Networks as Critical Infrastructures: Robustness

Carlo PICCARDI

DEIB - Department of Electronics, Information and Bioengineering
Politecnico di Milano, Italy

email carlo.piccardi@polimi.it
https://piccardi.faculty.polimi.it

Robustness (or resiliency) is the ability of a system to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.

For networks, typical faults are modeled as:

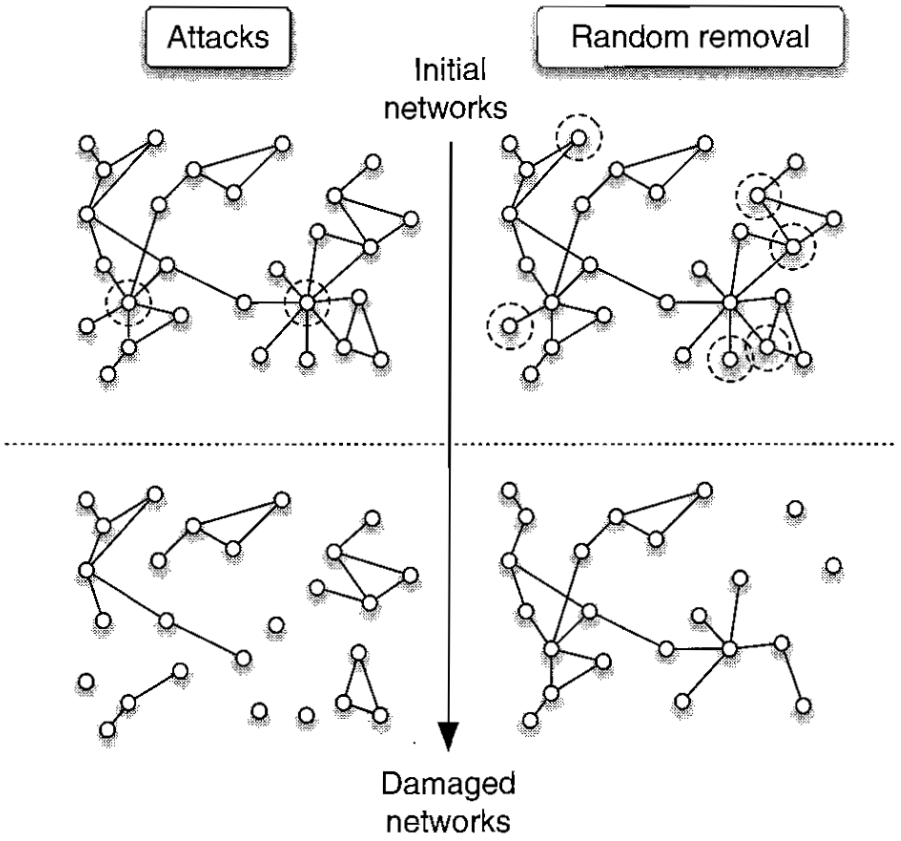
- the removal of a link
- the removal of a node, with all links incident to it

Are some topologies more resilient than others?

How to identify the most fragile nodes/links?

failures: nodes/links are removed at random

attacks: the most important nodes/links (i.e., the most central, or the most loaded) are purposely removed



How to measure the level of service after a fraction f of nodes (or links) has been removed?

A few purely topological proxies (i.e., no knowledge of the network function):

- relative size of the largest connected component

$$\frac{S}{N}$$

- average distance (undefined if the network splits in components)

