

Proactive Vulnerability Assessment of P2P Network

Scott Dejmal, Alan Fern, Thinh Nguyen
School of EECS, Oregon State University

MAX-DAMAGE Problem:

What is the worst case DoS attack for this network w/ given security mechanism and attack budget?

Attacker

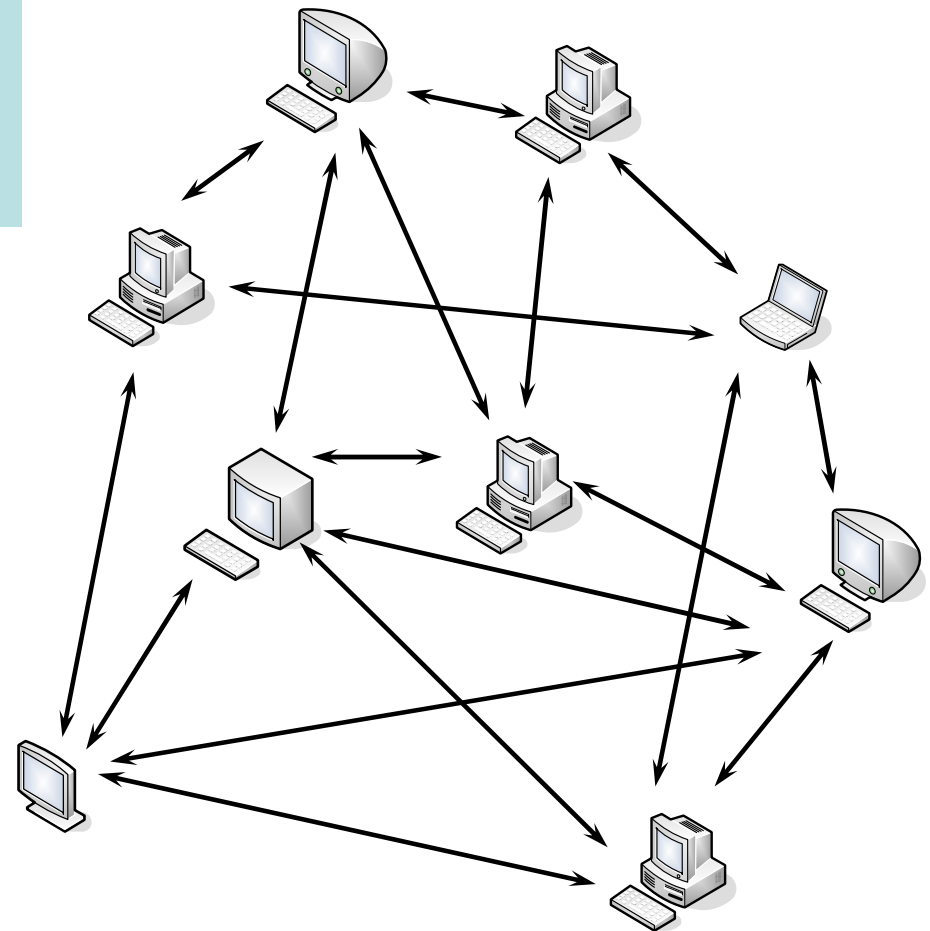


Bad Queries



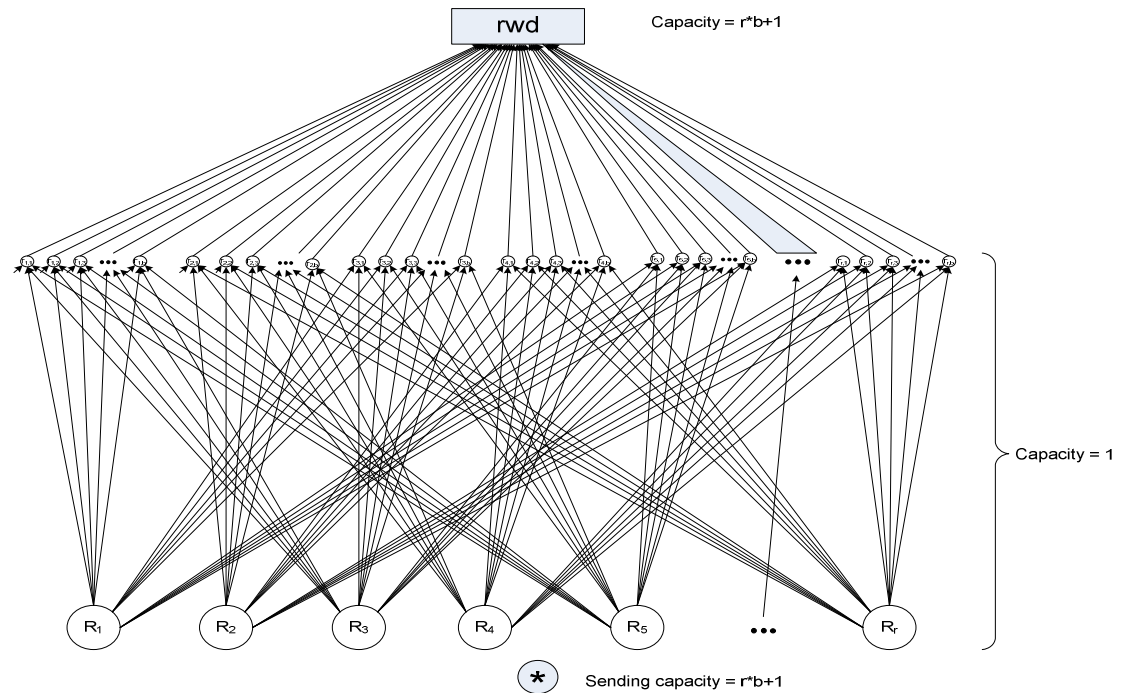
MAX-DAMAGE is APX-complete

Fair use DoS defense mechanism



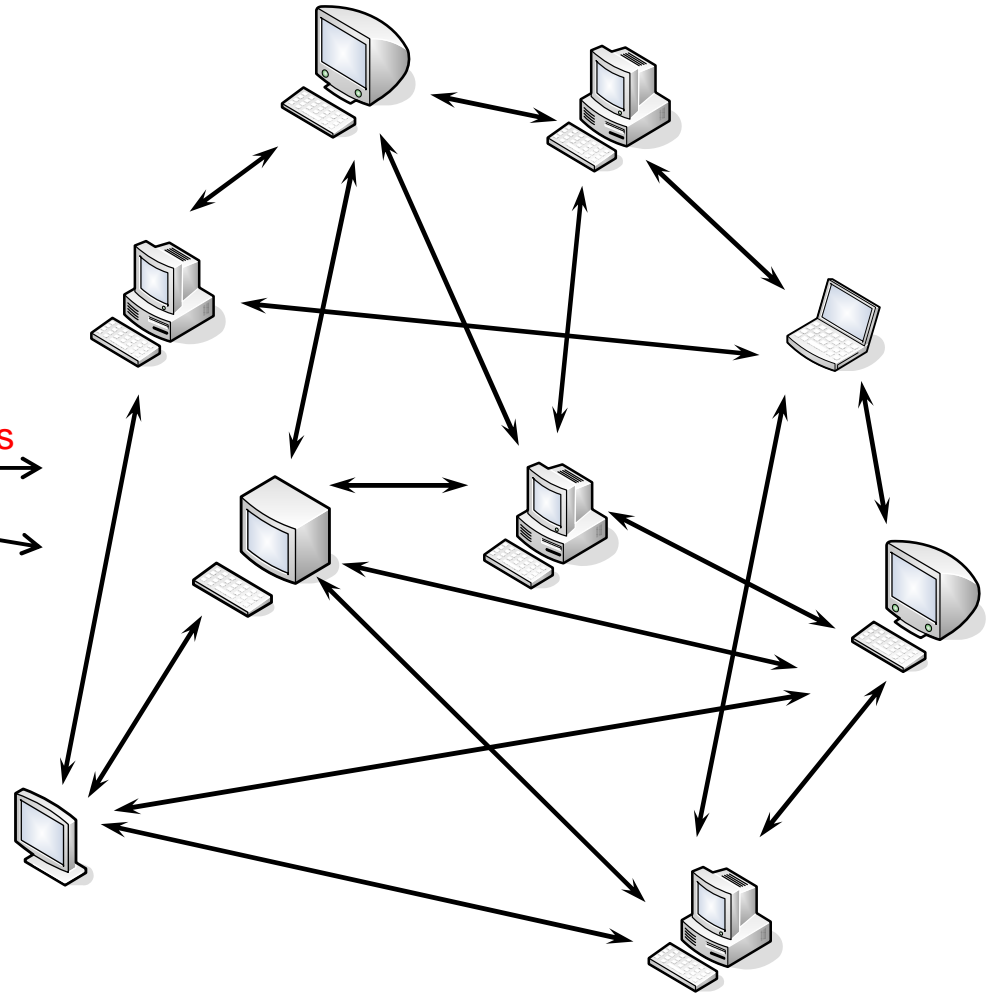
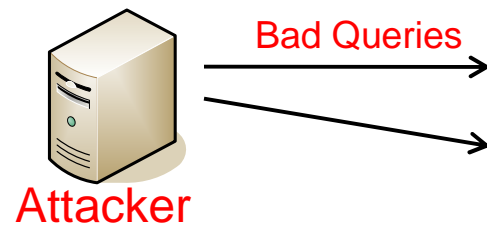
Greedy Algorithms

- **Memoryless Fair Use Mechanisms:** treat all queries identically
 - Cumulative damage function is monotonic and submodular
 - Greedy algorithm gives $1 - 1/e$ approximation
- **Caching Fair Use Mechanism:** recognize & discard duplicate queries
 - Cumulative damage is *not* monotonic
 - Greedy algorithm can be arbitrarily bad



Heuristic Algorithm: Policy Gradient RL

Learn stochastic attack policy
(multinomial over network nodes)



- We use the OLPOMDP policy gradient algorithm
- Compared to greedy, OLPOMDP can incorporate state features, and does not require a model of the network