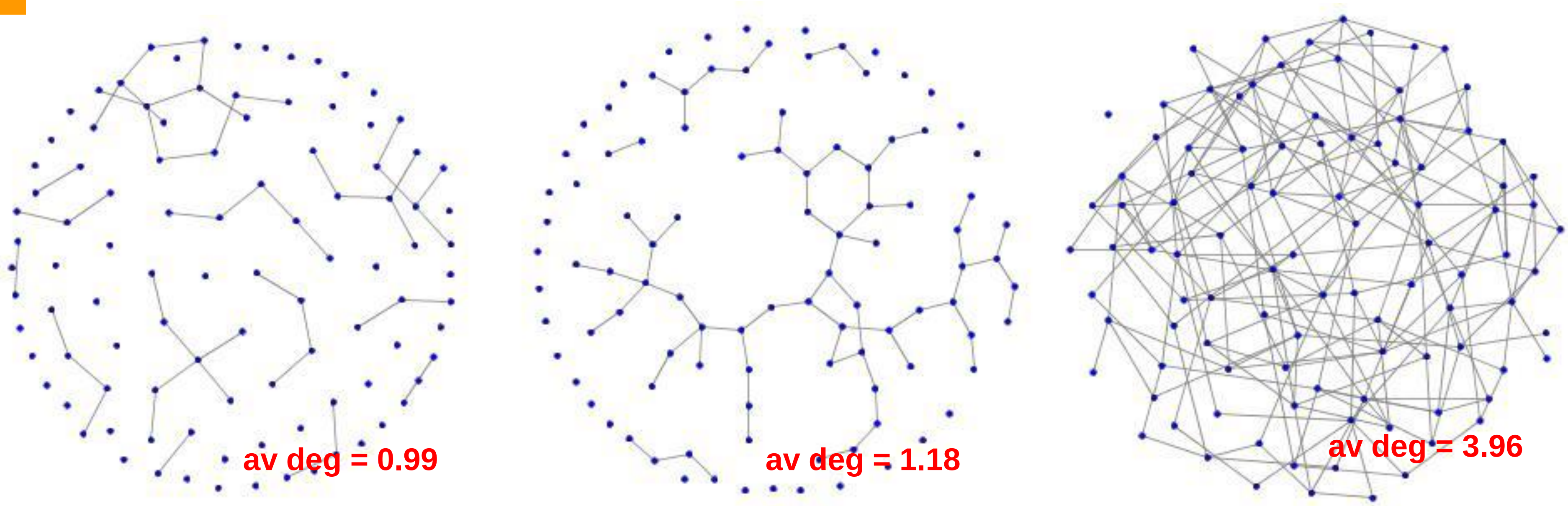
Percolation threshold in Erdos-Renyi Graphs



Percolation theshold: how many edges have to be removed before the giant component disappears?

As the average degree increases to z = 1, a giant component suddenly appears

Edge removal is the opposite process – at some point the average degree drops below 1 and the network becomes disconnected



Calculating the phase transition for networks with arbitrary degree distributions that are otherwise random

- Let p_k be the probability density function for the degrees of nodes in the network.
- Let q_k be the probability density function for the degree of a node at the end of a randomly chosen edge: $q_k = k\, p_k / \langle k \rangle$.
- Let f be the occupation probability for each edge.
- Assume that we start with one node and we want to find the size of the component connected to that node.
- Let z_n be the number of neighbors reachable in n steps.
- $z_{n+1} = z_n$ x the average excess degree of nodes reachable in n steps (the expectation value of $(k-1)$ over the distribution q_k) x the occupation probability, f

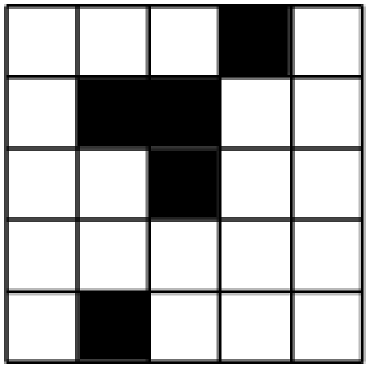
$$z_{n+1} = f\, z_n(\langle k^2 \rangle - \langle k \rangle)/\langle k \rangle$$