$$d = \frac{1}{N(N-1)} \sum_{i,j(i \neq j)} d_{ij}$$

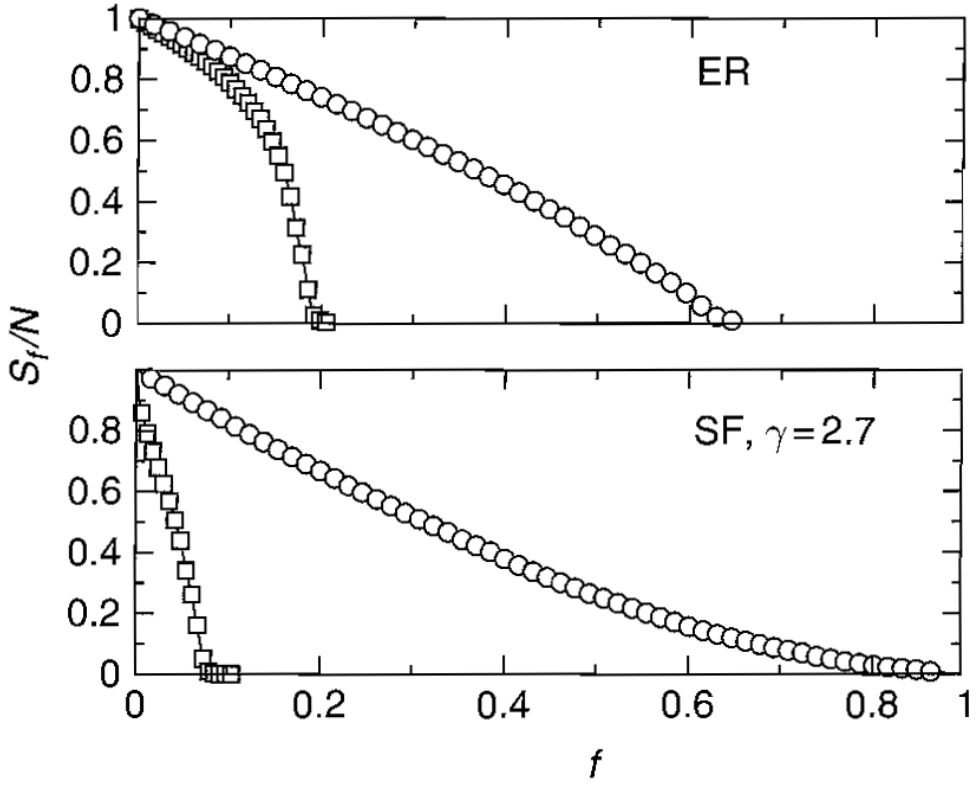
- efficiency

$$E = \frac{1}{N(N-1)} \sum_{i,j(i \neq j)} \frac{1}{d_{ij}}$$

Failures and attacks on Erdös-Rényi and Scale-Free networks

Failures: random removal hardly impacts on hubs (they are rare): SF nets are (slightly) more resilient (no threshold).

Attacks on higher degree nodes: in SF nets hubs are crucial for connectivity, which is therefore destroyed much faster than in ER nets.



Recap: A scale-free network is

- robust with respect to failures: if a node is removed at random (with all its links), the connected fraction of the network remains large, and the average distance remains small.
- fragile with respect to attacks: if nodes are removed starting from those with highest degree, the connectivity rapidly decays.

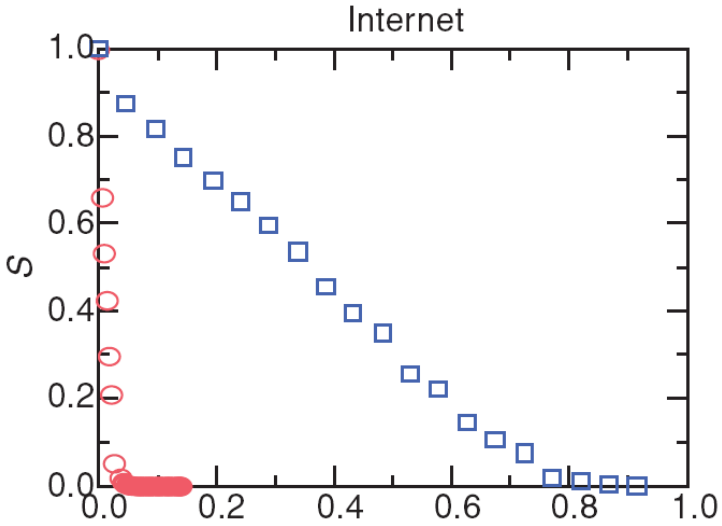
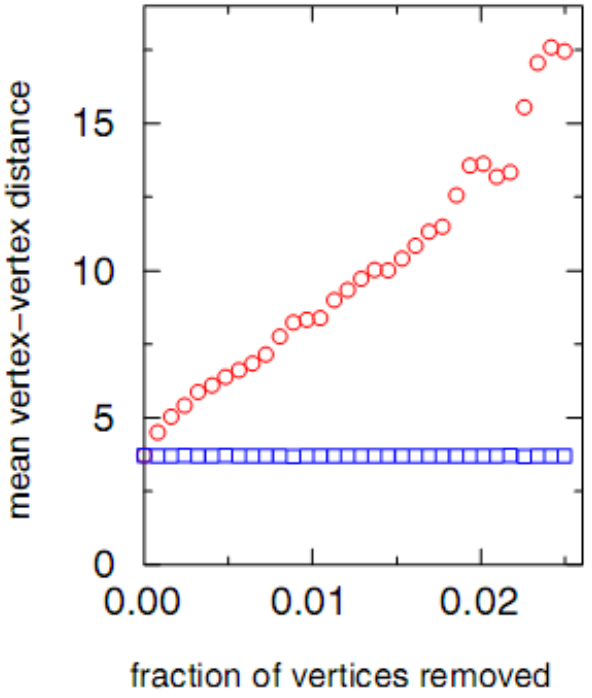


