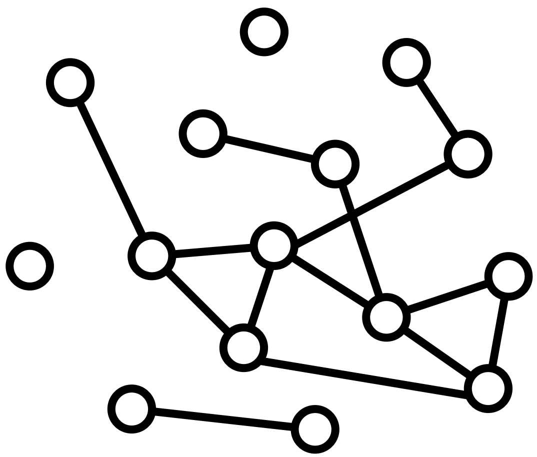
Simulation I: Dynamics of Networks

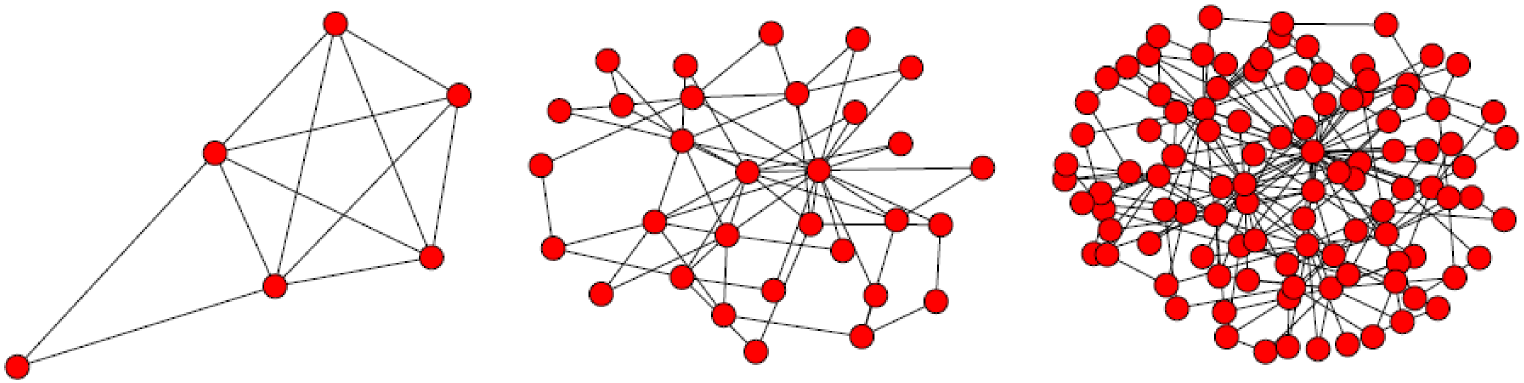


Hiroki Sayama
sayama@binghamton.edu

Modeling and Simulation of Dynamical Networks

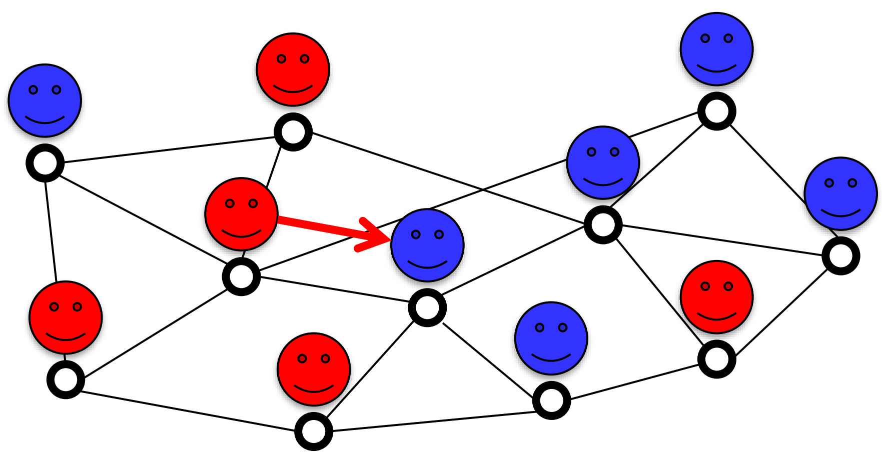
Dynamics of networks

- **Dynamic growth and transformation of network topologies**
  - Social network formation
  - Growth of the Internet and WWW
  - Growth of scientific citation networks