- Critical value of f:

$$f = \langle k \rangle / (\langle k^2 \rangle - \langle k \rangle)$$

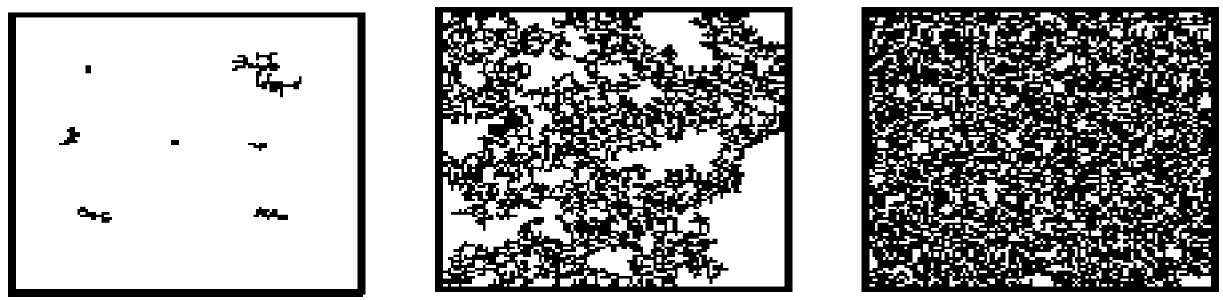
slide: Michelle Girvan

Node removal and site percolation



site percolation

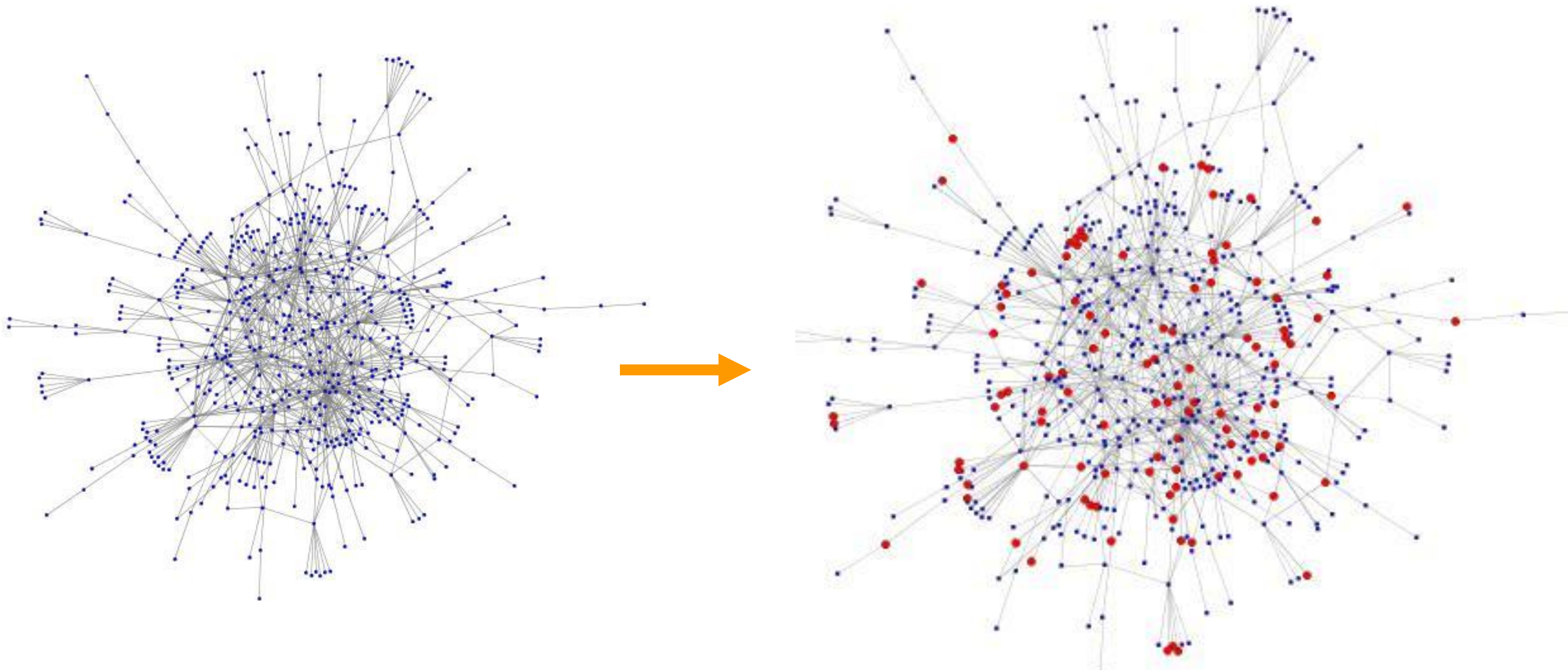
Ordinary Site Percolation on Lattices:
Fill in each site (site percolation) with probability p



- **low p**: small islands of connected components.
- **p critical**: giant component forms, occupying finite fraction of infinite lattice. Other component sizes are power-law distributed
- **p above critical value**: giant component occupies an increasingly large fraction of the system. Mean size of remaining component has a characteristic value.

