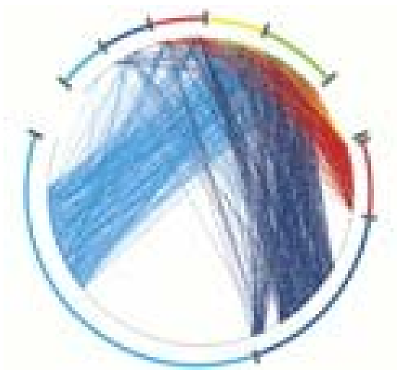
Lecture 16: Network Resiliency



Robustness

Definition: A [property] of [a system] is ***robust*** if it is [invariant] for [a set of perturbations]

Robustness to different kinds of perturbations:

Reliability	component failures
Efficiency	resource scarcity
Scalability	changes in size and complexity of the system as a whole
Modularity	structured component rearrangements
Evolvability	lineages to possibly large changes over long time scales

Strategies for Creating System Robustness

Increasing Complexity

1. Improve robustness of individual components
2. Functional redundancy: components or subsystems
3. Sensors that trigger human intervention
   - Monitor system performance
   - Detect individual component wear
   - Indentify external threats
4. Automated control

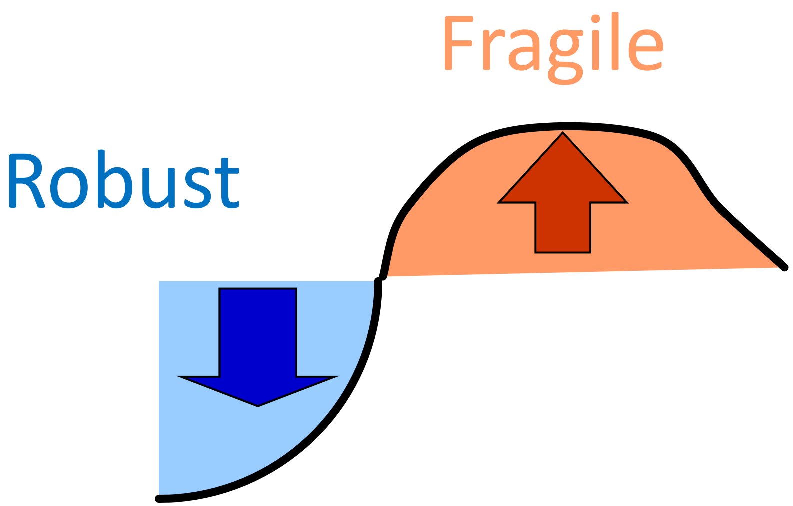
Complexity – Robustness Spiral

- The same mechanisms responsible for robustness to most perturbations
- allows possible extreme fragilities to others
- Usually involving hijacking the robustness mechanism in some way

Robust yet Fragile

[a system] can have
[a property] ***robust*** for
[a set of perturbations]

Yet be ***fragile*** for
[a different property]
Or [a different perturbation]



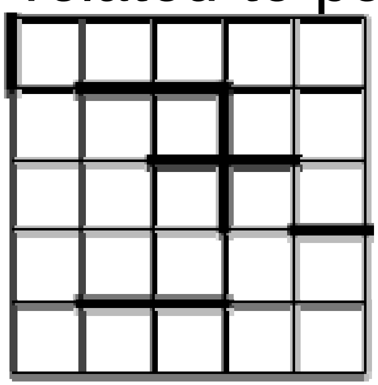
<u>Proposition</u> :
The RYF tradeoff is a ***hard limit*** that cannot be overcome.

Network resiliency

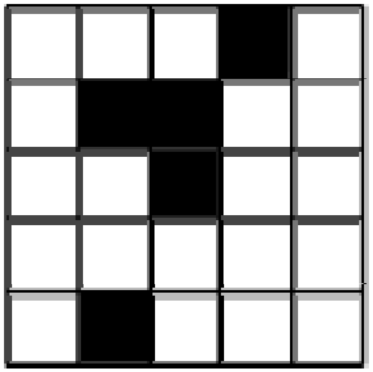
- Reasons for studying error and attack tolerance
  - Designing robust networks
  - Protecting existing networks
- network resiliency
  - effects of node and edge failure
- Two kinds of component removals:
  - Error: random failure
  - Attack: intentional failure, e.g. removing nodes with high degrees
- Error/attack tolerance of networks!

Network resiliency

- <u>Question</u>: 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
  - How is the efficiency
  - How are the spectral properties
  - ...
- This topic is related to percolation



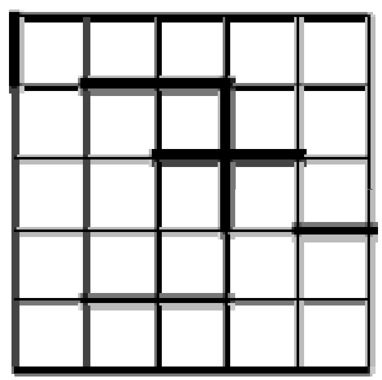
bond percolation



site percolation

Bond percolation in Networks

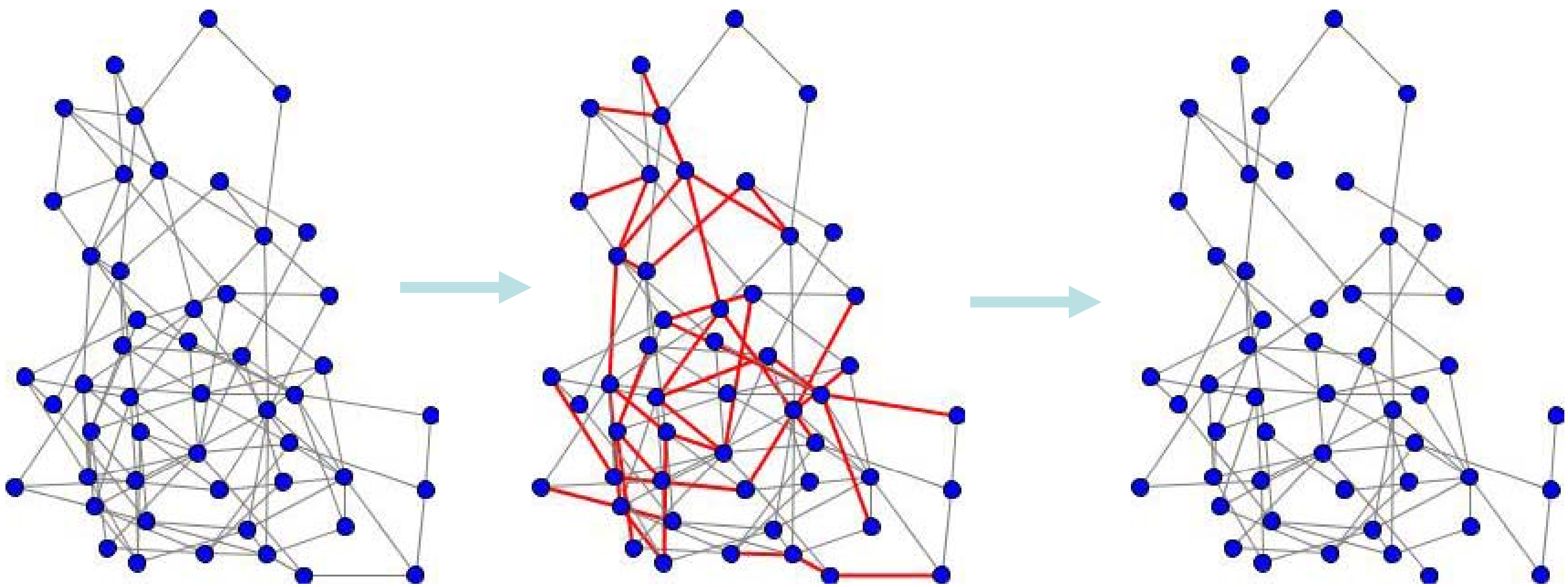
- Edge removal
  - bond percolation: each edge is removed with probability (1-p)
    - corresponds to random failure of links
  - targeted attack: causing the most damage to the network with the removal of the fewest edges
    - strategies: remove edges that are most likely to break apart the network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



bond percolation

Source: http://mathworld.wolfram.com/BondPercolation.html

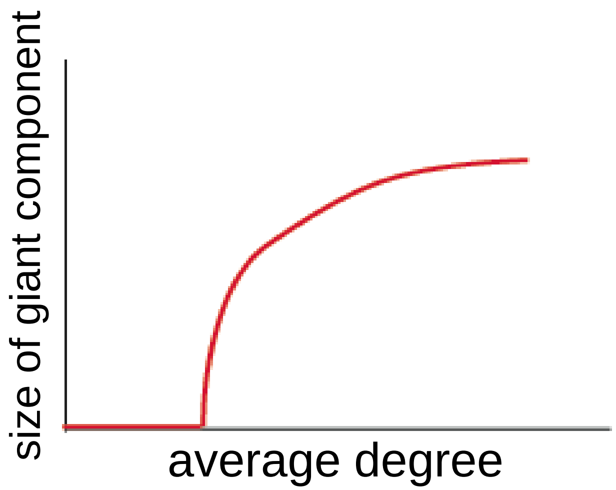
Edge percolation



How many edges would you have to remove to break up an Erdos-Renyi random graph? e.g. each node has an average degree of 4.6

50 nodes, 116 edges, average degree 4.64
after 25 % edge removal
76 edges, average degree 3.04 – still well above percolation threshold

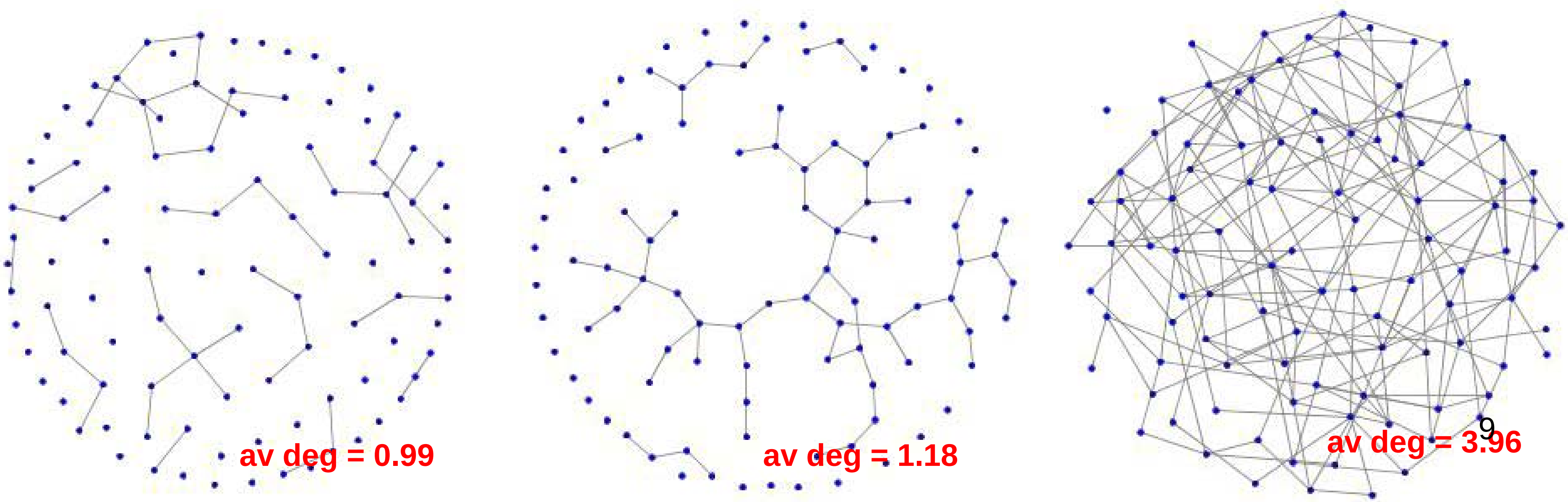
Percolation threshold in Erdos-Renyi Graphs



Percolation threshold: the point at which the giant component emerges

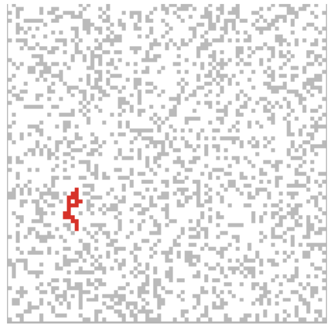
As the average degree increases to z = 1, a giant component suddenly appears

Edge removal is the opposite process –as the average degree drops below 1 the network becomes disconnected

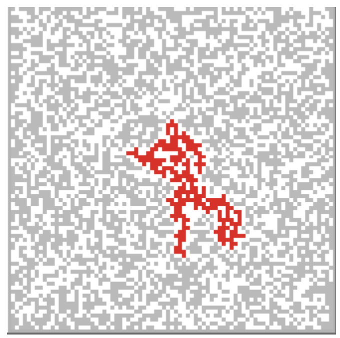


Site percolation on lattices

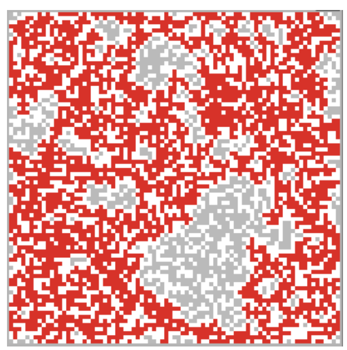
Fill each square with probability p



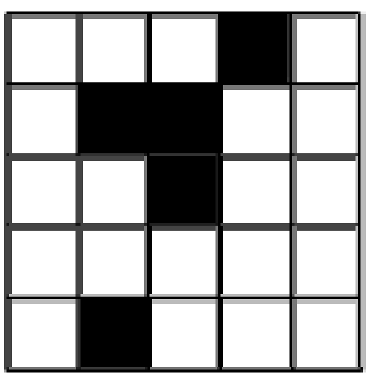
- **low p:** small isolated islands



- **p critical**: giant component forms, occupying finite fraction of infinite lattice.
  Size of other components is power law distributed