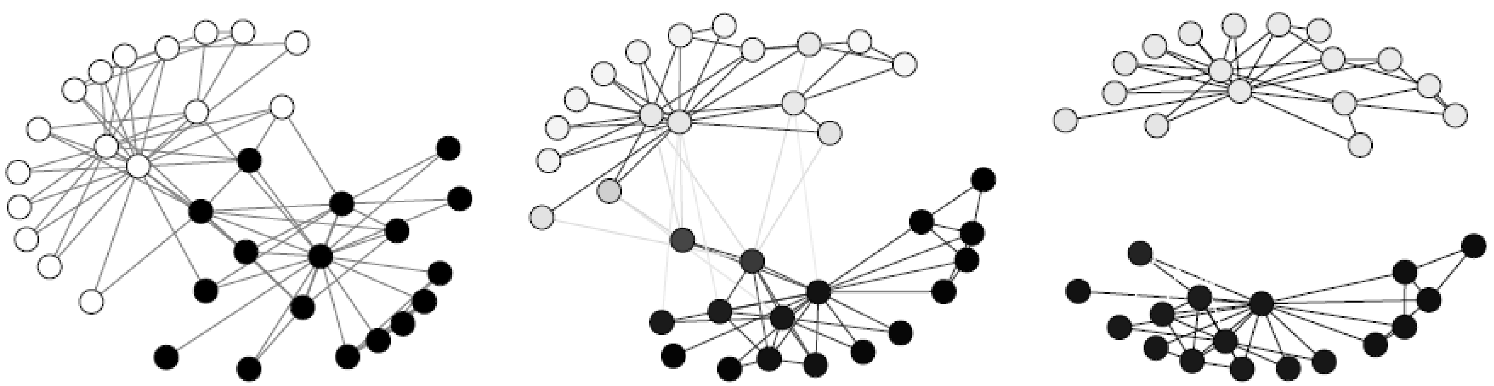
Dynamics *on* networks

- Dynamic state changes taking place on a static network topology
  - Gene/protein regulatory networks
  - Population dynamics on food webs
  - Spread of disease/opinion/failure



Adaptive Networks

- Complex networks whose states and topologies co-evolve, often over similar time scales
  - Link (node) states adaptively change according to node (link) states



Modeling and Simulation of Dynamics of Networks

Dynamics of networks

- Dynamic growth and transformation of network topologies
  - Social network formation
  - Food web formation over ecological/ evolutionary time scales
  - Growth of the Internet and WWW
  - Growth of scientific citation networks
  - Effects of node/link removal or rewiring

Network Percolation

Percolation in random networks

- Number of connected components decreases with increasing link probability

- Above a critical probability p_c, a **giant connected component** emerges

Giant connected component

- Largest connected component whose size (relative to the total number of nodes N) remains positive even if N is very large

$$\lim_{N \to \infty} |GCC|/N > 0$$

  - If LCC is not giant, $\lim_{N \to \infty} |LCC|/N = 0$

Exercise

- Simulate the emergence of a giant connected component by randomly introducing edges one by one
- Monitor the process and see how the giant connected component emerges

Exercise

- Plot (1) the size of the largest connected component and (2) the number of connected components of a random network made of 10,000 nodes over varying p

Review: Degree distribution of ER networks

- Degree distribution of an ER random network is given by a binomial distribution:

$$P(k) = {}_{N-1}C_k \; p^k \; (1-p)^{N-1-k}$$

- With large N (with fixed Np), it approaches a Poisson distribution:

$$P(k) \sim (Np)^k \; e^{-Np} \; / \; k!$$

Percolation threshold

- Let s be the probability for a node to belong to LCC (i.e., |LCC| = sN)
- Degree dist.: $P(k) = (Np)^k e^{-Np} / k!$
- Probability for a node to be separated from LCC is given by:

$$1-s = \Sigma_{k=0\sim\infty} P(k) (1-s)^k$$

  - $(1-s)^k$ is the probability for all k neighbors to be separated from LCC

Exercise

- Using the following equations, show that s can take positive values if and only if $\langle k \rangle = Np > 1$

$$P(k) = (Np)^k e^{-Np} / k!$$

$$1-s = \Sigma_{k=0\sim\infty} P(k) (1-s)^k$$

Exercise

- Choose two link probabilities, one below and one above p_c
- Create ER random networks for each probability with varying N, and see how the size of their LCCs scales along N

Exercise

- If $1-s < 1/N$, that means all nodes are essentially included in LCC, and thus the network is made of just one connected component

- Obtain the critical threshold of $\langle k \rangle$ above which this occurs

Edge Rewiring and Growth

Exercise: Rewiring for "small-world"

- Create a ring-shaped network made of n nodes; connect each node to k nearest neighbors
- Visualize the network by coloring nodes using their closenesses
- Randomly rewire edges one-by-one
- Monitor what happens to the network topology and node colors

Exercise: Preferential attachment

- Simulate the growth process of the Barabasi-Albert network growth model with m = 1, m = 3 and m = 5

- See how the process is affected by variation of this parameter

Exercise

- Modify the simulation code so that the node selection preference is:
  - Independent of the node degree
  - Proportional to the square of the node degree
  - Inversely proportional to the node degree