adapted from slides by Michelle Girvan

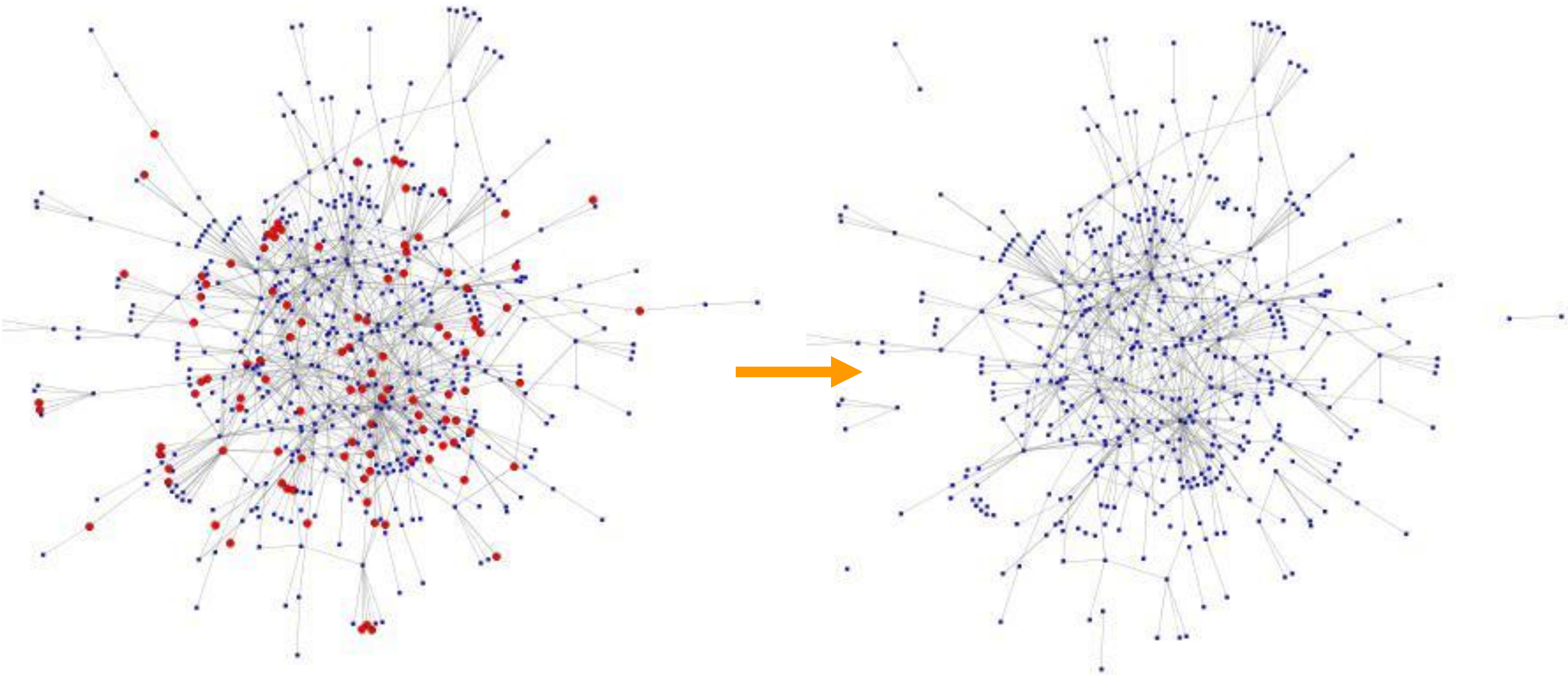
Percolation on Complex Networks



- Percolation can be extended to networks of arbitrary topology.
- We say the network percolates when a giant component forms.