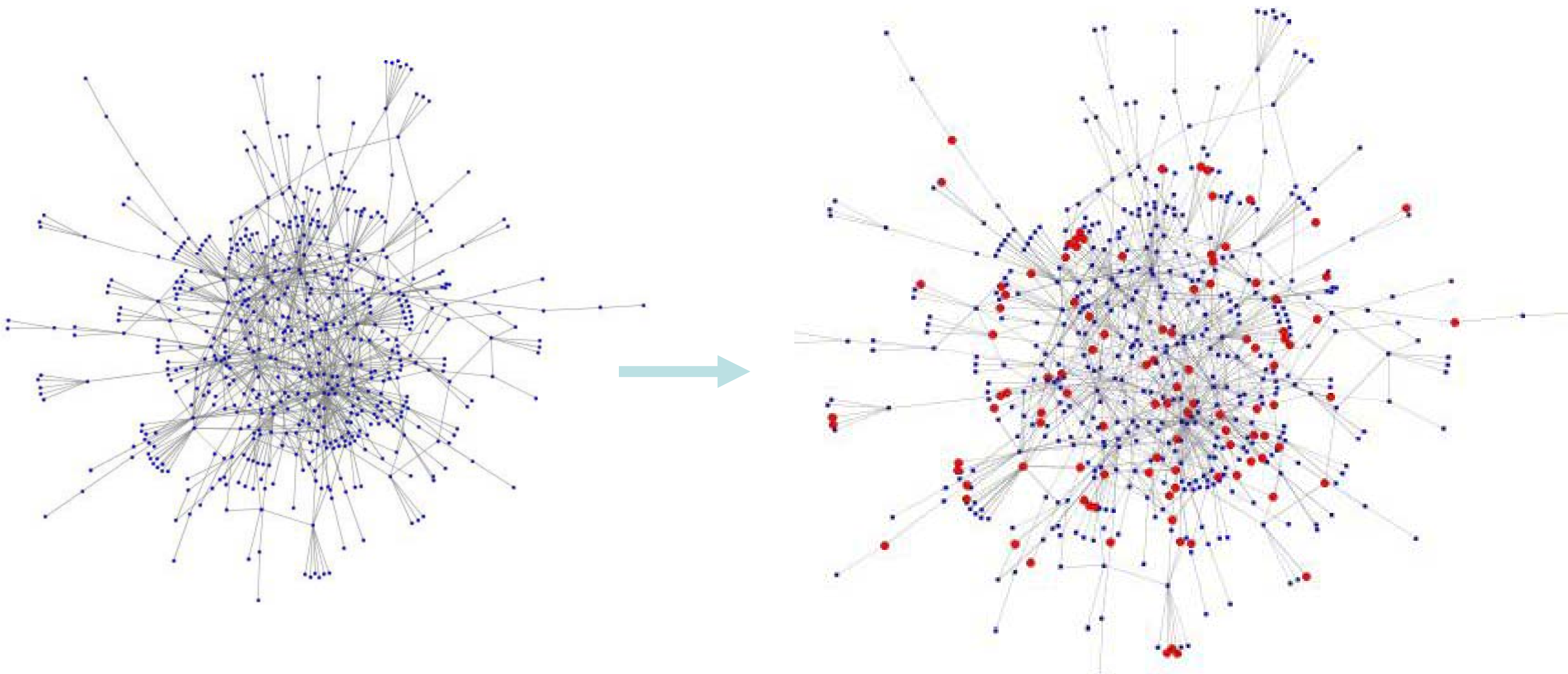
- **p above critical**: giant component rapidly spreads to span the lattice.
  Size of other components is O(1).



site percolation

Source: site percolation, http://mathworld.wolfram.com/BondPercolation.html

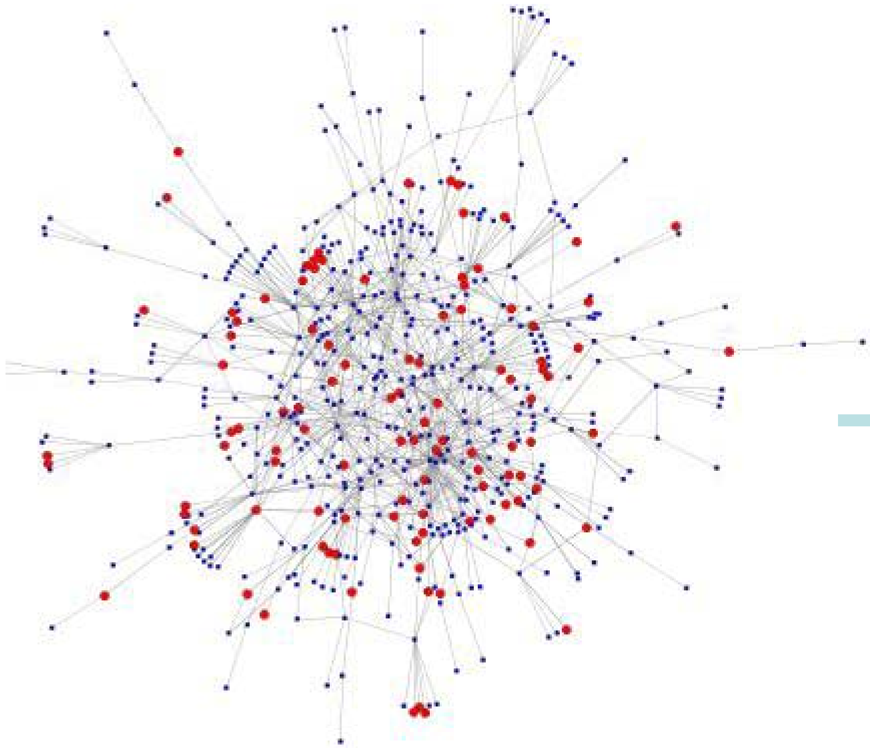
Percolation on Complex Networks



- 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 error

Example: gnutella network, 20% of nodes removed

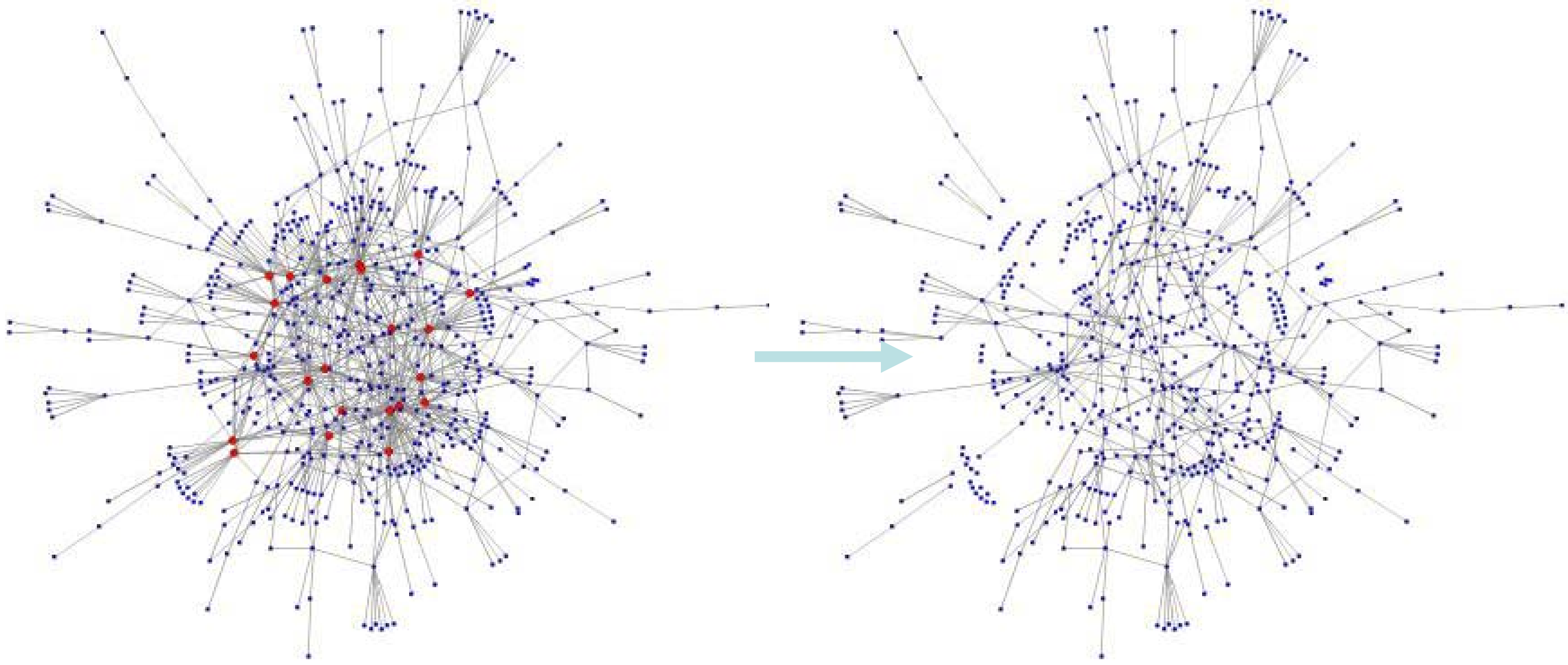


574 nodes in giant component

427 nodes in giant component

Targeted attacks are affective against scale-free networks

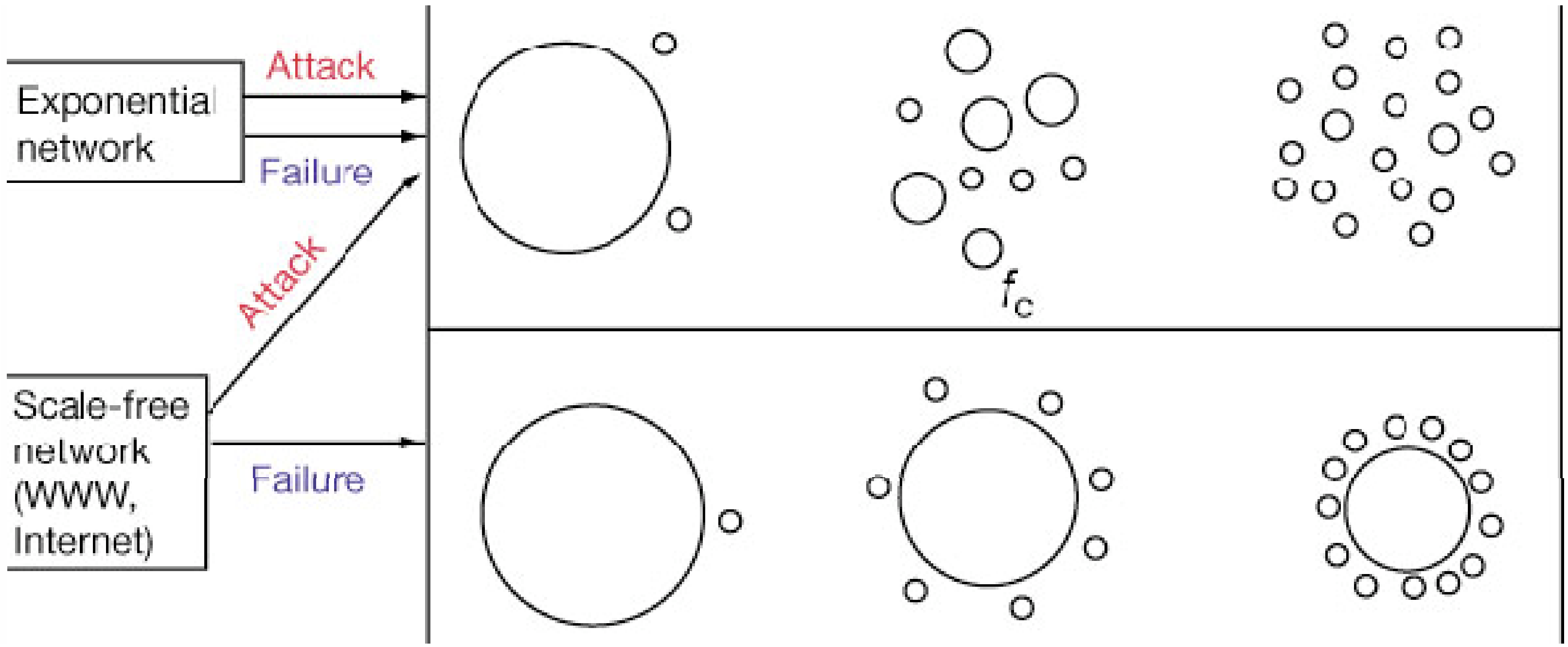
Example: same gnutella network, 22 most connected nodes removed (2.8% of the nodes)



574 nodes in giant component

301 nodes in giant component

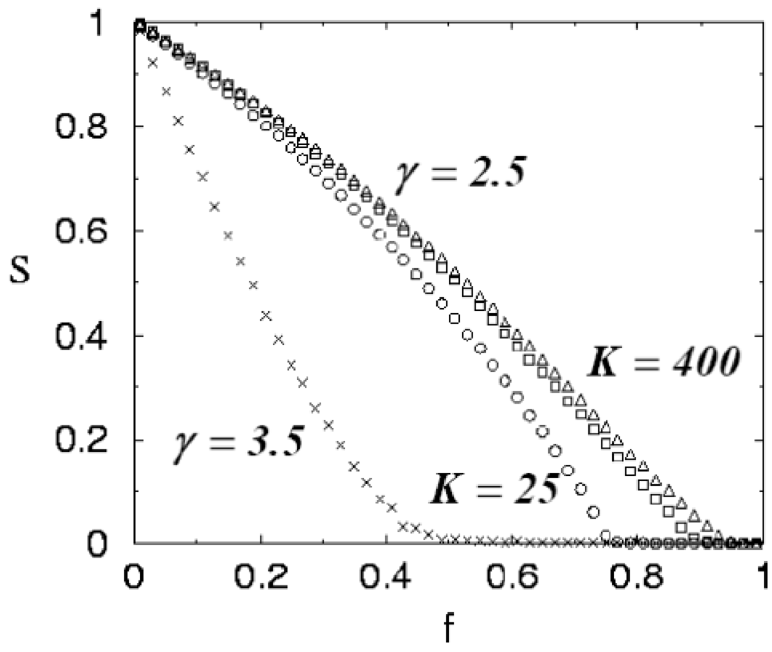
Random failures vs. attacks



Source: Error and attack tolerance of complex networks. Réka Albert, Hawoong Jeong and Albert-László Barabási. Nature 406, 378-382(27 July 2000); http://www.nature.com/nature/journal/v406/n6794/abs/406378A0.html

Percolation Threshold in scale-free networks

- What proportion of the nodes must be removed in order for the size (S) of the giant component to drop to 0?
- For scale free graphs there is always a giant component (the network always percolates)