- Conduct simulations and compare the resulting network topologies

Exercise

- Modify the simulation code of the preferential attachment model so that a node whose degree exceeds a certain capacity limit splits into two (and each node inherits about half of the original connections)
- Conduct simulations and compare the resulting network topologies

Robustness and Vulnerability of Complex Networks

Robustness and vulnerability

- How do these networks respond to dynamic topological changes caused by external forces?
  - Input: Removal of nodes
  - Output: Changes in characteristic path length and connectivity

Two types of node removals

- Error: Random removal of nodes
  - Occurs stochastically
  - Same error probability for all nodes
- Attack: Selective removal of most connected nodes
  - Occurs deterministically
  - The attacker knows network hubs

Examples in real-world networks

- **WWW:**
  - Error ⇒ Occasional server breakdown
  - Attack ⇒ Server breakdown due to DoS etc.
- **Warfare:**
  - Error ⇒ Accidental local actions
  - Attack ⇒ Strategic actions to hit the central core of opponents
- **Marketing:**
  - Error ⇒ Indiscriminate direct mail, spam
  - Attack ⇒ Targeting on influential customers

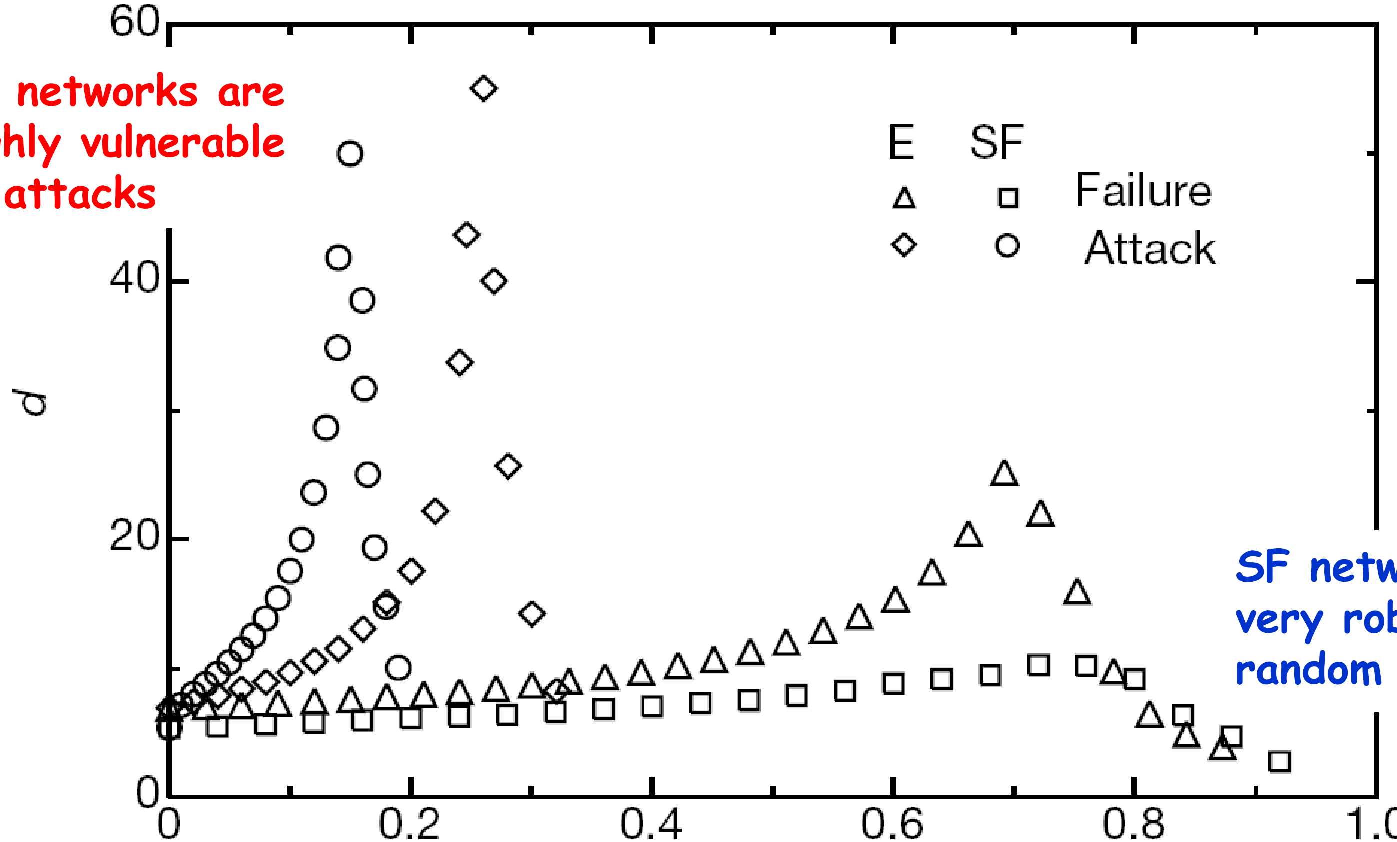
Robustness and vulnerability of scale-free networks