Scale-free networks are resilient with respect to random attack

- Example: gnutella network, 20% of nodes removed

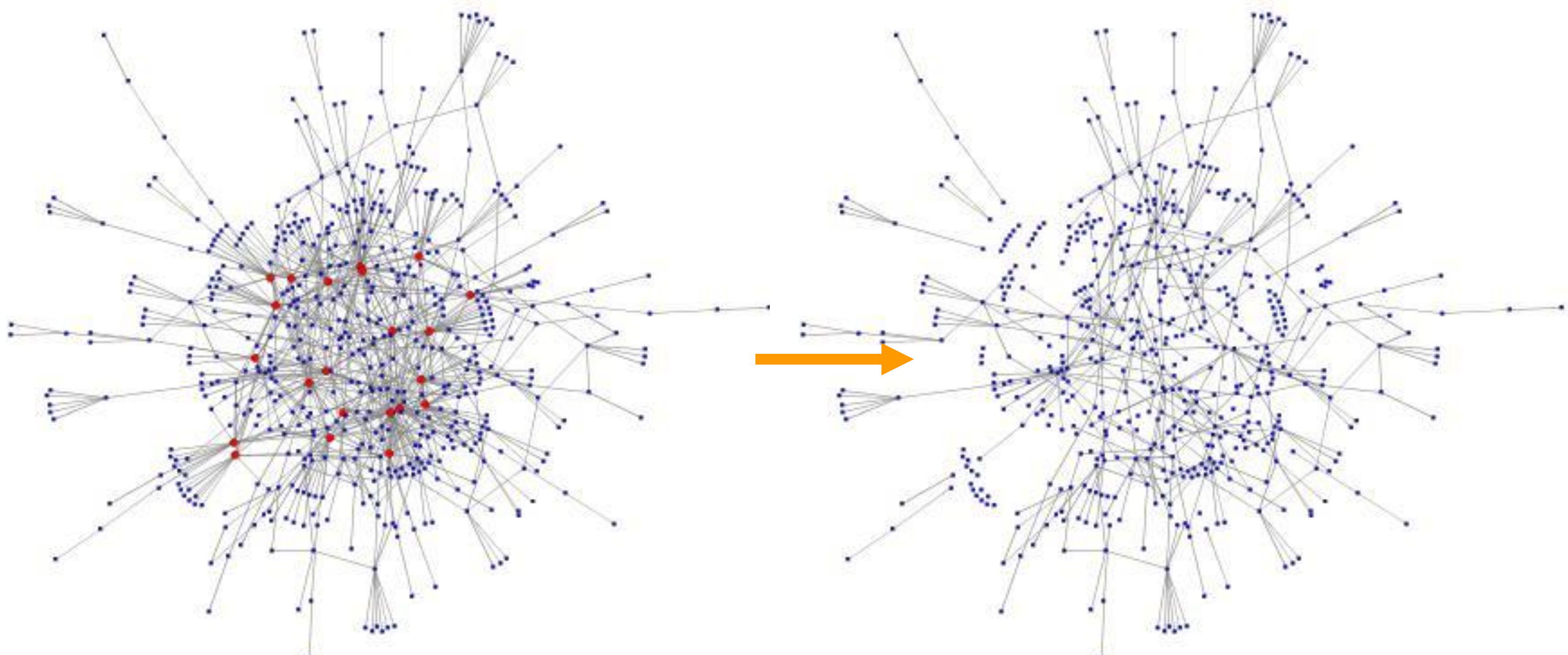


574 nodes in giant component

427 nodes in giant component

Targeted attacks are affective against scale-free networks

- Example: same gnutella network, 22 most connected nodes removed (2.8% of the nodes)



