Attacking and Defending Random Networks

Vilhelm Sjöberg

November 24, 2009

How hard is it to break up a network?

Motivating examples:

- Police targeting terrorist networks
- Music industry disrupting P2P networks
- Drugs attacking biological pathways in bacteria
- Health service containing an epidemic disease

Exponential vs Scale-free networks

Recall:

- The Erdős-Rényi model produces a Poisson degree distribution with a sharp peak and exponential fall-off.
- The preferential-attachement model produces a degree distribution $P(k) \sim k^{-3}$.

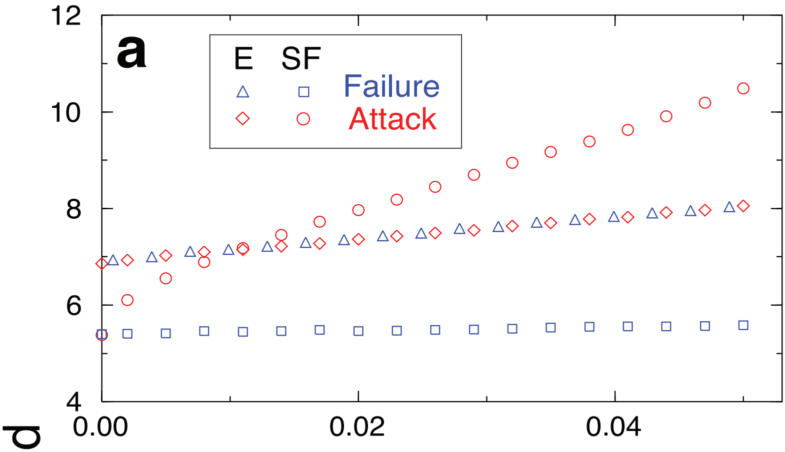
...what if we attack them?

Error and Attack Tolerance[1]

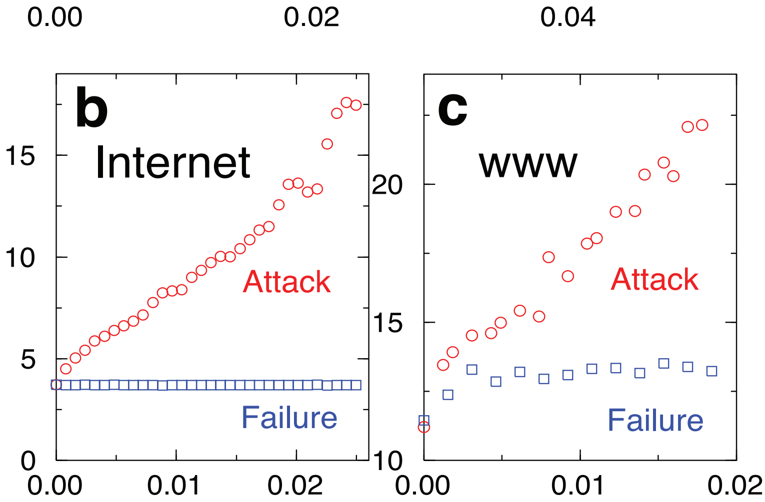
- Generate an Erdős-Rényi and a preferential-attachment network, with parameters so that both have $n = 10,000$ nodes and $20,000$ links.
- Either
  - Randomly delete r nodes.
  - Delete the r highest degree nodes.
- How does the diameter of the networks change?

[1] Reka Albert, Hawoong Jeong, and Albert-Laszlo Barabasi. Error and attack tolerance of complex networks. *Nature*, 406:378, 2000

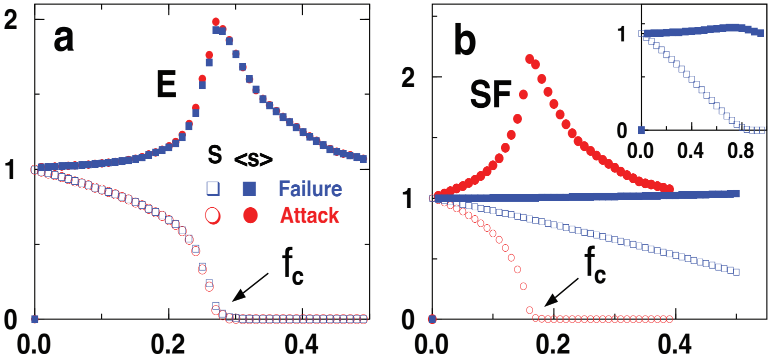
Results



“Two networks of increasing economic and strategic importance”



Thresholds for fragmentation



- The size of the largest cluster (as fraction of network size), S.
- Average size of all clusters except the largest one, $\langle s \rangle$.