- R. Albert, H. Jeong & A.-L. Barabasi, Error and attack tolerance of complex networks, Nature 406:378-382, 2000.
  - Considered the effects of random errors & targeted attacks on scale-free networks (both simulated and actual ones)

Change of diameter (experiments with artificially generated networks)

Characteristic path length

SF networks are highly vulnerable to attacks

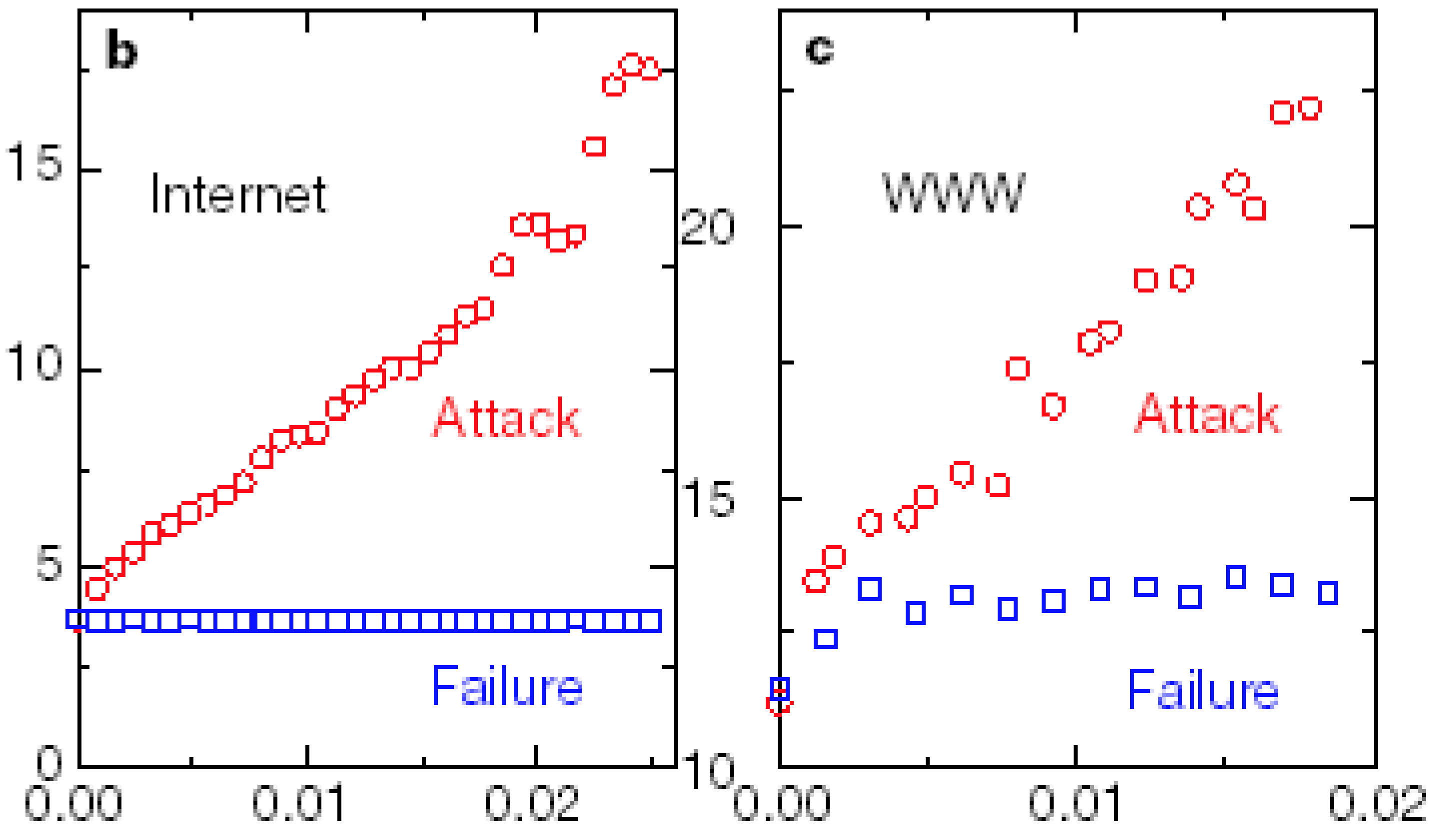


SF networks are very robust to random failures

Fraction of removed nodes

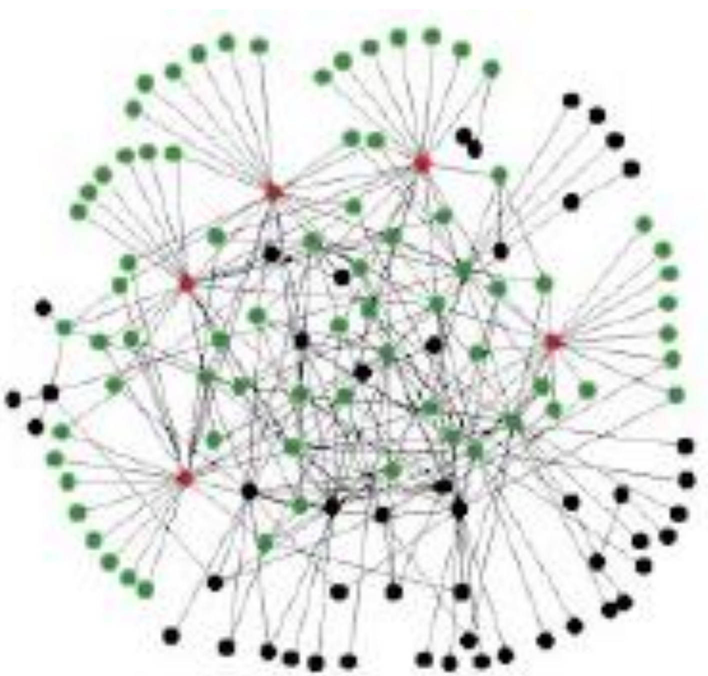
Change of diameter (experiments with networks based on real data)

Characteristic path length



Fraction of removed nodes

Why such robustness / vulnerability occurs?