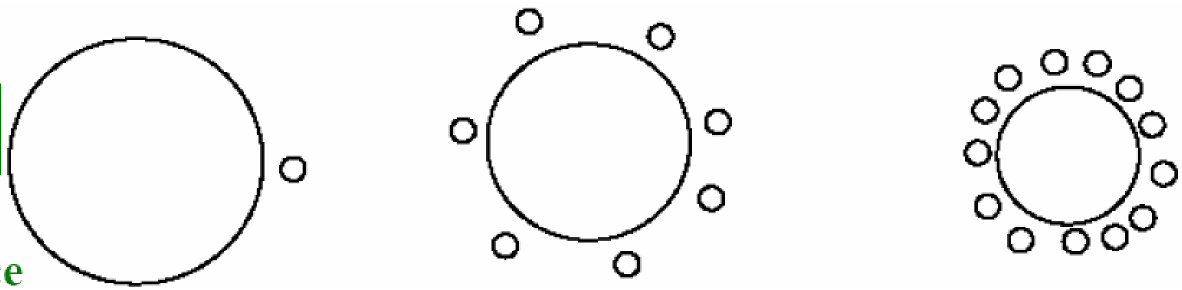
574 nodes in giant component

301 nodes in giant component

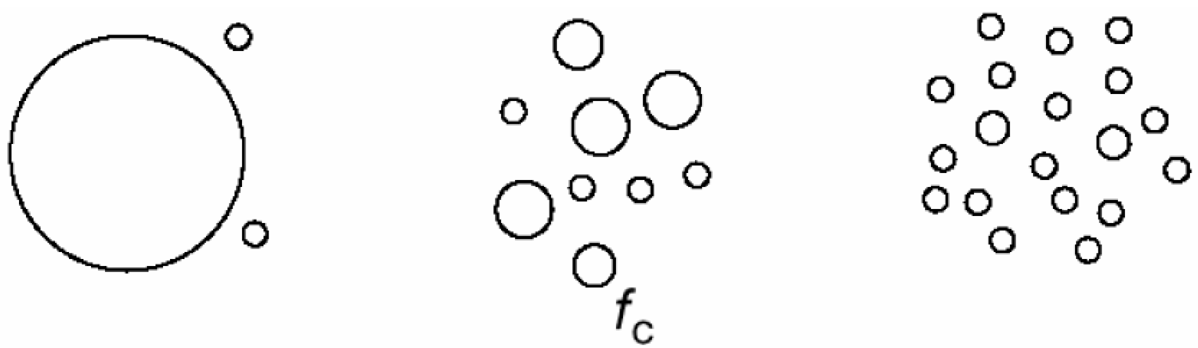
random failures vs. attacks

Failures

Topological error tolerance



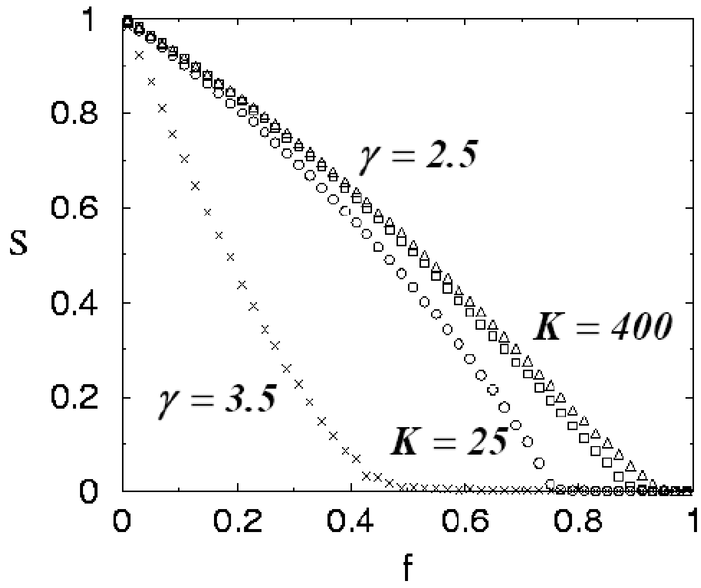
Attacks



adapted from slide by Reka Albert

Percolation Threshold scale-free networks

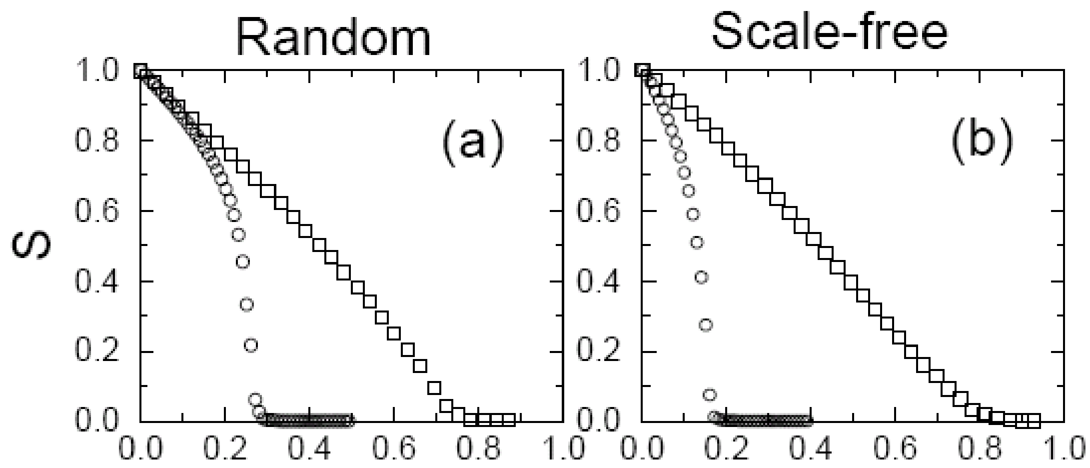
- For scale free graphs there is always a giant component (the network always percolates)