Figure 11. The relative size S of the largest cluster in the Internet, when a fraction f of the domains are removed [25]. □ , random node removal; ◯, preferential removal of the most connected nodes.

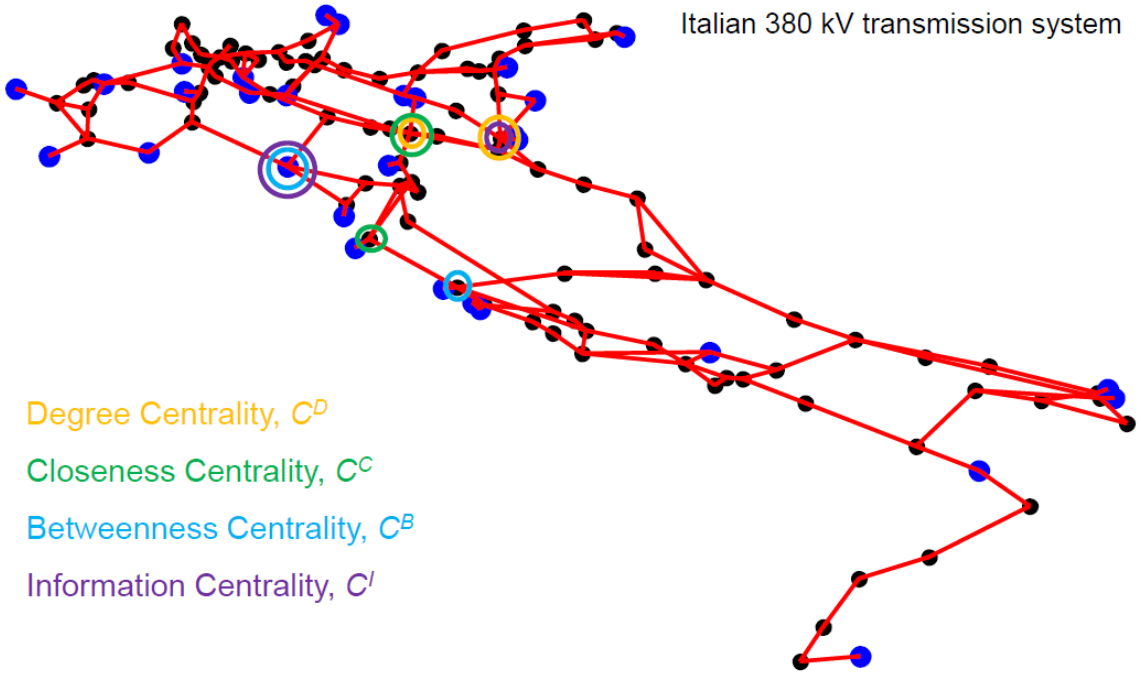


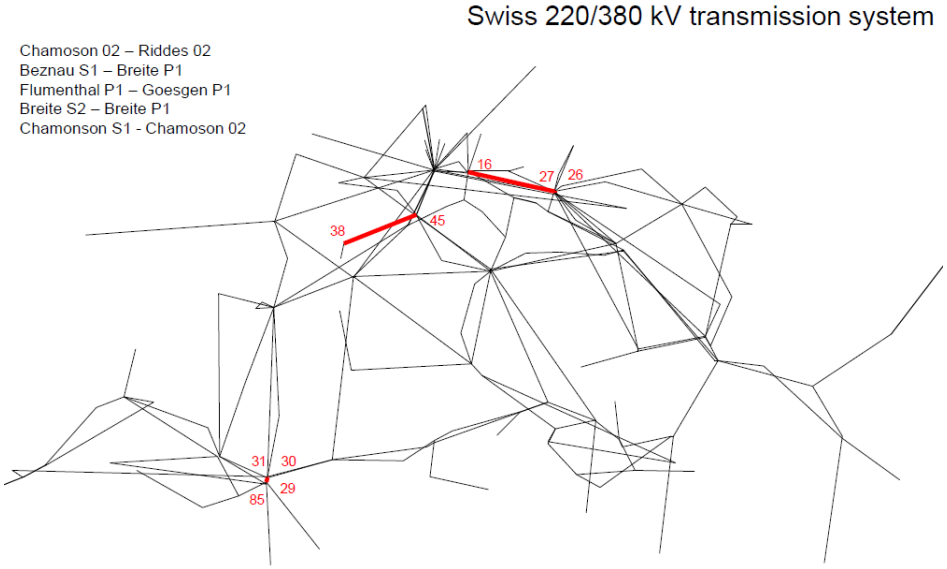
Identifying the critical elements in infrastructures

centralities: degree, closeness, betweenness

information centrality (node): loss of efficiency after removal of all links incident in node i