A scale-free network has a few hub nodes and a lot of non-hub (mostly terminal) nodes

→Random errors are likely to hit non-hub nodes, causing only limited influence

→Attacks always hit hubs, causing great impacts on the whole

Fragmentation analysis

- If node removal goes on further, the network will eventually fall apart (fragmentation)

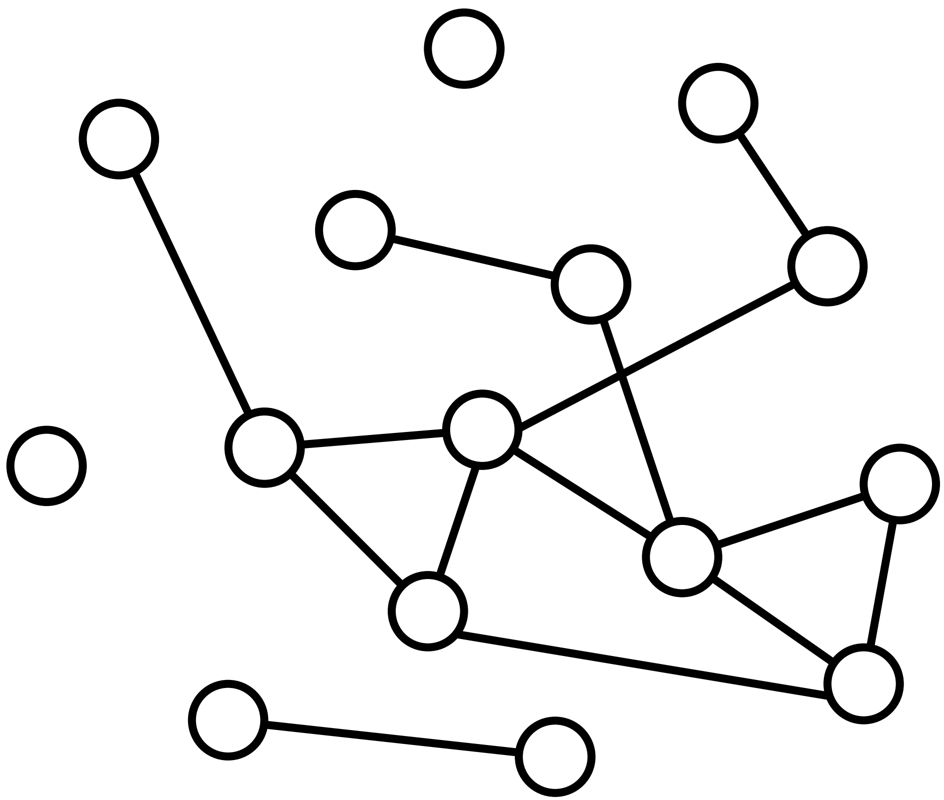
  One can detect such fragmentation by monitoring the following:

  S : Size of LCC

  <s> : Average size of all other smaller connected components

Exercise

- Calculate S and <s> for this graph



What S and <s> tells us

- While individual nodes drop out one by one from the largest connected body:

  → S decreases slowly, <s> ~ 1

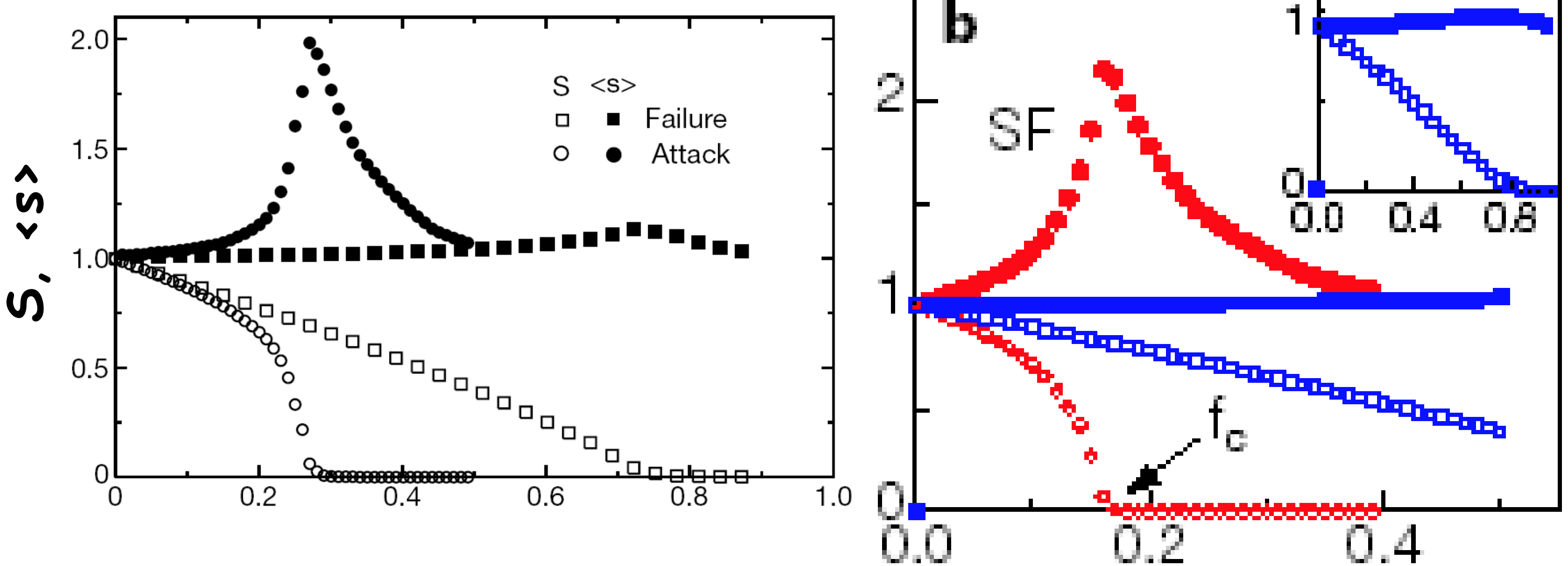
- When the LCC falls apart:

  → S drops suddenly, <s> > 1

The latter indicates a critical moment of network fragmentation

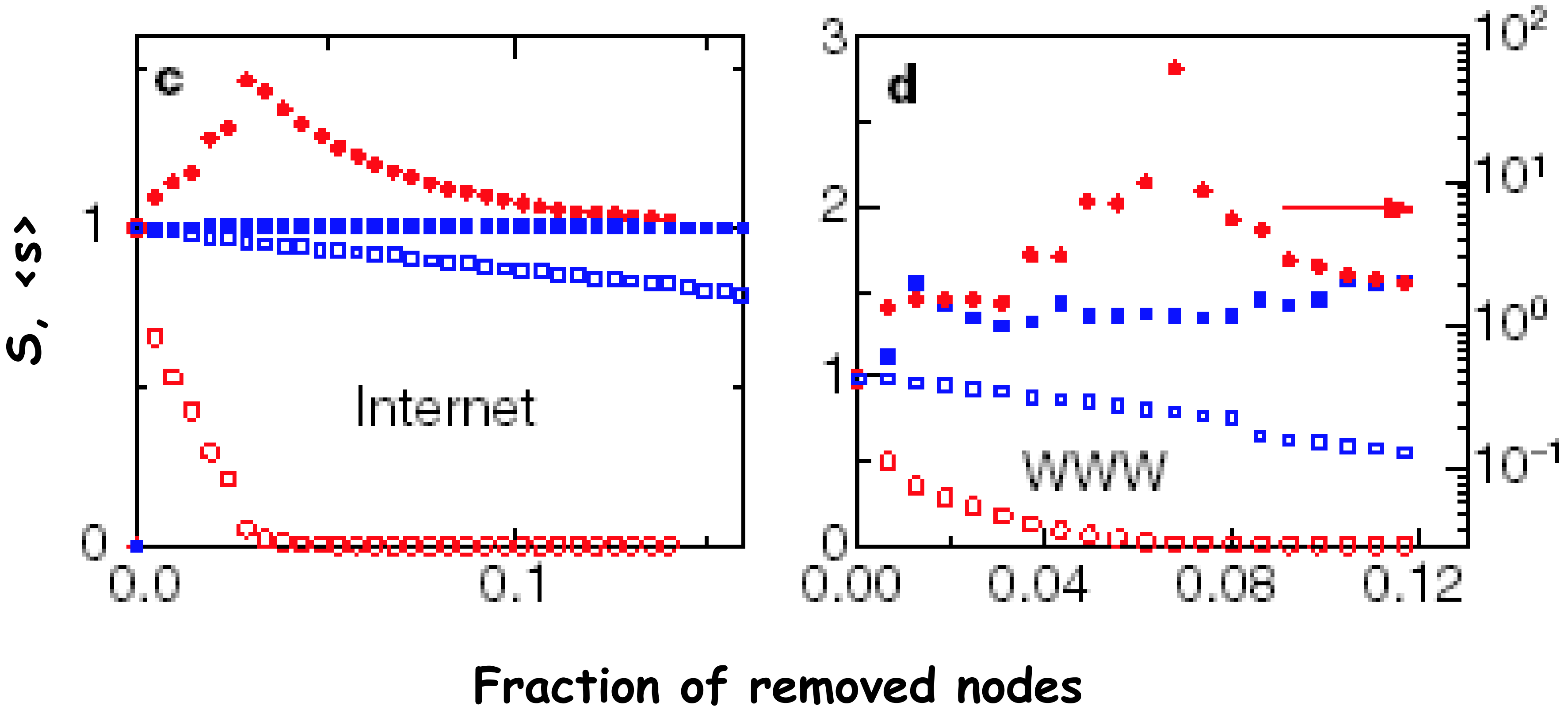
Fragmentation process (experiments with artificially generated networks)