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

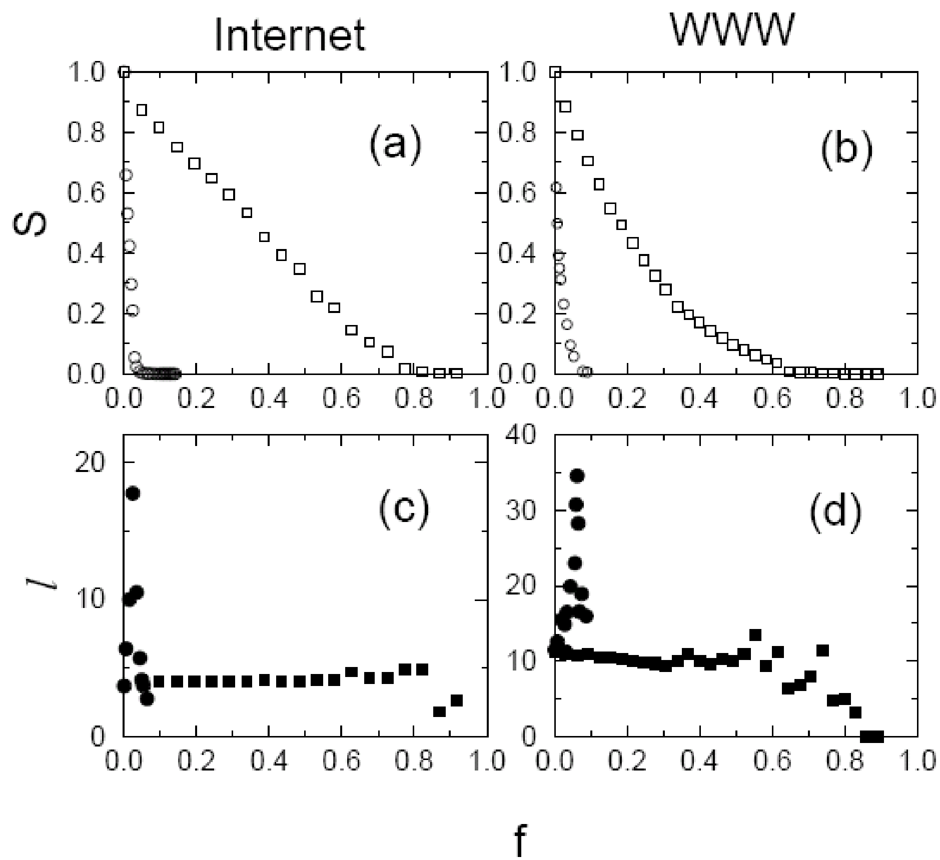
Network resilience to targeted attacks

- Scale-free graphs are resilient to random attacks, but sensitive to targeted attacks. For random networks there is smaller difference between the two

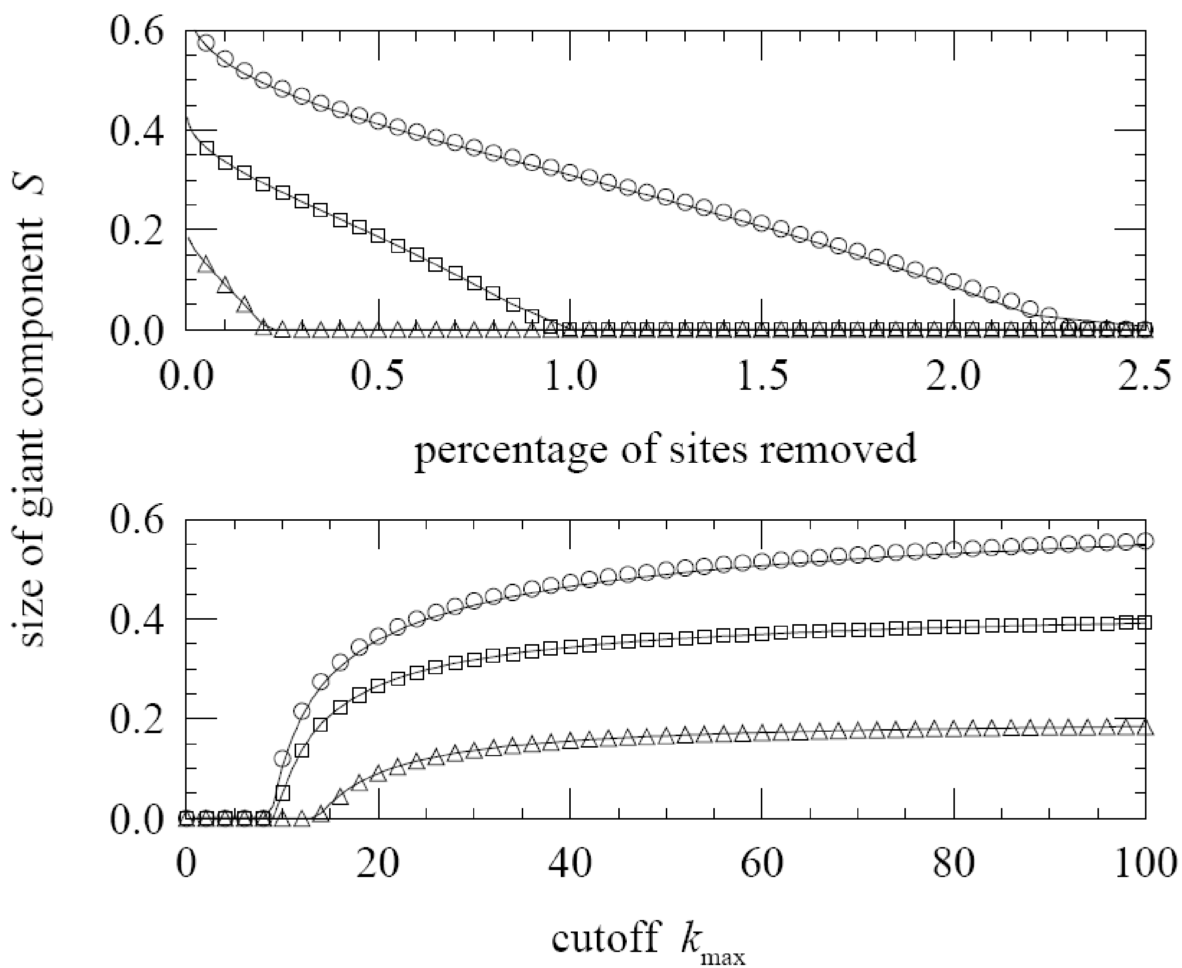


R. Albert, H. Jeong, and A.-L. Barabasi, *Attack and error tolerance of complex networks*, Nature, 406 (2000), pp. 378–382.