Better Attack Strategies[2]

Define the *betweenness centrality* of a node v in graph G as

$$C(v) = \sum_{w \neq w' \in G} \frac{\sigma_{ww'}(v)}{\sigma_{ww'}}$$

where $\sigma_{ww'}$ is number of shortest paths between w and w', and $\sigma_{ww'}(v)$ is number of shortest paths passing through v.

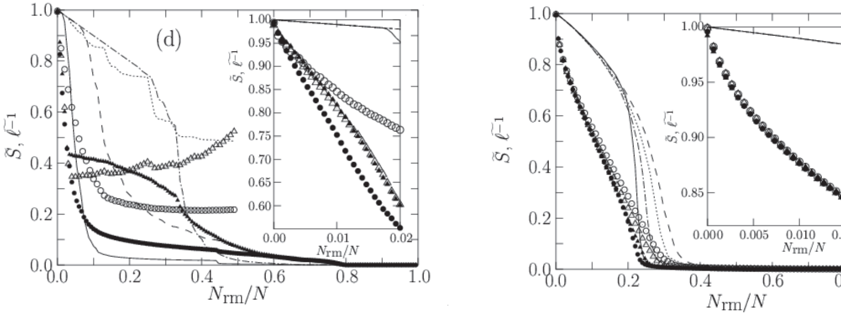
[2] Petter Holme, Beom Jun Kim, Chang No Yoon, and Seung Kee Han. Attack vulnerability of complex networks. *Physical Review E*, 65:056109, 2002

Better Attack Strategies

We can attack the nodes in order of

- Initial degree (ID)
- Recalculated degree (RD)
- Initial betweenness (IB)
- Recalculated betweenness (RB)

Results



Solid = RB, Dash-dotted = RD, Dotted=ID, Dashed = RB.
(d) is Watts-Strogatz, (e) is preferential attachment

Defending against network attacks[3]

Change to an iterative model.

- One-shot games vs Evolutionary game theory
- Desert Storm vs Counter-insurgency warfare

[3] Shishir Nagaraja and Ross Anderson. The topology of covert conflict. Technical Report UCAM-CL-TR-637, Cambridge University Computer Laboratory, July 2005

Defending against network attacks

The game proceeds in rounds. Each round consists of three phases

- *Attack* – attacker removes r vertices
- *Defend* – defender adds r vertices
- *Adapt* – defender rewires any number of existing edges

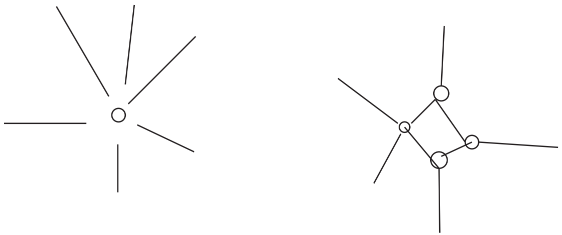
Defense strategy 1: Random Replenishment

The baseline for comparison.
The r new nodes connect randomly to the existing nodes with probability $p = k/(N - r)$.

Defense strategy 2: Rings

Inspiration: “dining steganographers”

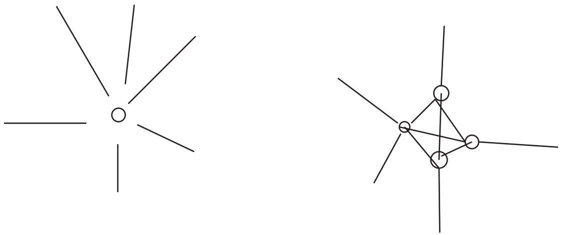
- A “vulnurable node” v recruits $n - 1$ other nodes from the newly added r nodes, or from its neighbours.
- All edges from the existing v nodes are dropped
- The n nodes form a ring.
- v’s links are uniformly distributed among the n nodes.