Random **Scale-free**



Fraction of removed nodes

Fragmentation process (experiments with networks based on real data)



Exercise

- Replicate Albert, Jeong & Barabasi's network fragmentation experiments for ER random networks and BA scale-free networks

Exercise

- Conduct fragmentation analysis on Mark Newman's Political Blogs network data

- Try several different attack strategies and see which one would be most effective in disrupting the connectivity of the network

Network vulnerability

- Scale-free networks are robust to stochastic errors, but quite fragile against intentional attacks targeted to hubs
- This conclusion directly applies to real-world networks
  - DoS attacks to key servers, terrorisms at commercial hubs, etc…
- Then, what can we do?

A Potential Solution:

(1,0) networks

Our attempt

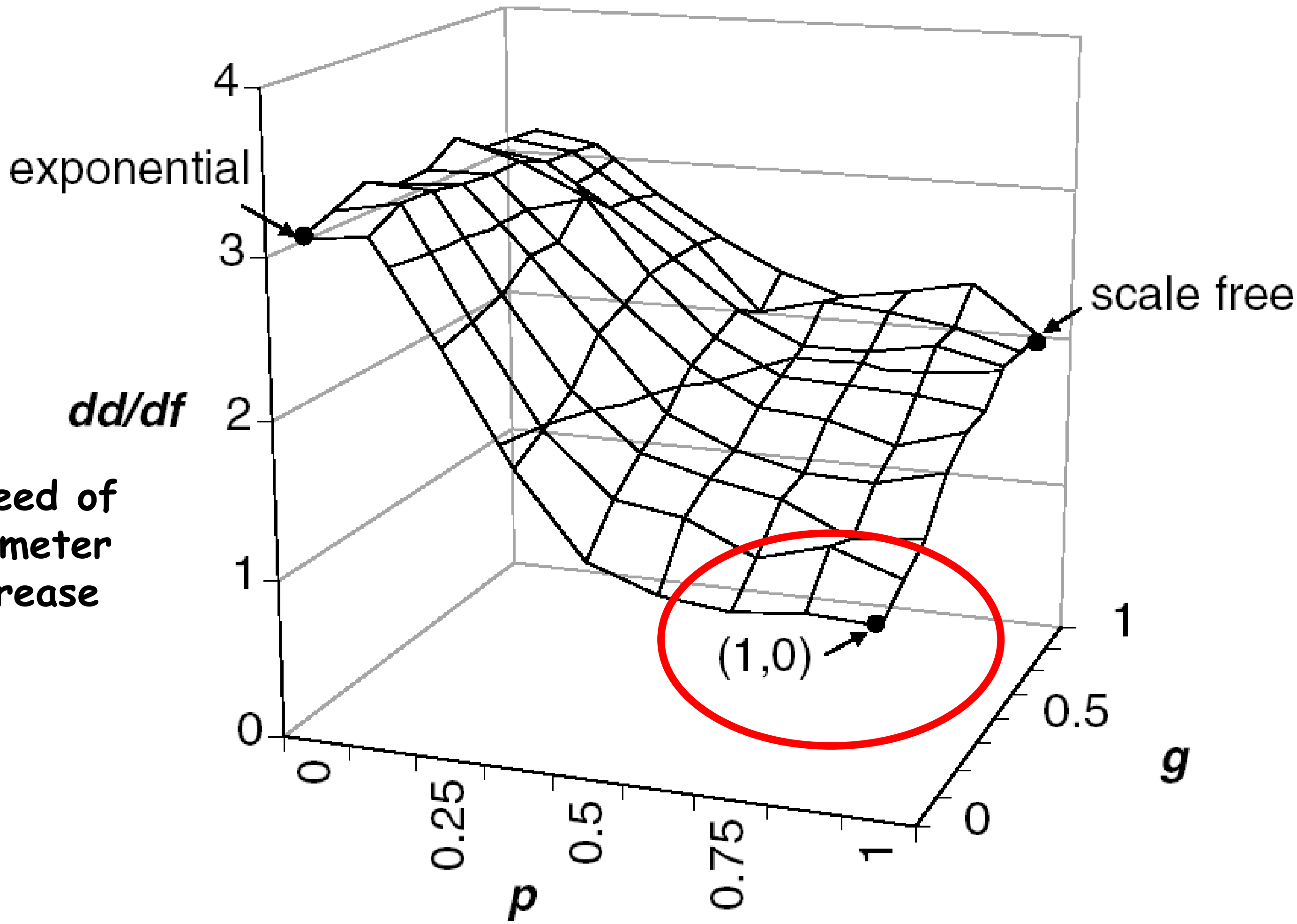
- B. Shargel, H. Sayama, I. R. Epstein & Y. Bar-Yam, Optimization of robustness and connectivity in complex networks, Phys. Rev. Lett. 90:068701, 2003.
  - Reconsidered the details of network development and proposed (1,0) networks that are more robust to both errors and attacks than pure scale-free networks