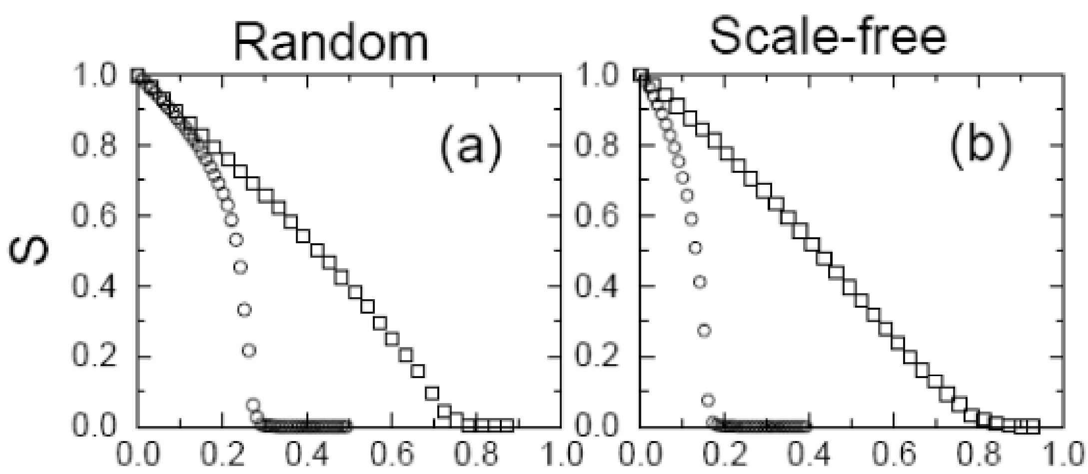
Source: Cohen et al., Phys. Rev. Lett. 85, 4626 (2000)

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

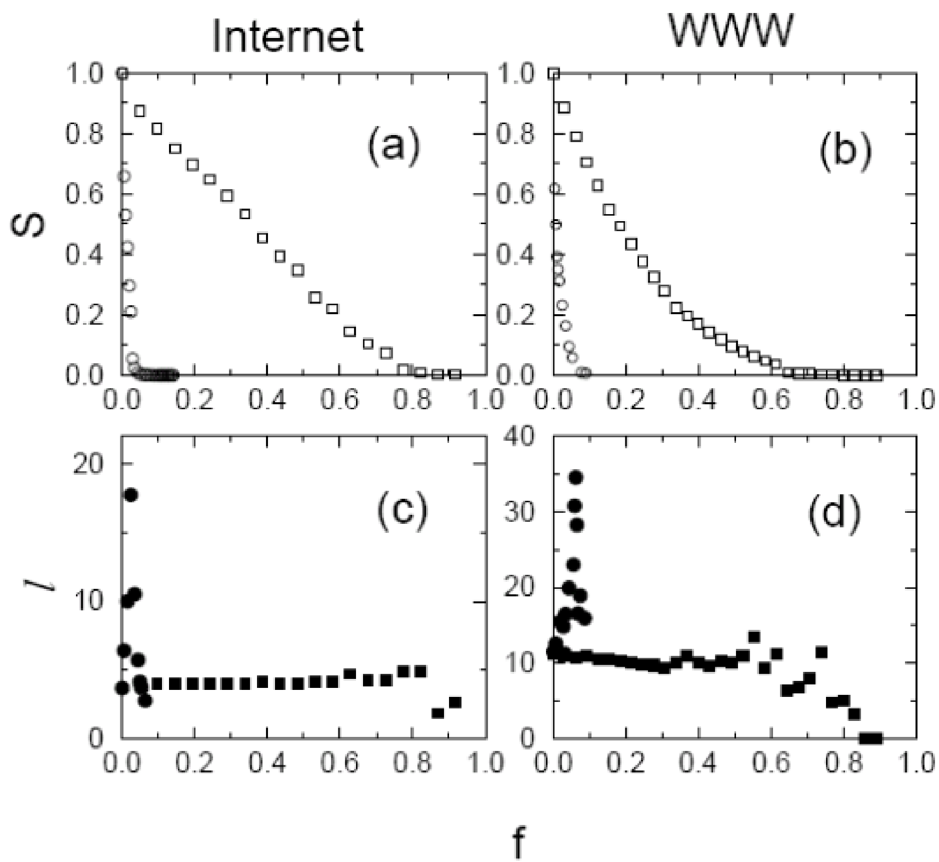
□ random failure

○ targeted attack



Source: **Error and attack tolerance of complex networks. Réka Albert, Hawoong Jeong and Albert-László Barabási. Nature 406, 378-382(27 July 2000); http://www.nature.com/nature/journal/v406/n6794/abs/406378A0.html**

Real networks

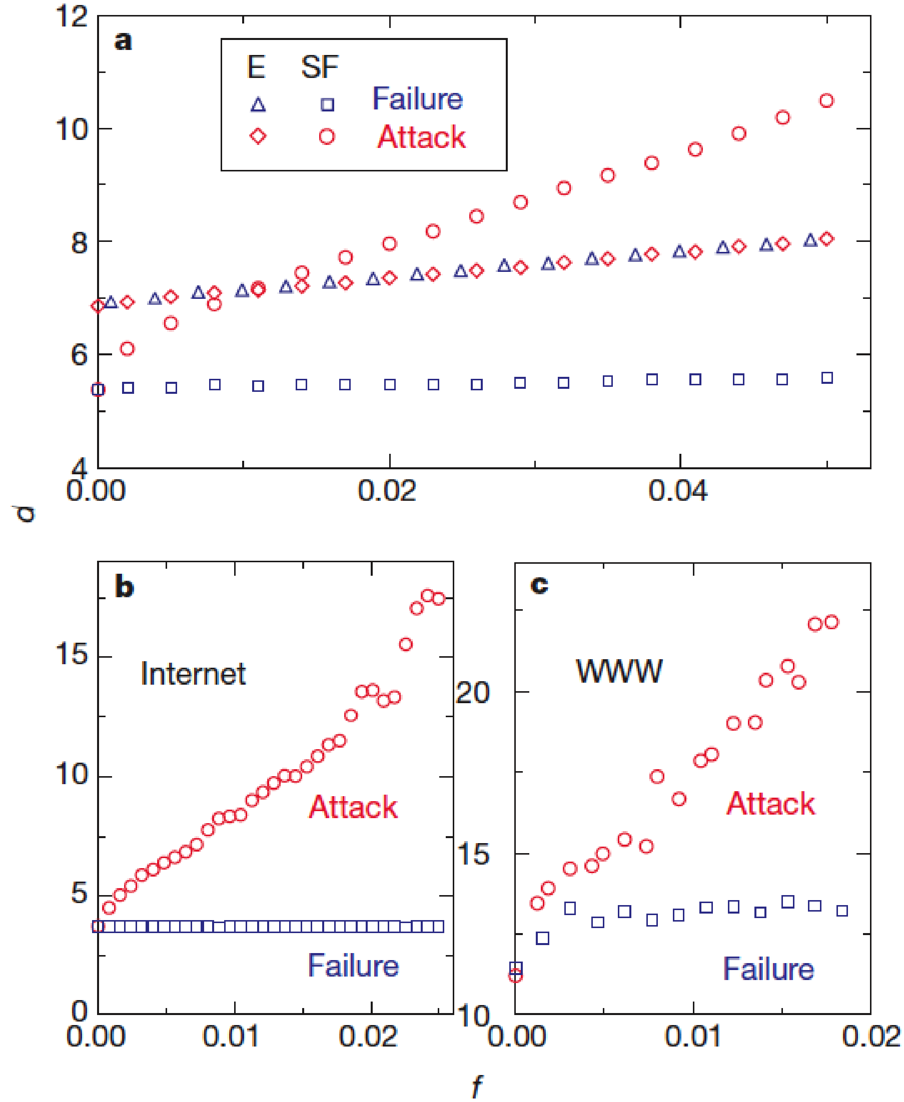


random failure

targeted attack

Source: Error and attack tolerance of complex networks. Réka Albert, Hawoong Jeong and Albert-László Barabási. Nature 406, 378-382(27 July 2000); http://www.nature.com/nature/journal/v406/n6794/abs/406378A0.html

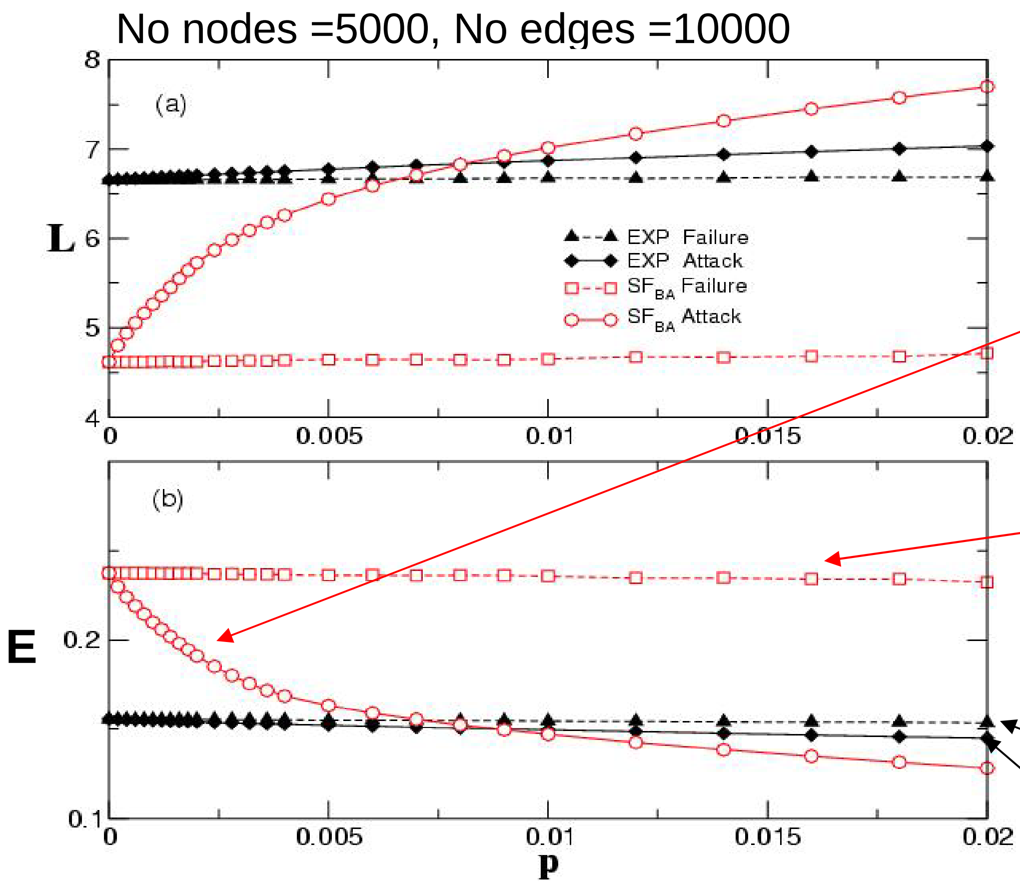
When the first few % of nodes removed



Source: Error and attack tolerance of complex networks. Réka Albert, Hawoong Jeong and Albert-László Barabási. Nature 406, 378-382(27 July 2000); http://www.nature.com/nature/journal/v406/n6794/abs/406378A0.html

Error/attack tolerance of global efficiency in scale-free networks

few removals



<u>Scale-Free (BA model)</u> (Heterogeneous)

Attacks: the removal of a tiny fraction of important nodes (2%) causes the network to lose 50% of its efficiency.

Errors: the network is nearly unaffected from the removal of a few nodes

<u>Erdös-Rényi Random graph (EXP)</u> (Homogeneous)

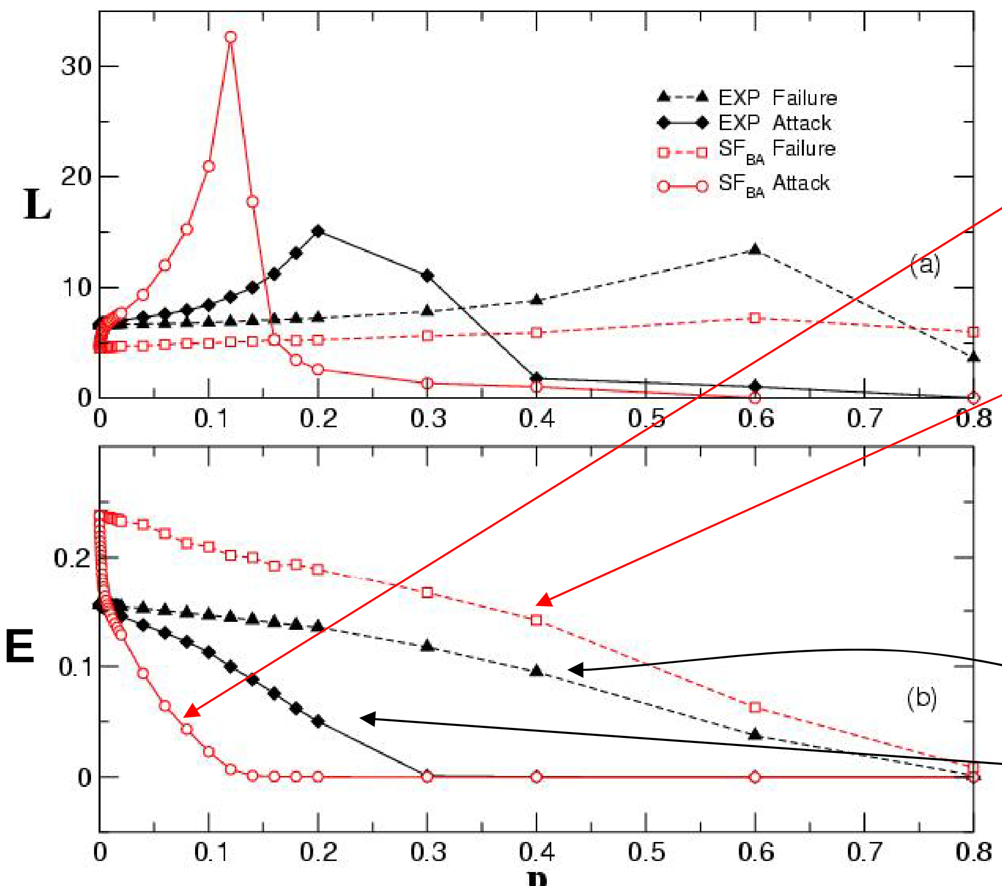
Attacks & Errors: the network is nearly unaffected from the removal of a few nodes

Soure: Crucitti, Latora, Marchiori, Rapisarda, Physica A 320 (2003) 622

Error/attack tolerance of global efficiency in scale-free networks

many removals

No nodes =5000, No edges =10000



Soure: Crucitti, Latora, Marchiori, Rapisarda, Physica A 320 (2003) 622

Scale-Free (BA model) (Heterogeneous)

Attacks: global efficiency of the network is completely destroyed, removing 10% of important nodes.

Errors: network's efficiency slowly decreases.

Erdös-Rényi Random graph (EXP) (Homogeneous)

Attacks & Errors: differences are evident, but less pronounced than in the BA model.