Real networks



Skewness of power-law networks and effects and targeted attack



% of nodes removed, from highest to lowest degree

k_{max} is the highest degree among the remaining nodes

D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, *Network robustness and fragility: Percolation on random graphs,* Phys. Rev. Lett., 85 (2000), pp. 5468–5471.

Preview of the next lecture
The link between percolation and traditional epidemiology

The traditional fully mixed model: Start with the SIR model of epidemic disease. The fraction of individuals in the states *s*, *i*, and *r* are governed by the equations:

$$\frac{ds}{dt} = -\beta i s, \qquad \frac{di}{dt} = -\beta i s - \gamma i, \qquad \frac{dr}{dt} = \gamma i$$

Grassberger (1983) showed that this can be mapped onto a *bond* percolation problem with occupation probability *T* given by the following expression

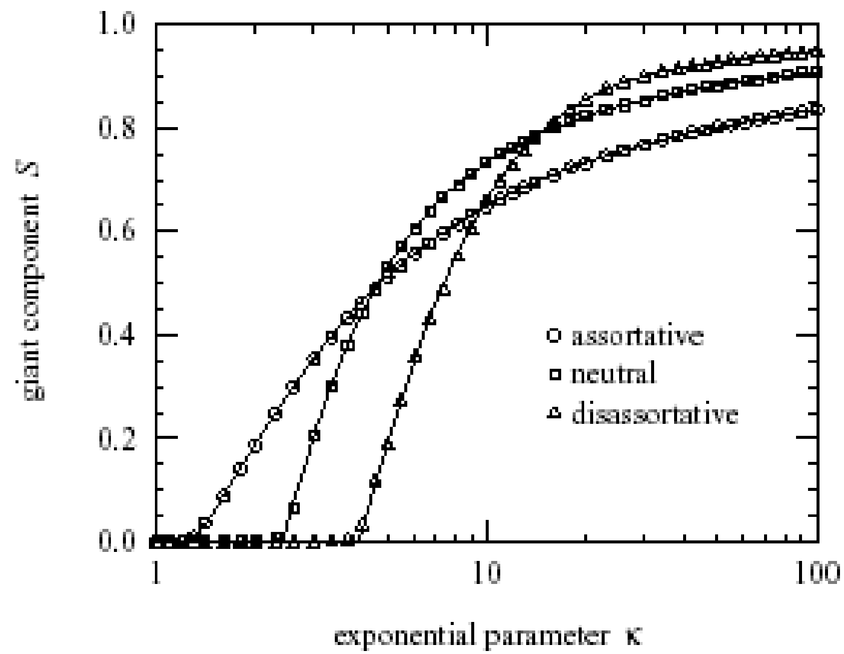
$$T = 1 - \int_0^\infty P_i(\beta) P_r(\gamma) e^{-\beta/\gamma} d\beta d\gamma$$

Site percolation can be used to consider vaccination strategies, which can be thought of as a scheme for node removal.

slide by Michelle Girvan

How does assortative mixing impact SIR dynamics?

- In assortatively mixed networks, the epidemic transition occurs sooner as the transmissibility is increased. In other words, epidemics occur at lowe transmissibility than in neutral or disassortative networks.
- In parameter regimes where epidemics readily occur, the number c infected individuals is generally lower for assortatively mixed networks.

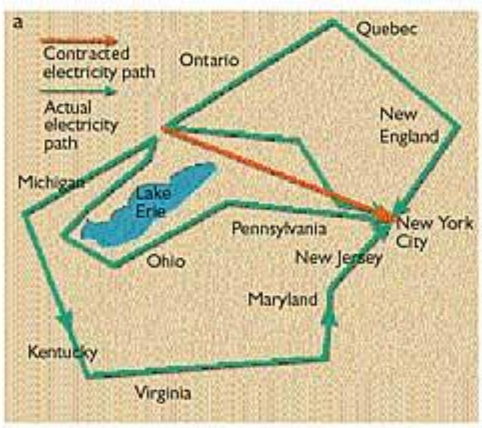


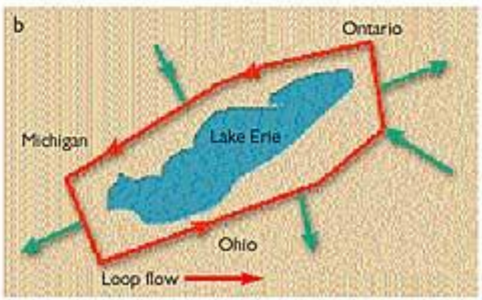
M. E. J. Newman, *Mixing patterns in networks,* Phys. Rev. E, 67 (2003), no. 026126.