$$I_i = \frac{\Delta E_i}{E} > 0$$





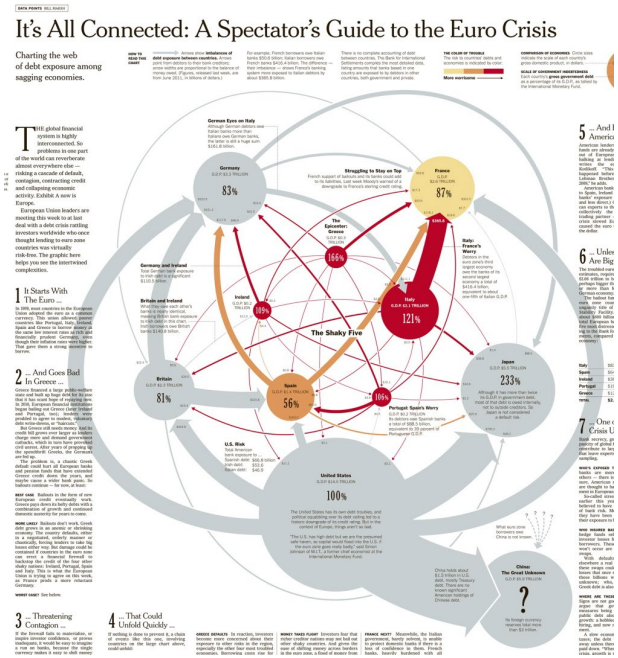
information centrality (link): loss of efficiency after removal of link $i \to j$

CASCADES OF FAILURES

How breakdown phenomena propagate over the network?

Applications: power distribution, financial systems, online social networks, ...

Figure 1. The 380 kV Italian power transmission network (TERNA 2002, Rosato, Bologna et al. 2007).