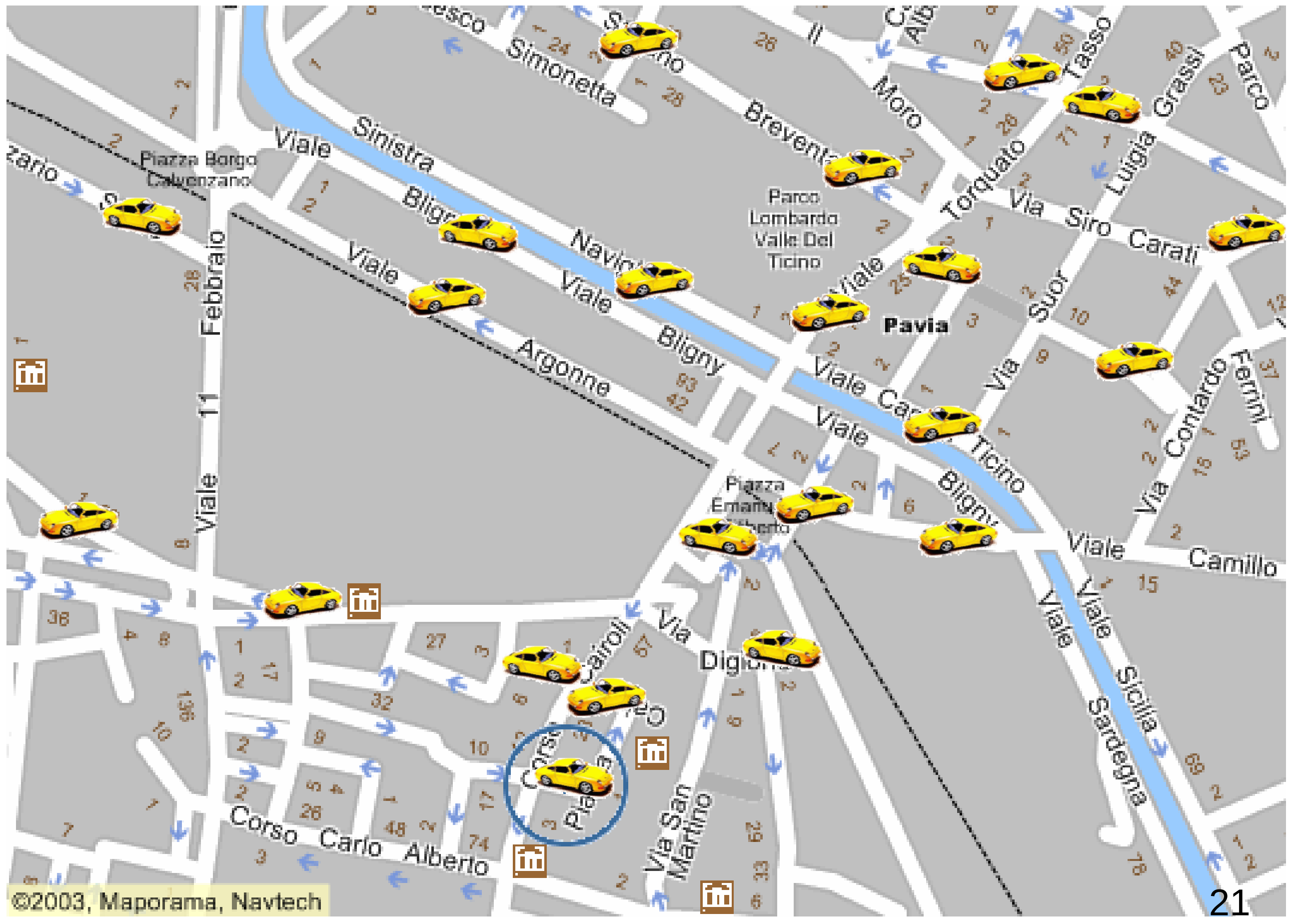
Let us consider a real system: the Pavia road system

Nodes = Crossings

Edges = Streets

Edge weights:

τ_{ij} = time spent in order to go from node i to node j



Soure: Crucitti, at al

Let us consider a real system: the Pavia road system

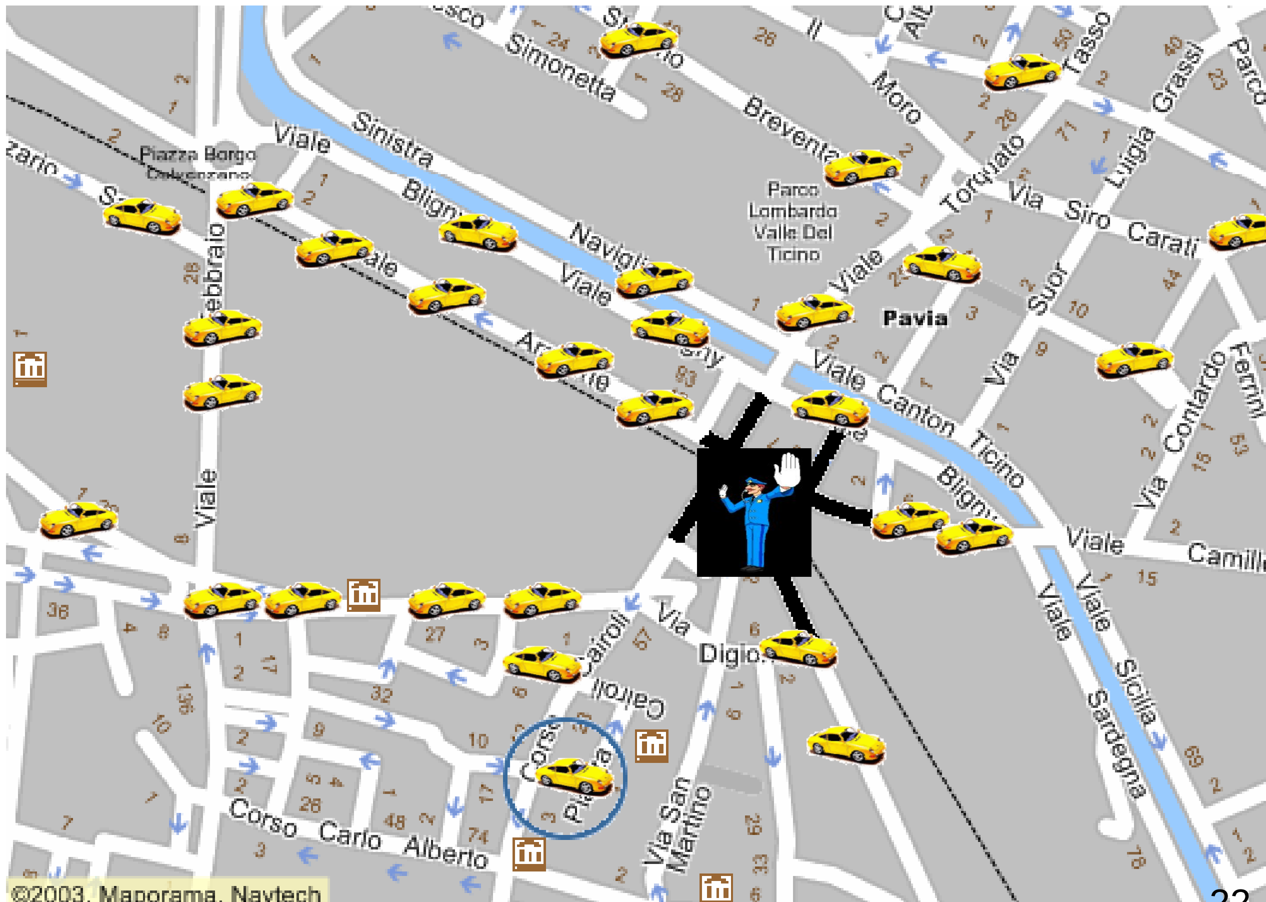
If today Piazza Emanuele iliberto is not practicable

↓

People have to find an alternative path.

↓

Load redistribution



Soure: Crucitti, at al

Let us consider a real system: the Pavia road system

Load redistribution can cause traffic in alternative routes.

↓

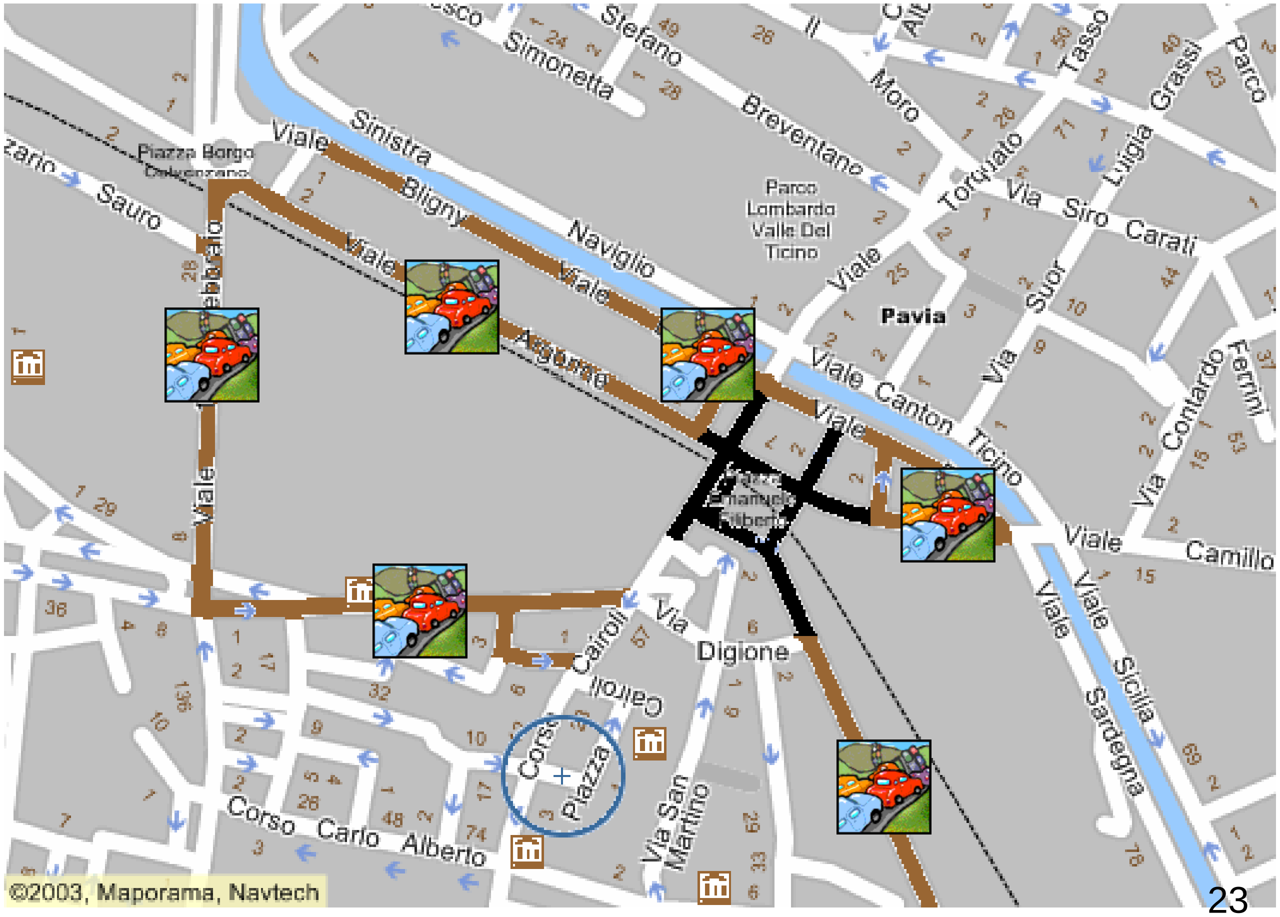
Overload

↓

Traffic hold up

↓

Degradation in efficiency
(times τ_{ij} grow longer)