Two parameters for network development

- Preference parameter p ($0 \leq p \leq 1$)
  - Specifies how much the selection of nodes is affected by their degrees
- Growth parameter g ($0 \leq g \leq 1$)
  - Specifies the fraction of nodes that are added through the developmental process to the total number of nodes

Seeking a more robust network in the p-g parameter space

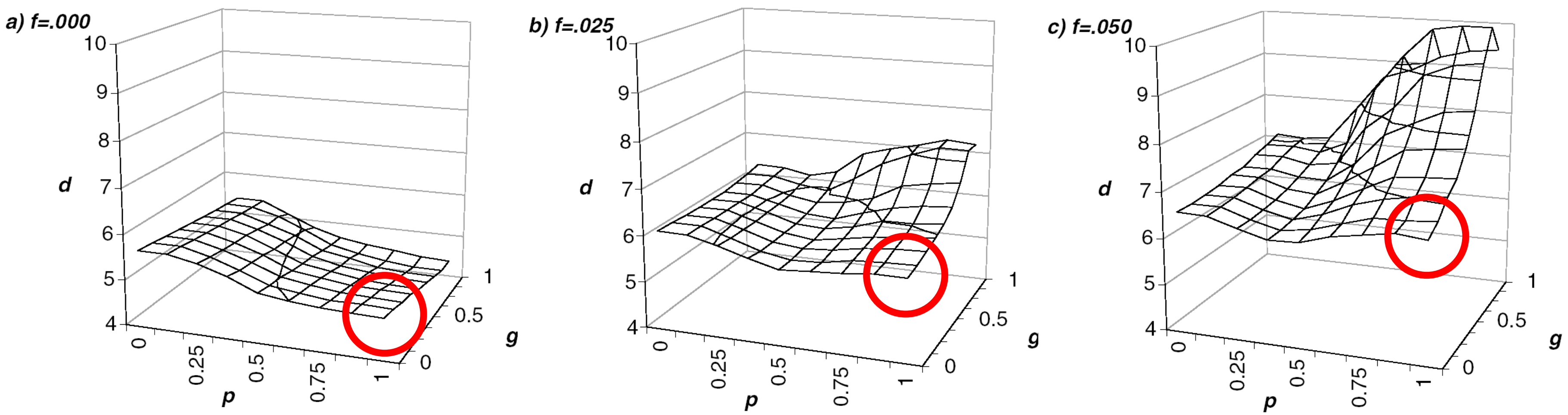
Response to random errors



Speed of diameter increase

Response to targeted attacks

d : characteristic path lengths



Intensity of attacks

Why robust to attacks?

- During the development of a (1,0) network, well-connected hubs can be connected to each other

→ Tightly connected clusters of hubs will emerge

(In the scale-free network growth with preferential attachment, isolated hubs cannot be connected to each other)

Exercise: Preferential attachment

- Simulate the development process of the (p, g) network model

- See how the resulting network topology differs among the following

  $(p, g) = (0, 0)$ (random)

  $(p, g) = (1, 1)$ (preferential attachment)

  $(p, g) = (1, 0)$

Implications

Networks that continue to reinforce connections between their internal parts can be more robust in many situations than other networks whose internal connections are enhanced only by the addition of newcomers