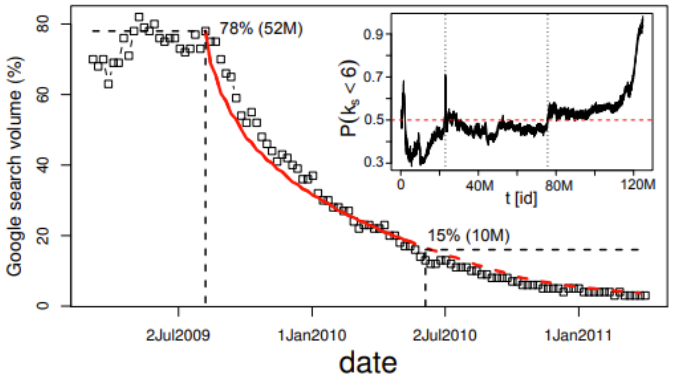
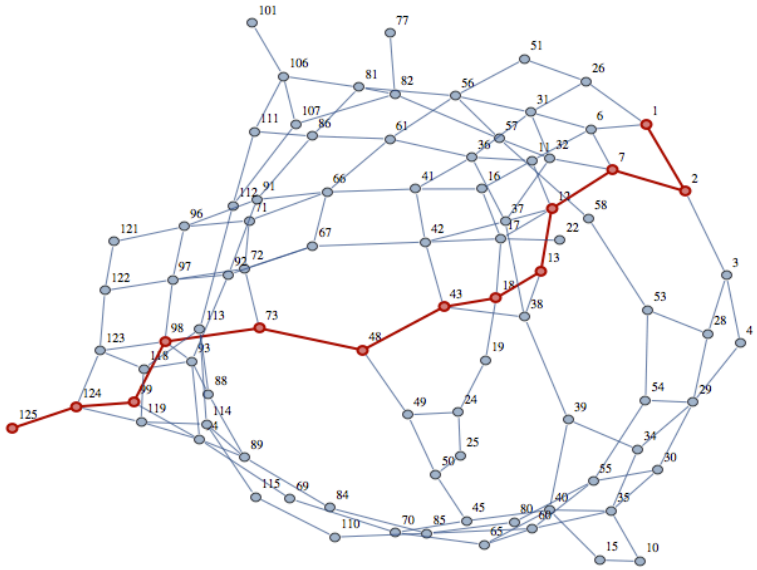


Figure 6: Weekly Google search trend volume for Friendster.

Maximum capacity model *(Motter and Lai, 2002)*



- every pair of nodes (i, j) exchanges one unit of material (energy, information,...) along the shortest path

  ⇒ at time $t = 0$ the load of each node i is proportional to its betweenness $b_i(0)$

- each node i has a maximum capacity $C_i = (1+\alpha)b_i(0)$ ($\alpha > 0$: tolerance parameter)

Failure or attack: one node is removed

⇒ the betweennesses b_i of all nodes change (and thus their load)

⇒ some more node fails if $b_i > C_i$

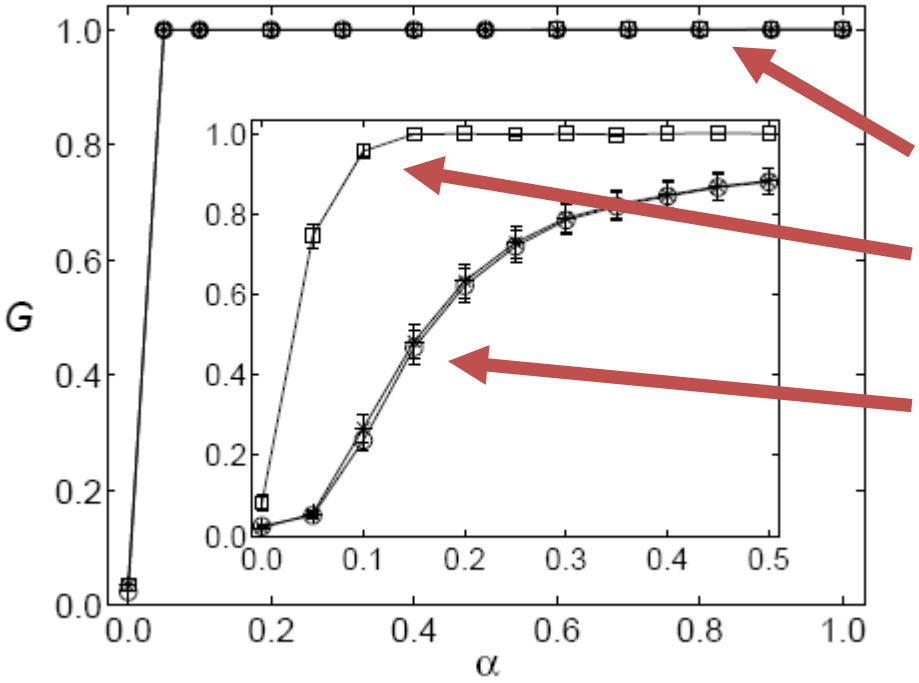
⇒ the betweennesses b_i of all nodes change

⇒ ...

At the end, $G = S/N$ is the largest fraction of nodes still connected.

Which topology is more robust?