Soure: Crucitti, at al

Let us consider a real system: the Pavia road system

Traffic hold up leads again to the choice of alternative routes

↓

New overload

↓

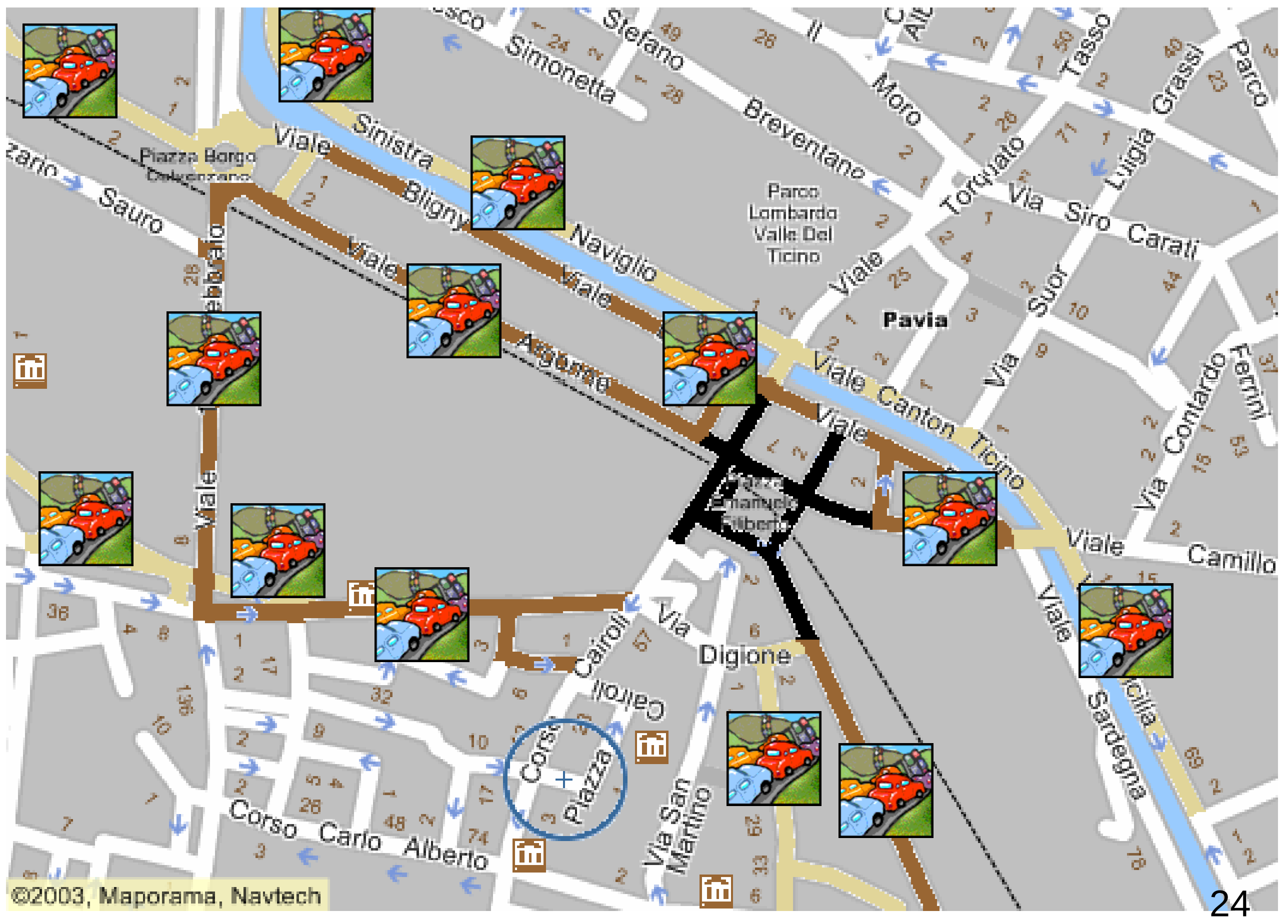
New degradation in efficiency

↓

…

↓

Cascading effect



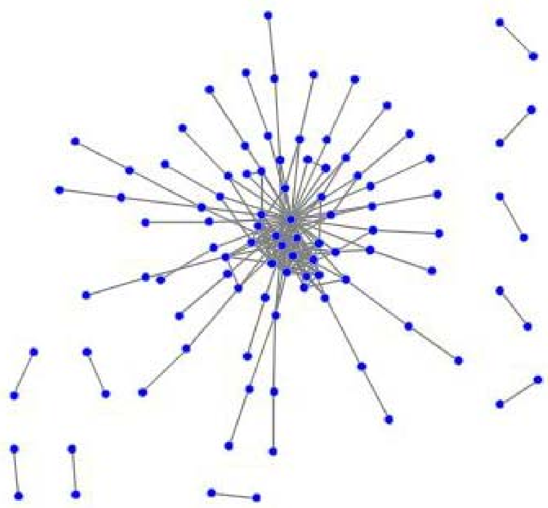
Soure: Crucitti, at al

Let us consider a real system: the Pavia road system

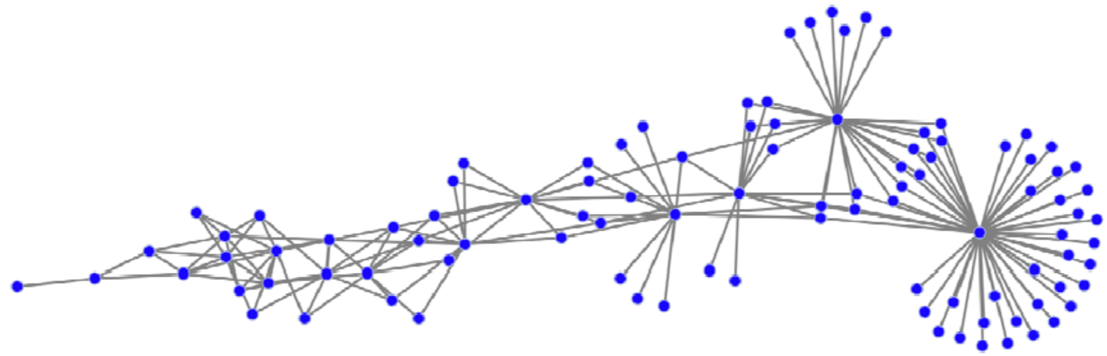
…and the result is…

Degree assortativity and resiliency

will a network with positive or negative degree assortativity be more resilient to attack?

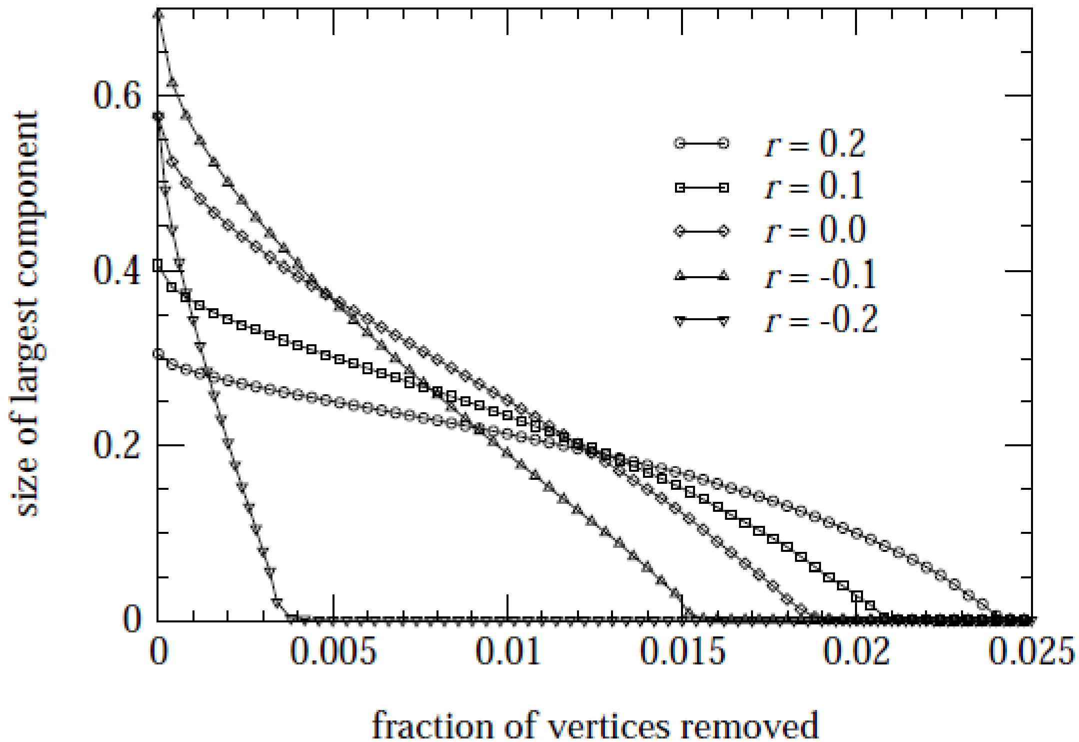


assortative



disassortative

Degree assortativity and resiliency



Each curve is for a single network of 107 vertices generated using the Monte Carlo method with different assortativity values

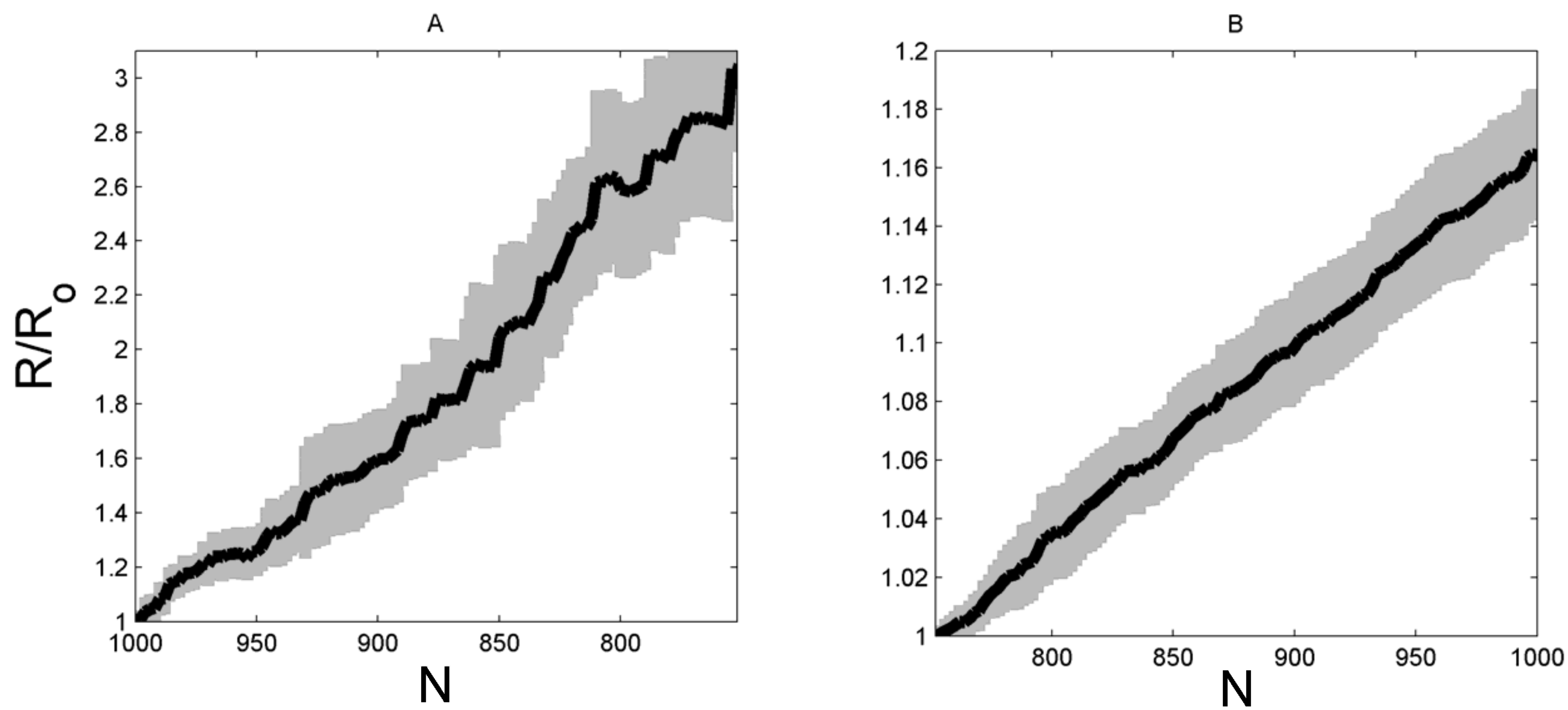
Soure: MEJ Newman, Physial Review E, 2002

Error tolerance of spectral properties

- Let us consider undirected and unweighted networks
- The eigenratio of the Laplacian R:
  - the largest eigenvalue / the second smallest eigenvalue
- The eigenratio represents somehow the synchronizability of the network (we will see later on)
- How random removal of nodes affect the synchronizability?
- Remember as a node is removed all its attaching edges are also removed

Source: Jalili, 2010

Error tolerance of spectral properties

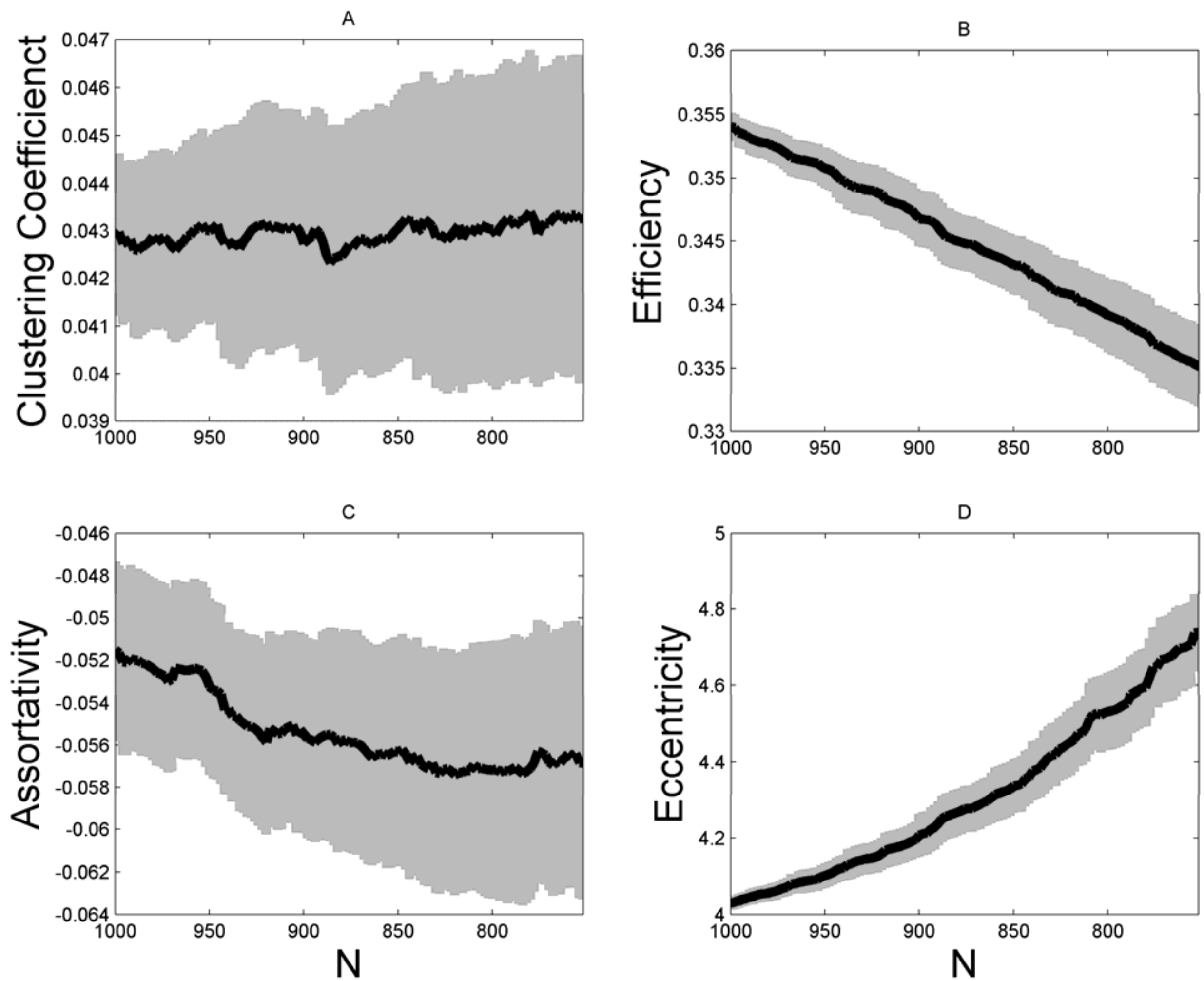


A) Scale-free networks are constructed with *N* = 1000, and then, nodes are randomly removed from the networks. B) Scale-free networks are grown starting with *N* = 750. Graphs show averages along with the standard deviations over 50 realizations.