slide by Michelle Girvan

Power grid

- Electric power does not travel just by the shortest route from source to sink, but also by parallel flow paths through other parts of the system. Where the network jogs around large geographical obstacles, such as the Rocky Mountains in the West or the Great Lakes in the East, loop flows around the obstacle are set up that can drive as much as 1 GW of power in a circle, taking up transmission line capacity without delivering power to consumers.





http://www.aip.org/tip/INPHFA/vol-9/iss-5/p8.html

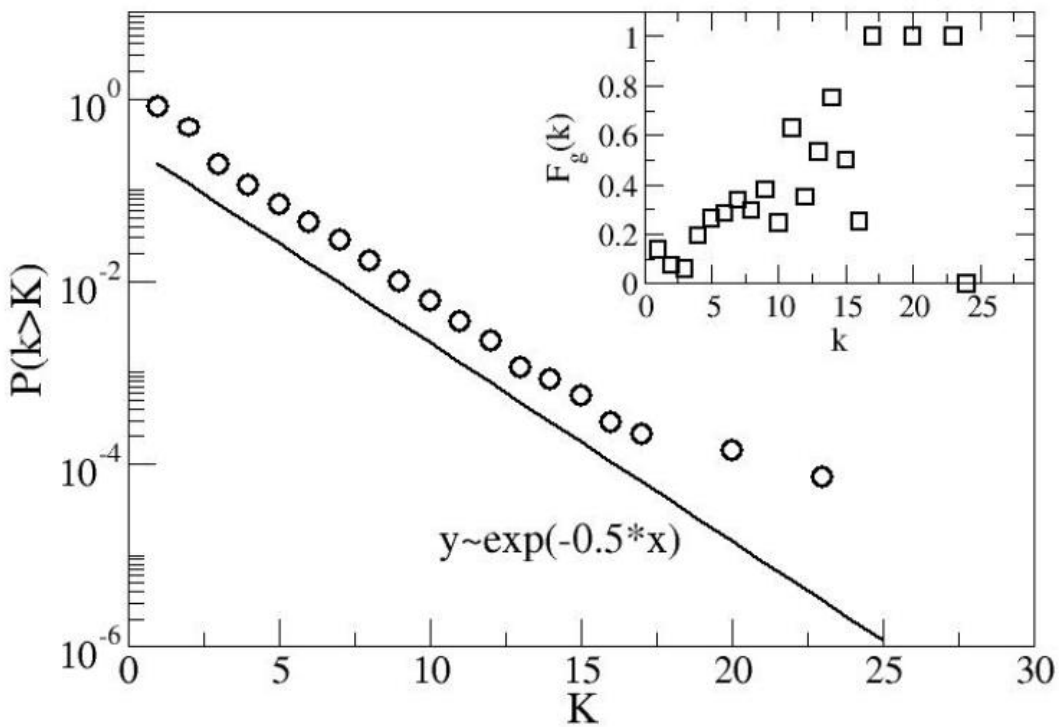
Cascading failures

- Each node has a load and a capacity that says how much load it can tolerate.
- When a node is removed from the network its load is redistributed to the remaining nodes.
- If the load of a node exceeds its capacity, then the node fails

Case study: North American power grid

- Nodes: generators, transmission substations, distribution substations
- Edges: high-voltage transmission lines
- 14099 nodes: 1633 generators, 2179 distribution substations, the rest transmission substations
- 19,657 edges

Degree distribution is exponential



$$P(k > K) \approx \exp(-0.5K)$$

Efficiency of the network

- Efficiency of the network:
  - average over the most efficient paths from each generator to each distribution station

$$E = \frac{1}{N_G N_D} \sum_{i \in G_G} \sum_{j \in G_D} \epsilon_{ij}$$

- Impact of node removal
  - change in efficiency

$$D = \frac{E(G_0) - E(G_f)}{E(G_0)}$$

Capacity and node failure

- Assume capacity of each node is proportional to initial load

$$C_i = \alpha L_i(0) \quad i = 1, 2..N$$

- Each neighbor of a node is impacted as follows

$$e_{ij}(t+1) = \begin{cases} e_{ij}(0) / \frac{L_i(t)}{C_i} \text{ if } L_i(t) > C_i \\ e_{ij}(0) \text{ if } L_i(t) \leq C_i \end{cases}$$

load exceeds capacity

- Load is distributed to other nodes/edges
- The greater a (reserve capacity), the less susceptible the network to cascading failures due to node failure

power grid structural resilience

- efficiency is impacted the most if the edge removed is the one with the highest load