Some tests on artificial networks...



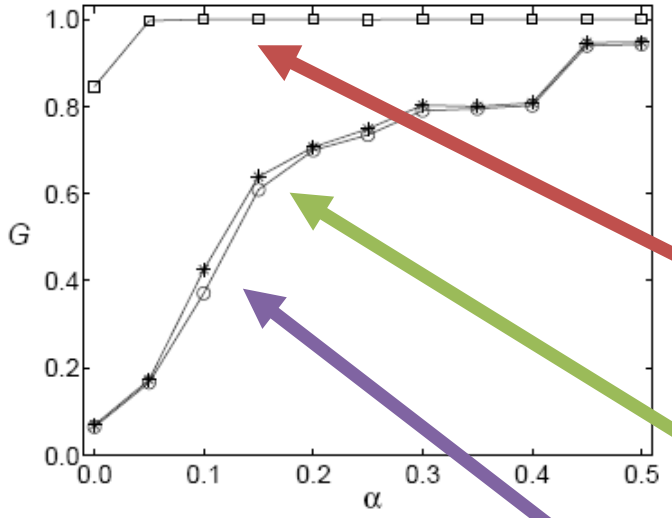
homogeneous networks (random failure or attack)

scale free network - random failure

scale free network - attack

Highly heterogeneous networks (e.g., scale-free) appear to be more fragile.

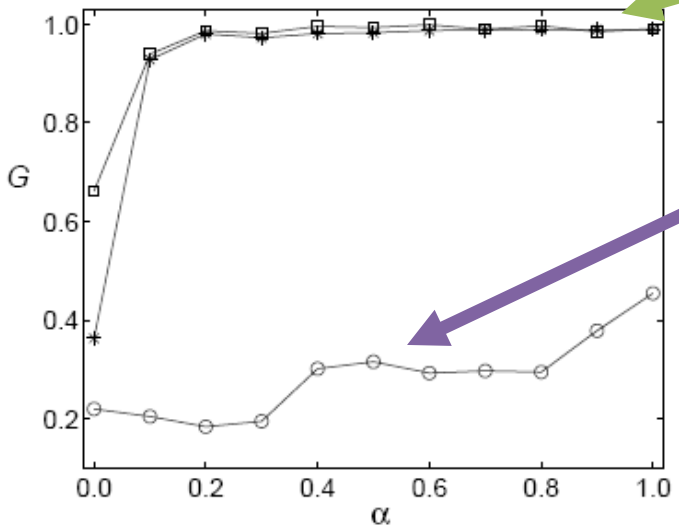
...and some simulations on (samples of) real-world networks:



Internet (autonomous systems, $N \cong 6500$)

random failure (□)

attack - node with largest degree (*)



attack - node with largest load (o)

US power grid ($N \cong 5000$)

KQ-cascade model *(Yu et al, PNAS, 2016)*

k-cascade model (value/risk of the current situation): a node leaves when its current degree is less than k

(outcome: reduction to the k-core)

q-cascade model (imitation effect): a node leaves when it has lost more than the fraction q of initial connections

(what is the critical q causing global crash?)

KQ-cascade model (integrating the two models above):