Source: Jalili, Physica A 2011

Error tolerance of spectral properties

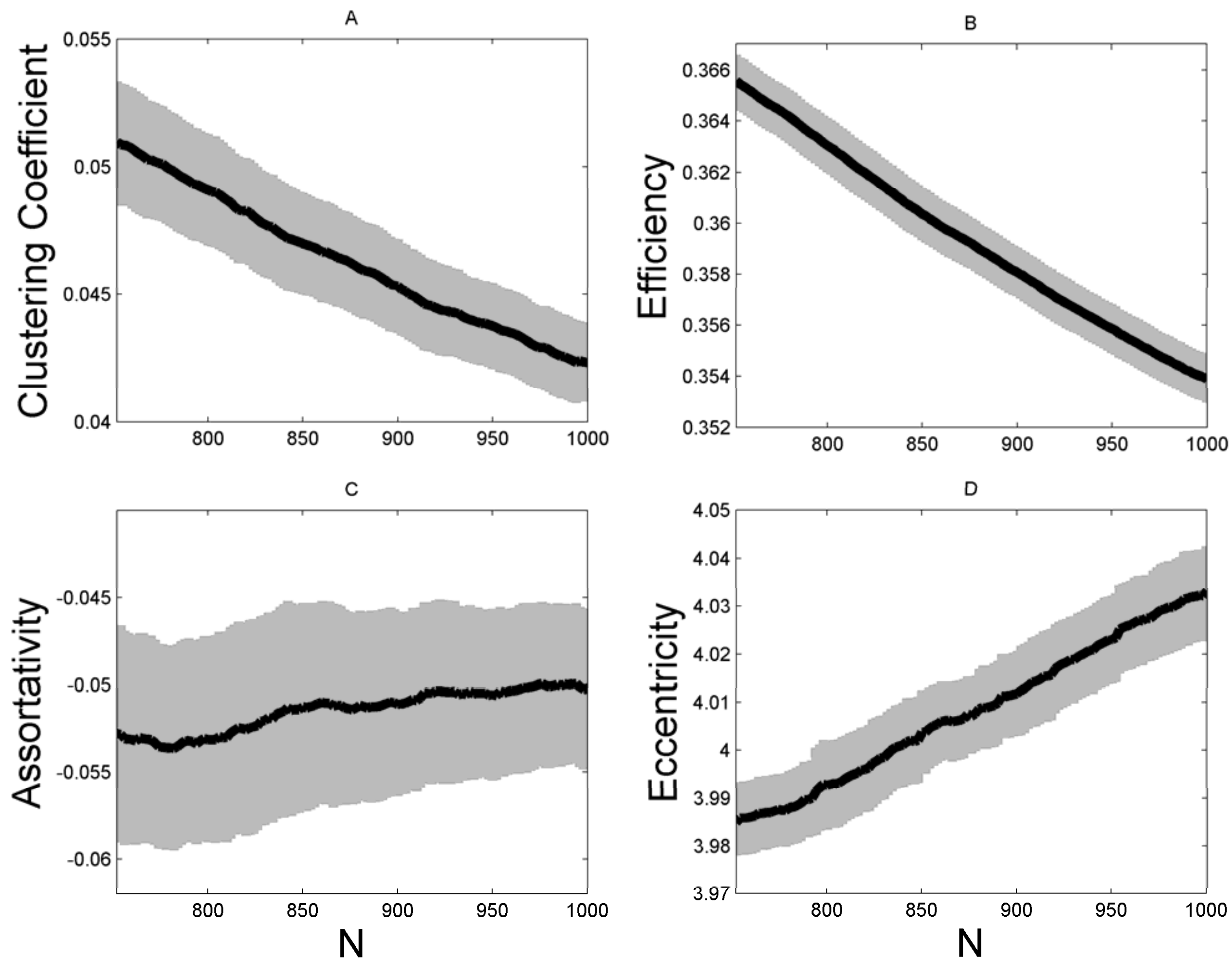
A) clustering coefficient, B) efficiency, C) assortativity, and D) eccentricity, as a function of network size in scale-free networks with *m* = 5. The networks are constructed with *N* = 1000, and then, nodes are randomly removed from the networks. Graphs show averages along with the standard deviations over 50 realizations.



Source: Jalili, Physica A 2011

Error tolerance of spectral properties

A) clustering coefficient, B) efficiency, C) assortativity, and D) eccentricity, as a function of network size in scale-free networks with *m* = 5. The networks are grown starting with *N* = 750. Graphs show averages along with the standard deviations over 50 realizations.



Source: Jalili, Physica A 2011

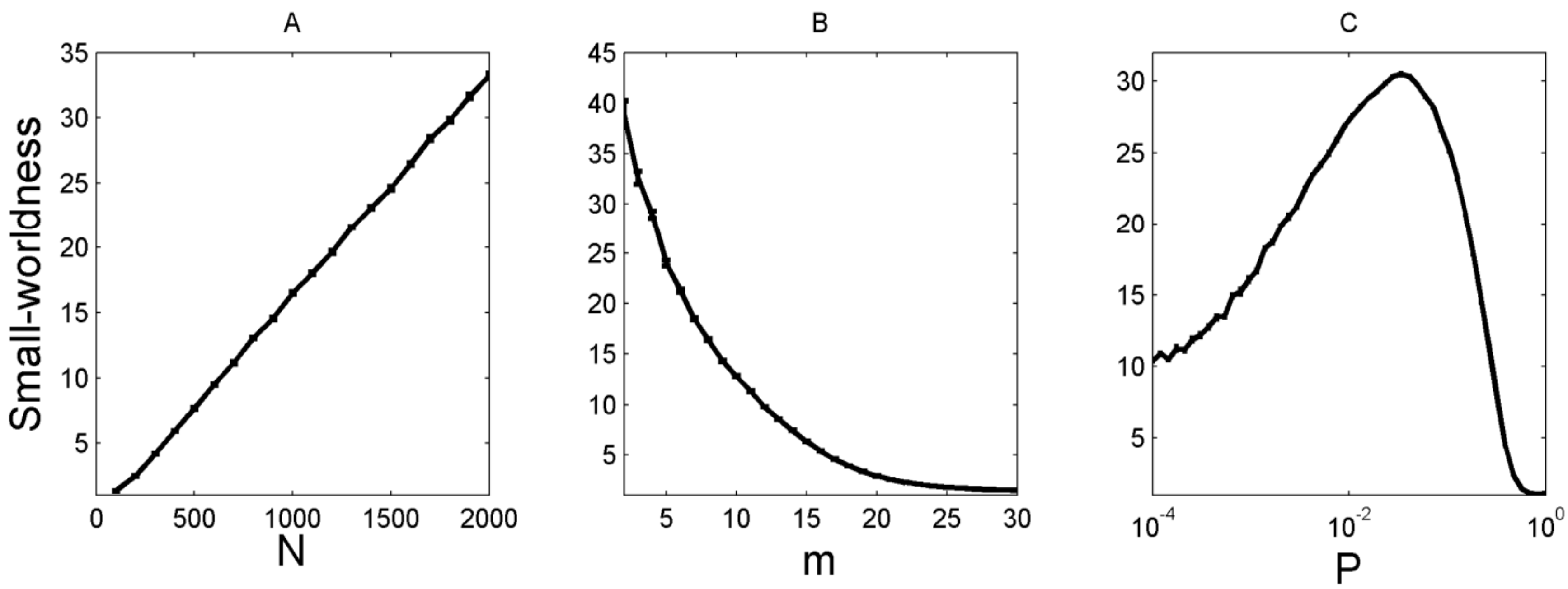
Error/attack tolerance of SW

- Many networks are small-world
- We can measure to what extent the networks are small-world

$$S = \frac{E_{local}}{E_{local-random}} \times \frac{E_{global}}{E_{global-random}}$$

- If S > 1, the network is small-world
- For the networks of the same size and average degree, the larger the value of S is the more the small-world the network is
- How S changes with random/intentional removal of nodes

Error/attack tolerance of SW

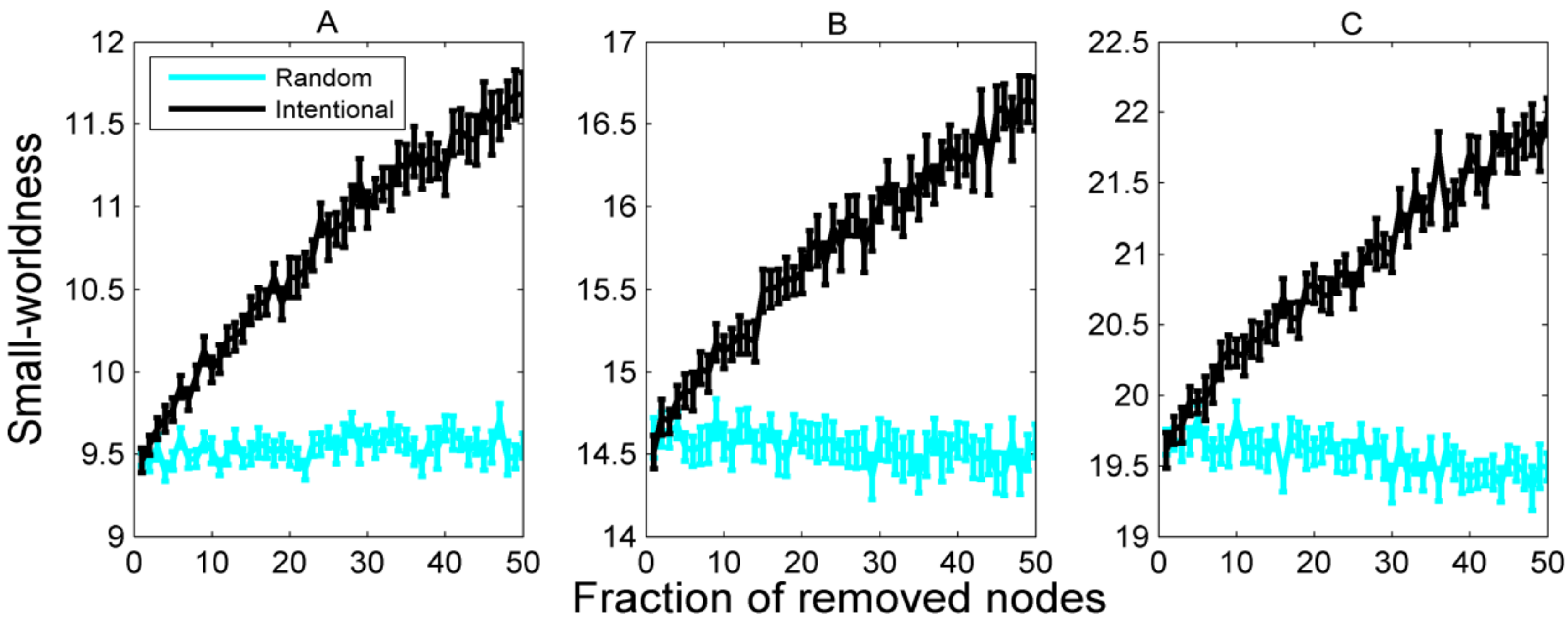


The small-worldness as a function of A) *N* (*m* = 8 and *P* = 0.1), B) m (*N* = 1000 and *P* = 0.1), and C) *P* (*N* = 1000 and *m* = 8).

m: average degree, N: size, P: rewiring probability

Source: Jalili, Informetrics 2011

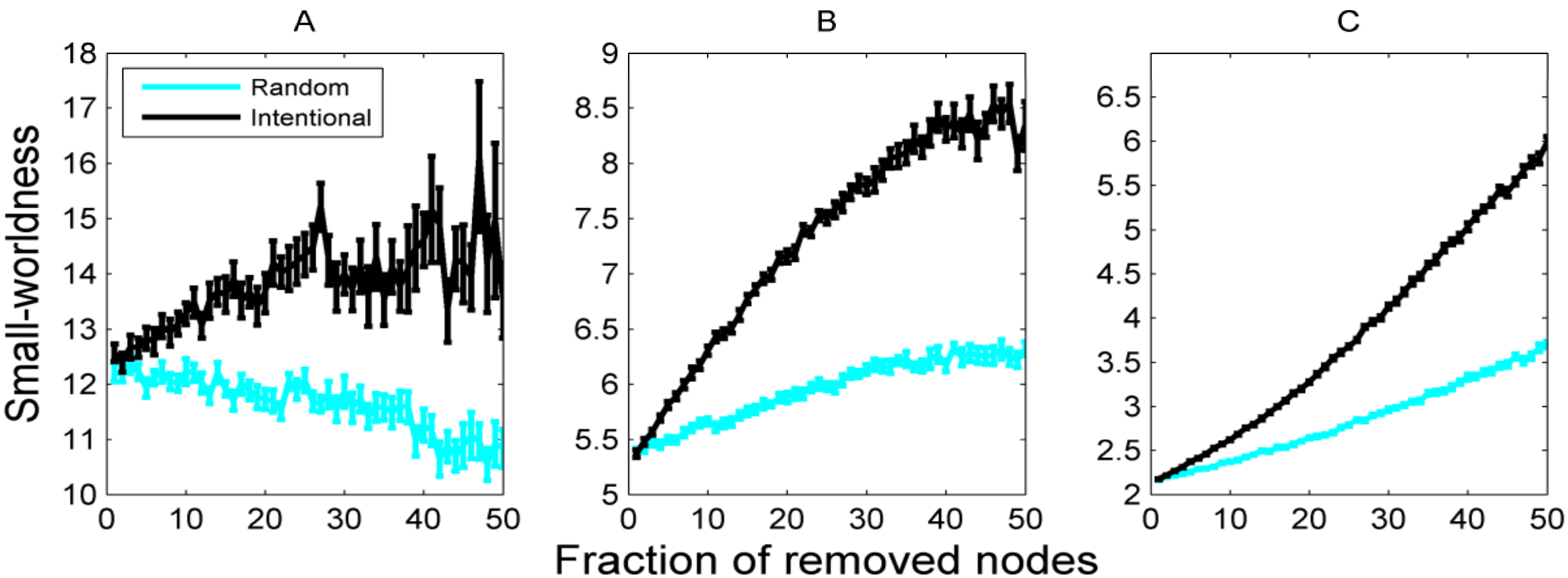
Error/attack tolerance of SW



The small-worldness as a function of the fraction of (randomly or systematically) removed nodes in Watts-Strogatz networks with $m = 8$, $P = 0.1$, and different number of nodes; A) $N = 600$, B) $N = 900$, and C) $N = 1200$.