Defense strategy 3: Cliques

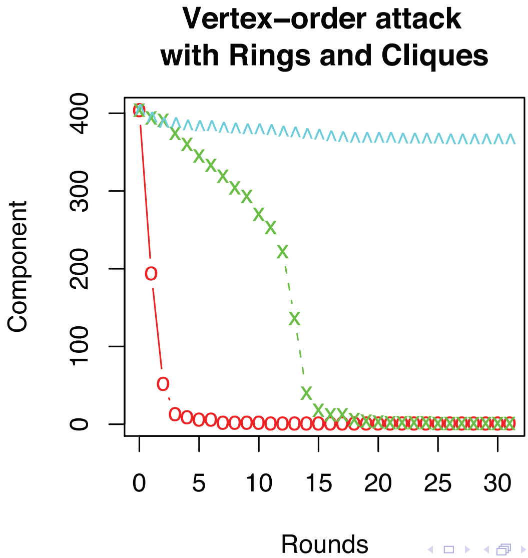
Inspiration: revolutionary cells

Same as before, except the n nodes form a clique.

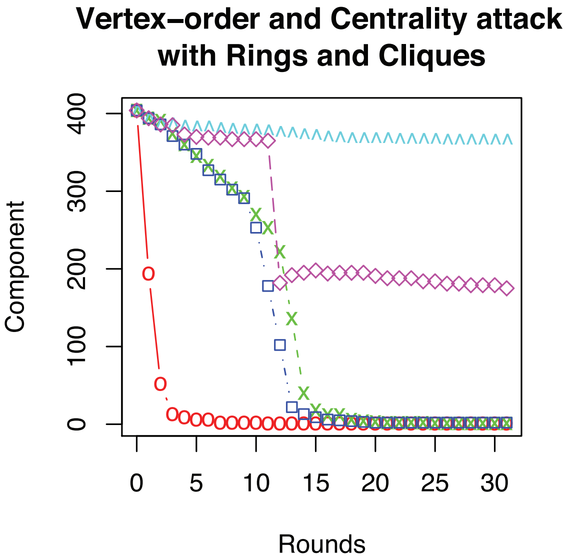


Results

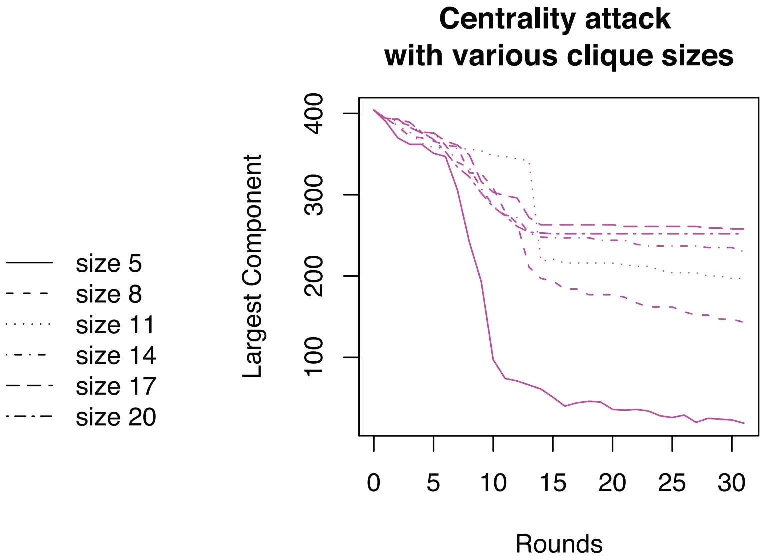
Red=baseline, green=rings, cyan=cliques



Better attack: Centrality order



Better defense: Varying clique size

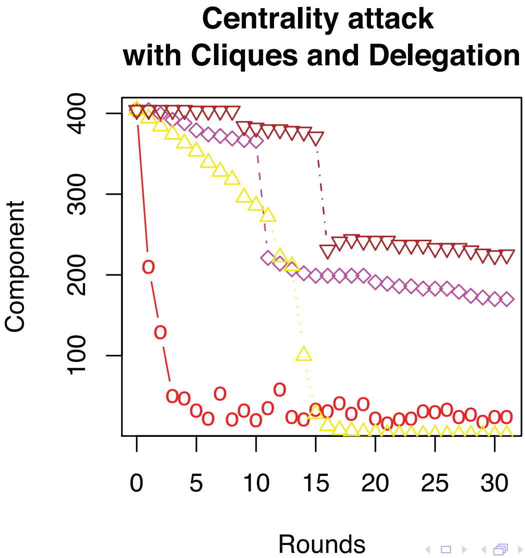


Better defense: Delegation

A vulnerable node selects two neighbours, connects them, and then disconnects from one of them.

Better defense: Delegation

Yellow=delegation only, dark red=cliques and delegation



Conclusions

- Scale-free networks are efficient but vulnerable.
- The way you attack them makes a difference.
- Defending networks is hard.