a node leaves at a certain probability f

(i) either when its current degree is less than k_s

(ii) or when it has lost more than the fraction q of initial connections

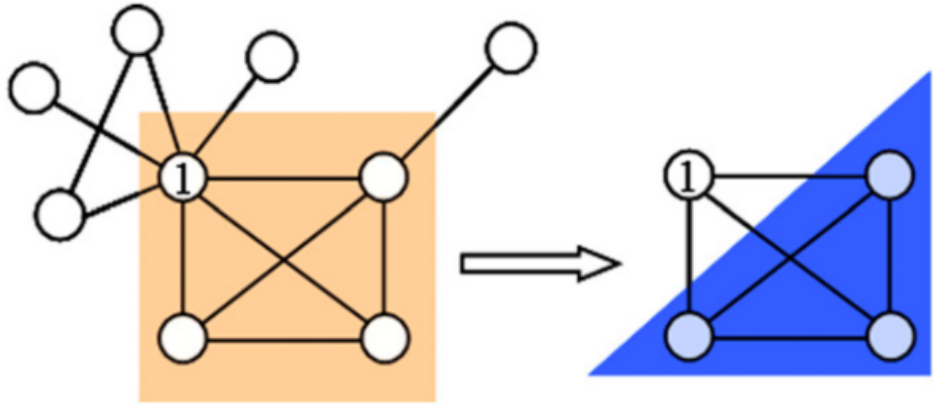
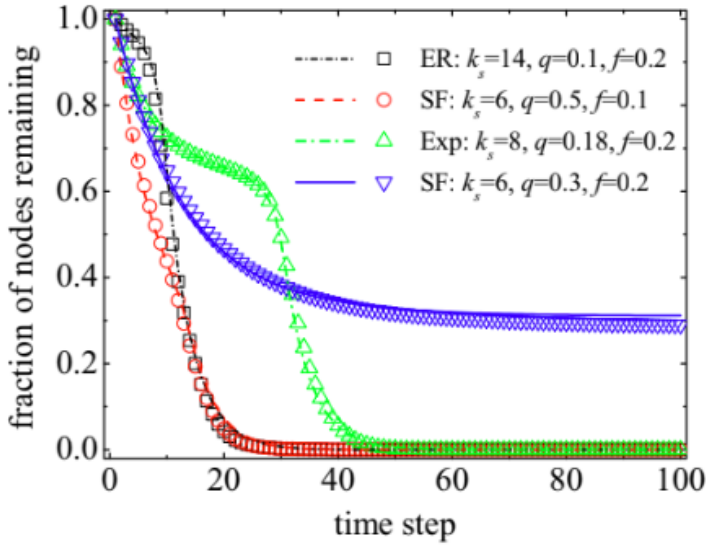
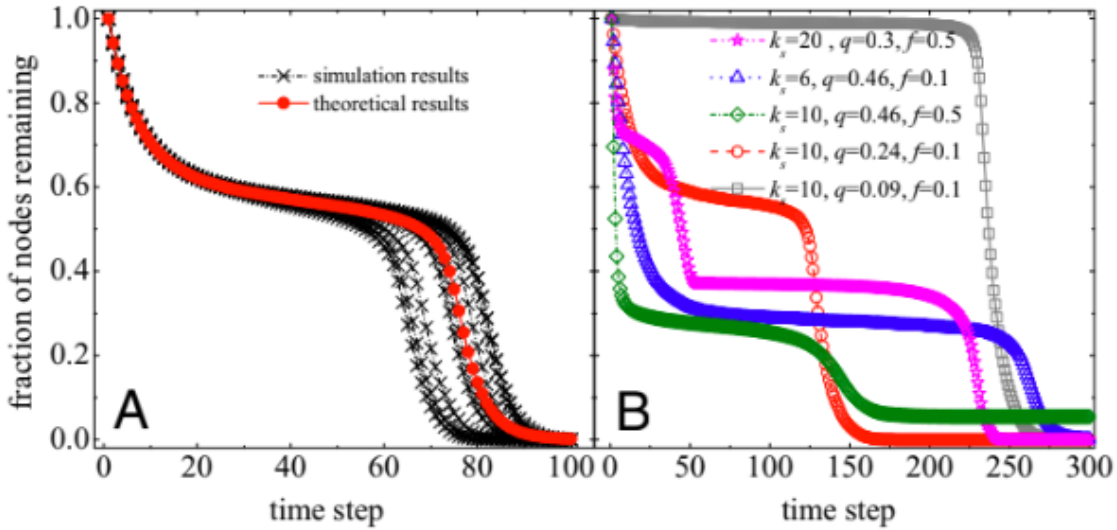


Fig. 1. Schematic illustration of KQ cascade with $k_s = 3$ and $q = 0.5$. In a classic k-core cascade, the four nodes within the yellow square forming up a three-core would stay on while other nodes would leave. In the KQ cascade, however, because node 1 has lost more than 50% of its original neighbors, it will leave in the next time step, which leaves each of the three nodes within the blue triangle with fewer than three connections, leading to the final crash of the network.

The outcome of the cascade depends on the network topology and on the cascade parameters.





A pseudo-steady state can be followed by a sudden crash.

The model fits very well the rapid decline of Friendster social network (from 68 million users in May 2009 to 10 million in August 2010, and then declining further).