Source: Jalili, Informetrics 2011

Error/attack tolerance of SW

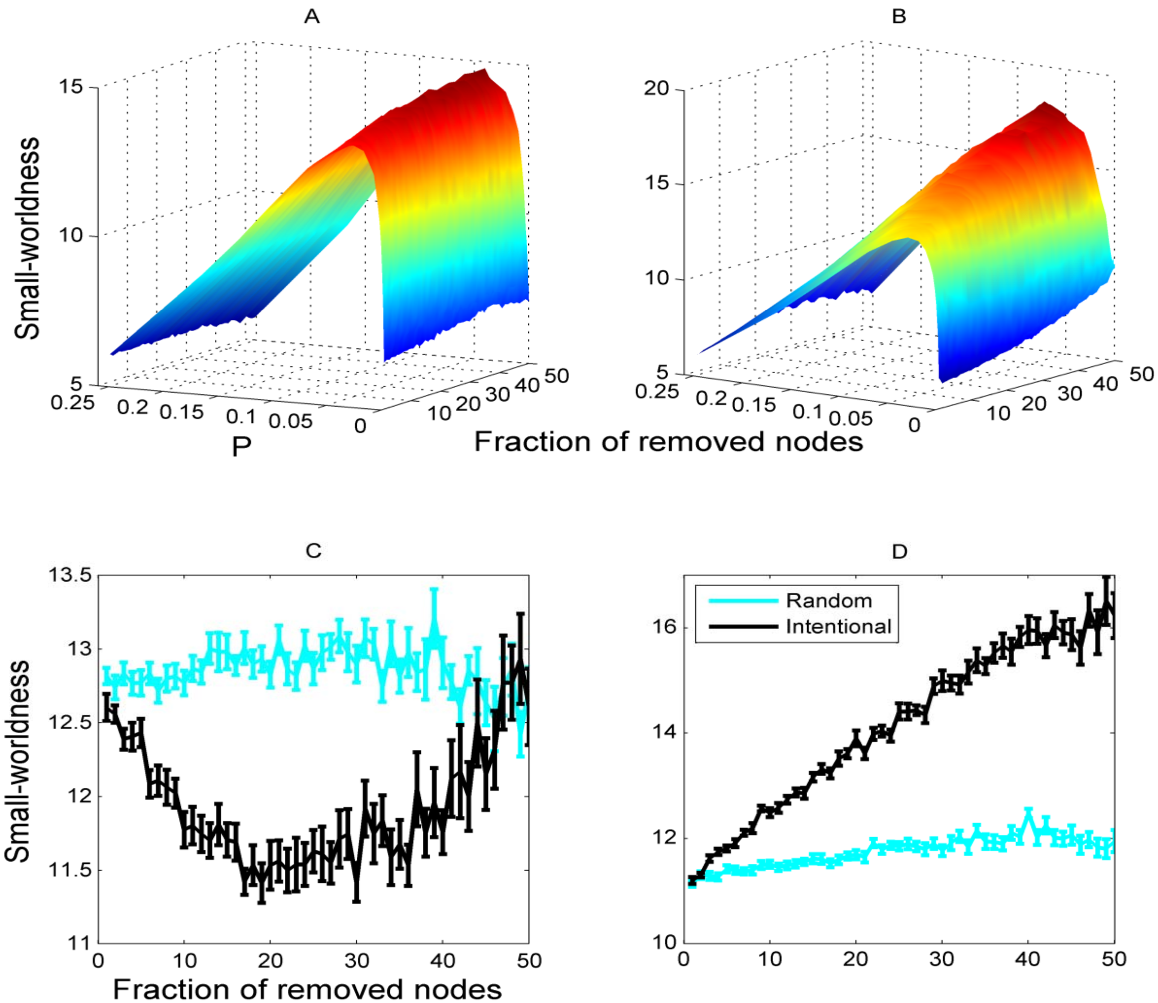


The small-worldness as a function of the fraction of removed nodes in Watts-Strogatz networks with N = 1000, P = 0.1, and different average degree; A) m = 5, B) m = 10, and C) m = 15.

Source: Jalili, Informetrics 2011

Error/attack tolerance of SW

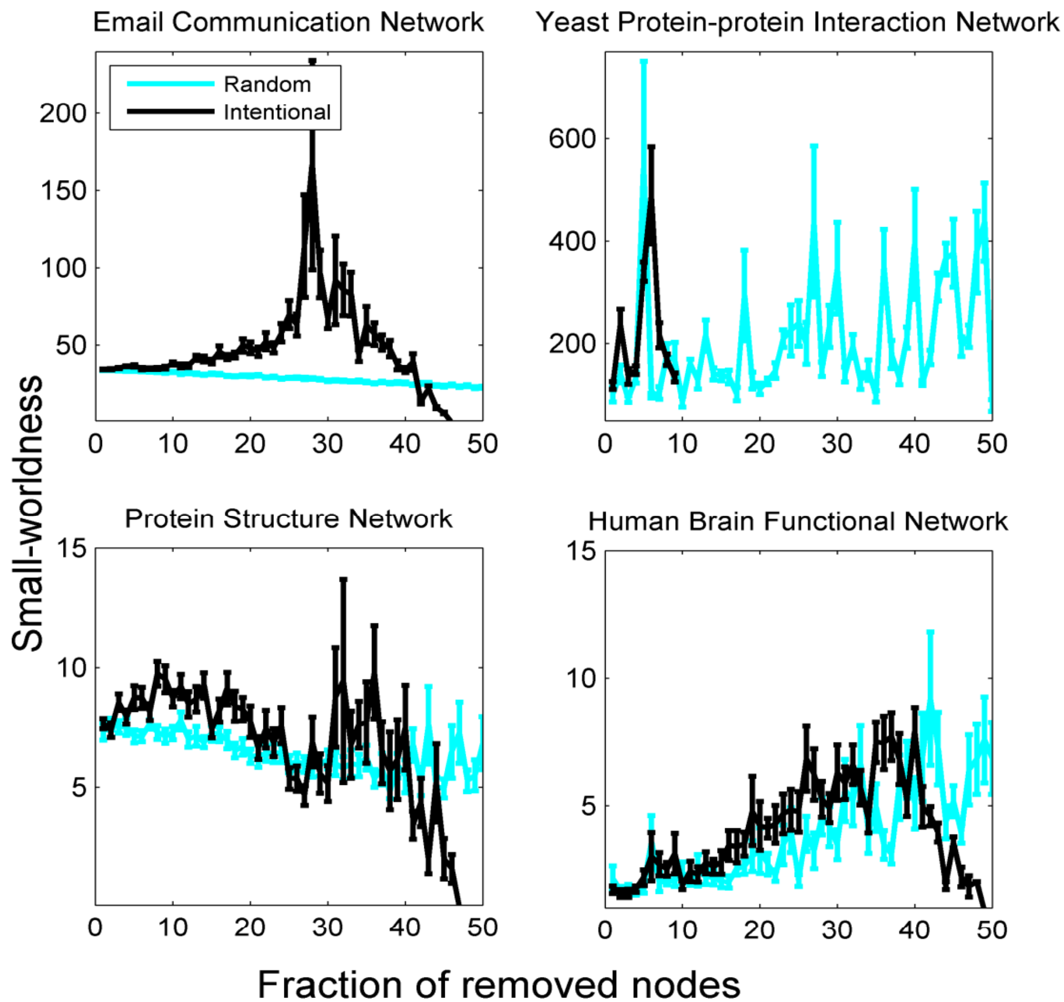
The small-worldness as a function of the rewiring probability *P* and the fraction of, A) Randomly and B) Systematically, removed nodes in Watts-Strogatz networks with *m* = 8, *N* = 1000. The figure also shows the small-worldness as a function of the fraction of removed nodes in two values of *P*; C) *P* = 0.005 and D) *P* = 0.05.



Source: Jalili, Informetrics 2011

Error/attack tolerance of SW

The small-worldness as a function of the fraction of removed nodes in a number of real-world networks



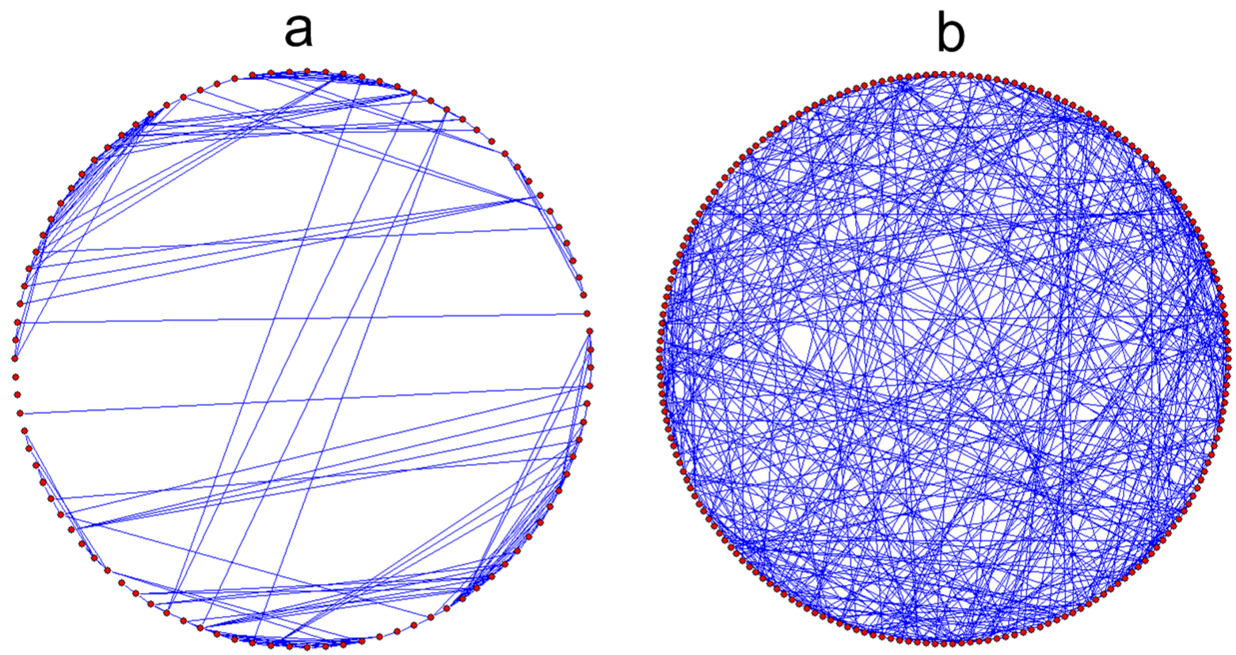
Source: Jalili, Informetrics 2011

Failure tolerance of motifs

- Motifs are important subgraphs in networks
- Network function depends on motif structure
- Let us see how failures in the edges influences motifs:
  - Random failure: at each step, one edge is randomly chosen and removed from the network
  - Failure based on the node degrees: at each step, the quantity $k_i k_j$ is calculated for each edge e_{ij}, and then, the edge with the maximum amount of $k_i k_j$ is removed from the network. k_i is degree of node *i.*
  - Failure based on the edge betweenness centrality: at each step, the edge with maximum betweenness L_{ij} is removed.
  - Failure based on the node closeness centrality: at each step, the edge with maximum $C_i C_j$ is removed where C_i is betweenness of node *i*

Source: Mirzasoleiman and Jalili, PLoS ONE 2011

Failure tolerance of motifs

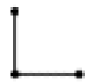
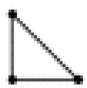
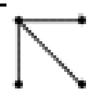
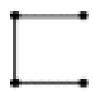
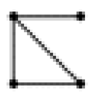
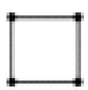
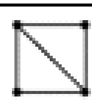
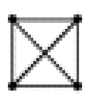


Network Type	N	<k>	std(k)	P	C
Protein structure	99	4.2828	0.4748	5.2607	0.3600
Functional human brain	200	4.5400	0.5690	5.2200	0.2858

a) Protein structure network and (b) human brain functional network extracted through functional magnetic resonance imaging

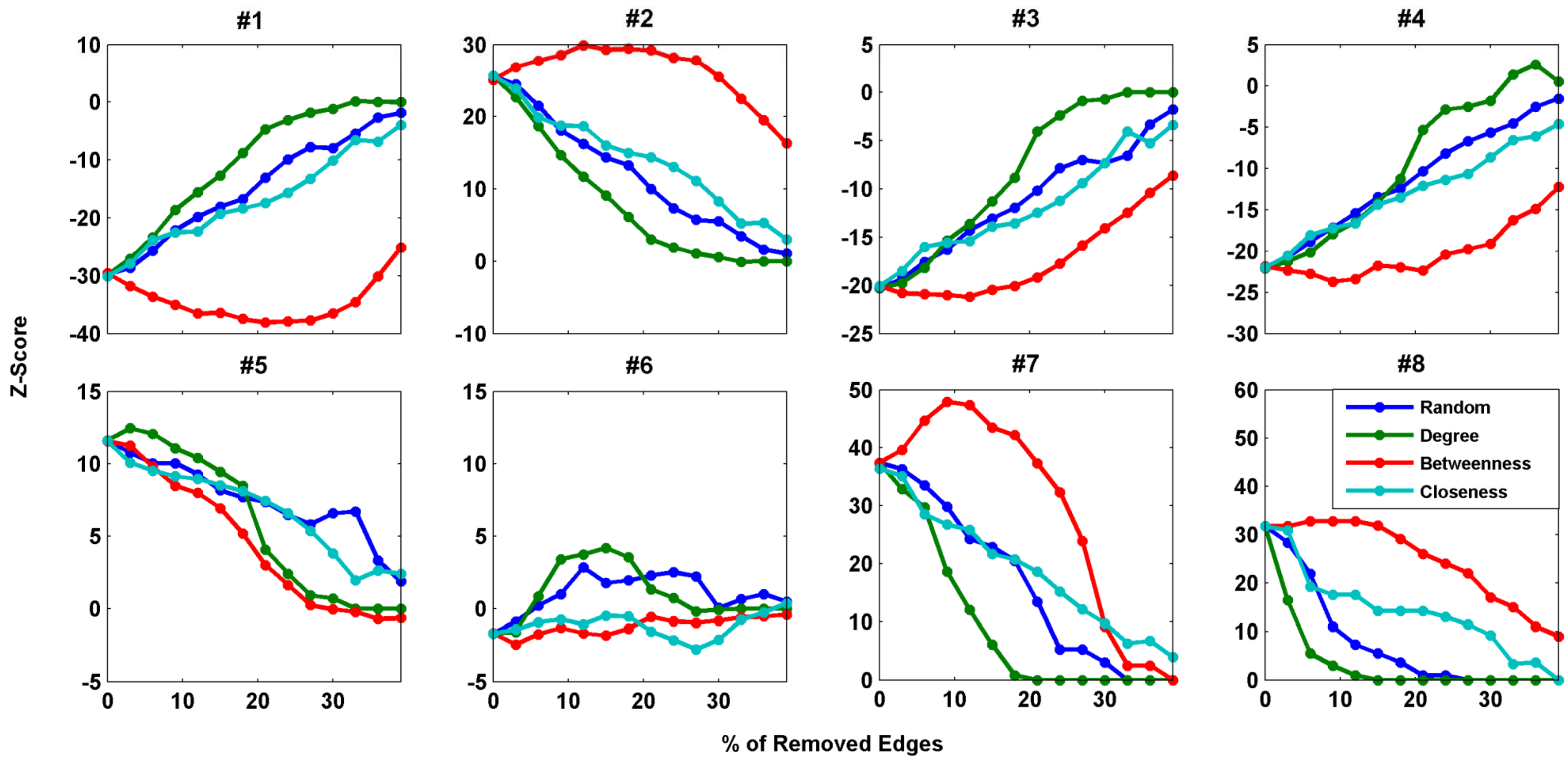
Source: Mirzasoleiman and Jalili, PLoS ONE 2011

Failure tolerance of motifs

Network Type		Protein structure			Functional Human brain		
Motif Number	**Motif Structure**	Motif frequencies	Non-normalized Z-scores	normalized Z-scores	Motif frequencies	Non-normalized Z-scores	normalized Z-scores
#1		544	-29.581	-0.0060	1388	-44.913	-0.0034
#2		130	25.086	0.0051	187	38.600	0.0029
#3		294	-20.086	-0.0041	1008	-33.844	-0.0025
#4		1359	-21.871	-0.0044	4020	-34.167	-0.0026
#5		661	11.529	0.0023	1196	24.000	0.0018
#6		29	-1.687	-0.0003	88	6.351	0.0005
#7		150	37.333	0.0076	205	81.360	0.0061
#8		38	31.666	0.0064	19	17.272	0.0013

Source: Mirzasoleiman and Jalili, PLoS ONE 2011

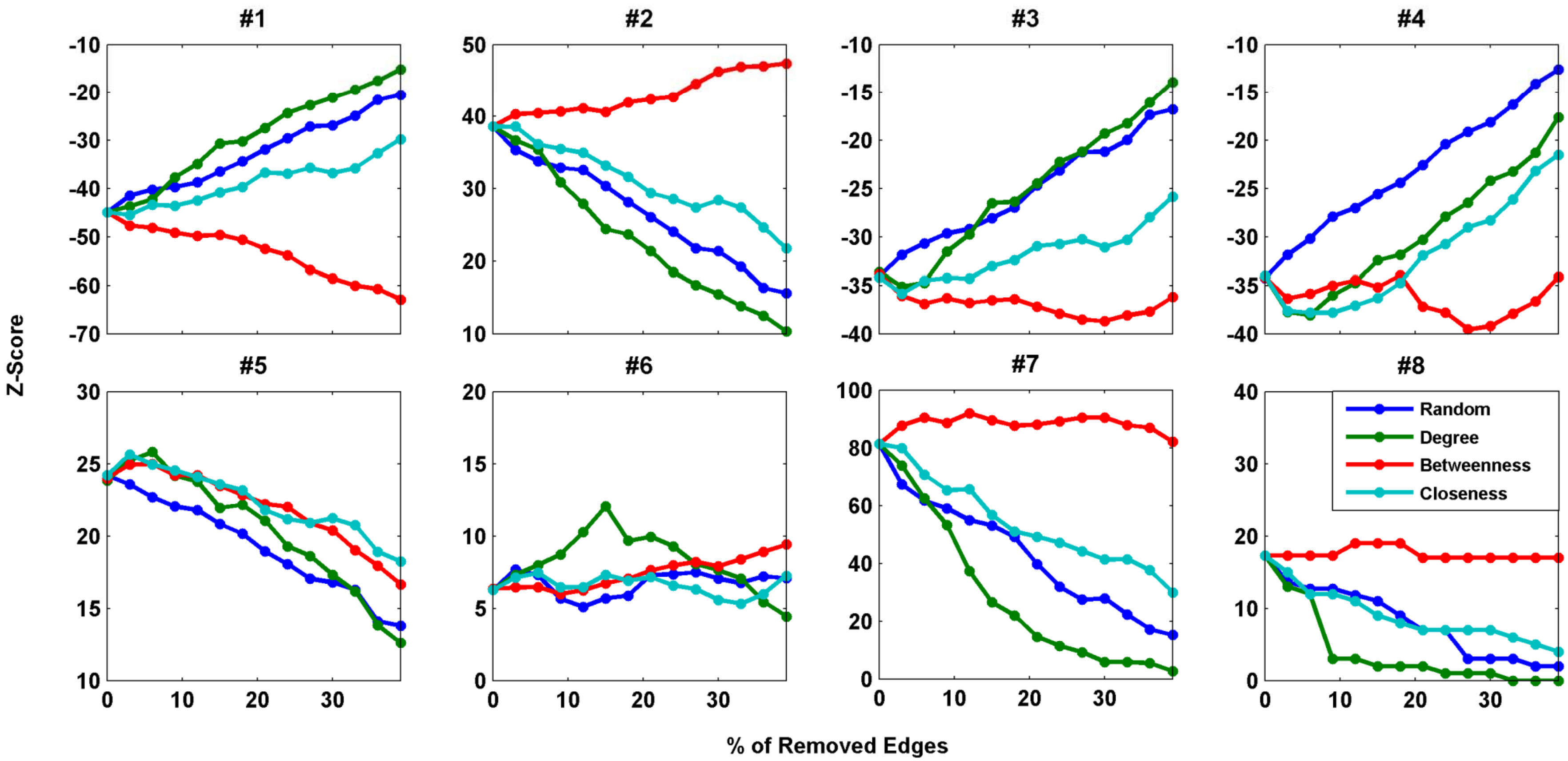
Failure tolerance of motifs



***Z*-score of motifs #1 - #8 as a function of the percentage of removed edges for protein structure network**

Source: Mirzasoleiman and Jalili, PLoS ONE 2011

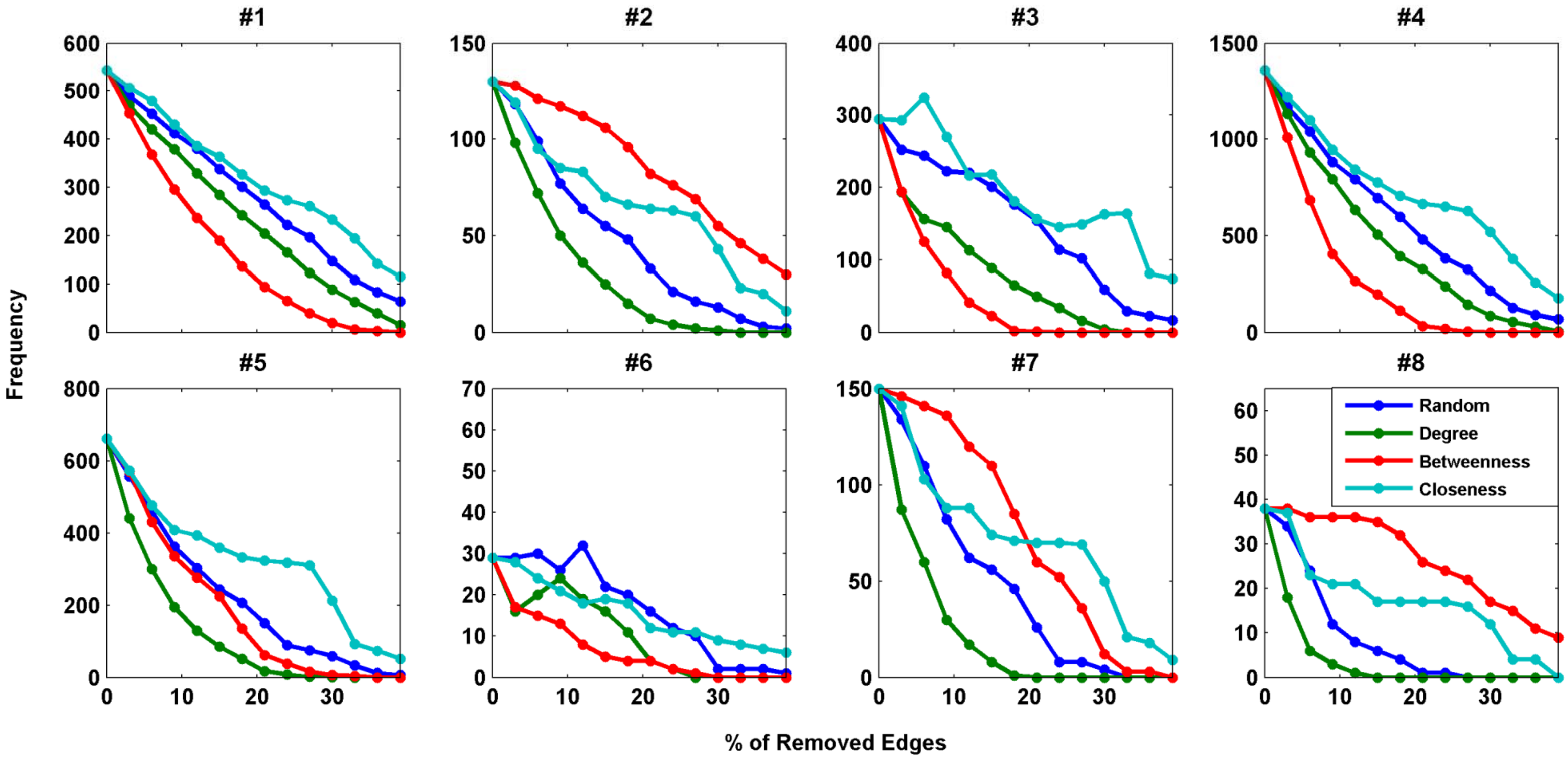
Failure tolerance of motifs



***Z*-score of motifs #1 - #8 as a function of the percentage of removed edges for human brain functional network**

Source: Mirzasoleiman and Jalili, PLoS ONE 2011

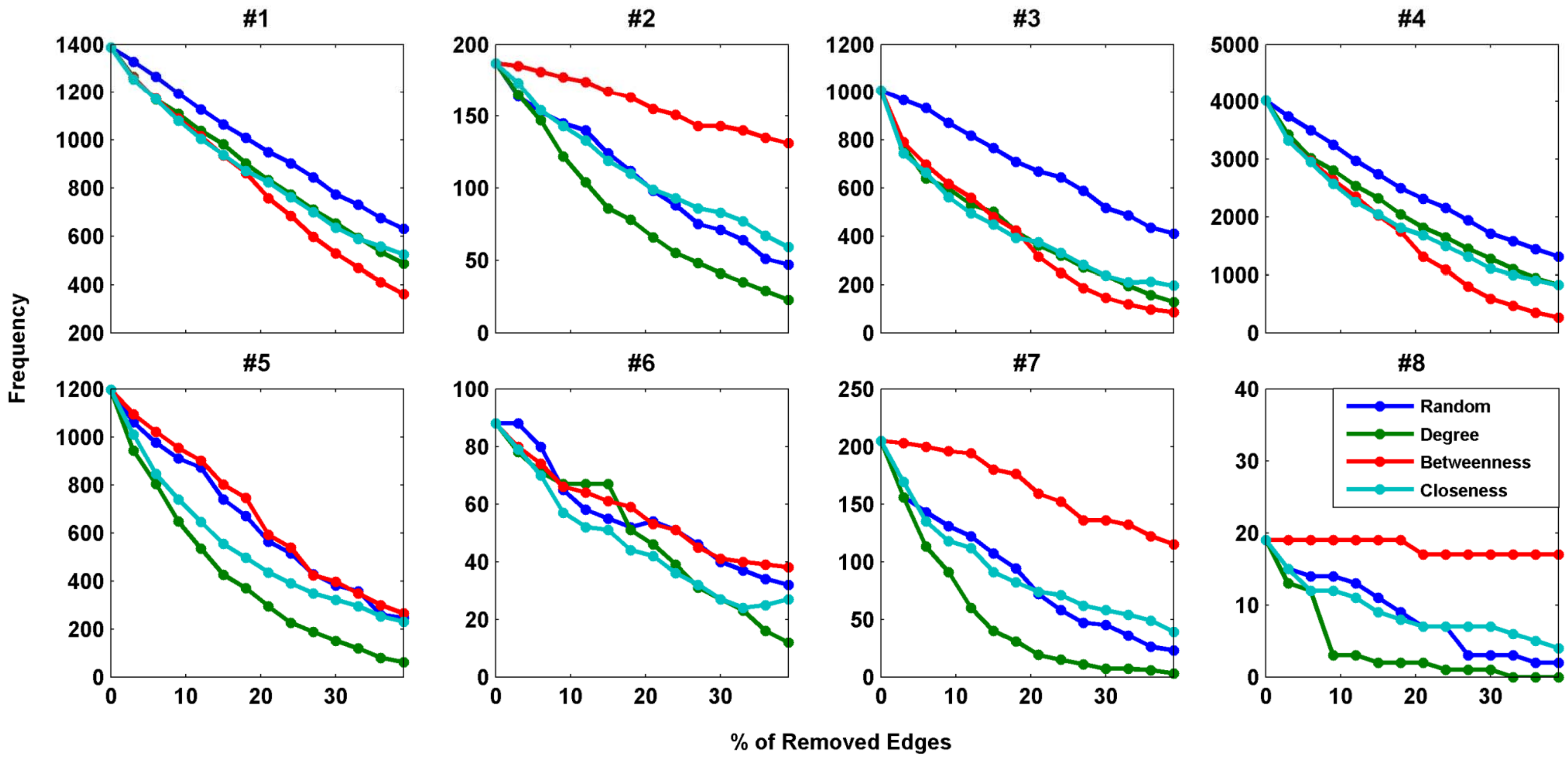
Failure tolerance of motifs



Frequencies of motifs #1 - #8 as a function of the percentage of removed edges for protein structure network

Source: Mirzasoleiman and Jalili, PLoS ONE 2011

Failure tolerance of motifs



Frequencies of motifs #1 - #8 as a function of the percentage of removed edges for human brain functional network

Source: Mirzasoleiman and Jalili, PLoS ONE 2011

Failure tolerance of motifs

- Although biological networks have been shown to be robust against random failures in terms of network connectedness and efficiency, such failures can have destructive effects on network motifs
- random failures could destroy motif structure
- Degree-based systematic failure had the most destructive role in most cases, i.e. causing in the largest decrease in the frequency of occurrence and absolute value of the *Z*-scores
- Attacks in the highly loaded edges had the least influence on the motif profile

Readings

- Crucitti P, Latora V, Marchiori M, & Rapisard A (2003) Efficiency of scale-free networks: error and attack tolerance. *Physica A* 320:622-642.
- Jalili M (2011) Synchronizability of dynamical scale-free networks subject to random errors. *Physica A* 390:4588-4595.
- Mirzasoleiman B , & Jalili M (2011) Failure tolerance of motif structure in biological networks. *PLoS ONE* 6:e20512.
- Jalili, M (2011) Error and attack tolerance of small-worldness in complex networks. *Journal of Informetrics* 5:422-430.