Proactive Vulnerability Assessment

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

Scope: Utilize artificial intelligence (AI) techniques to evaluate both worst-case and realistic scenarios before attackers do. Current focus is on DoS attacks of P2P networks.

Problem Formulation:

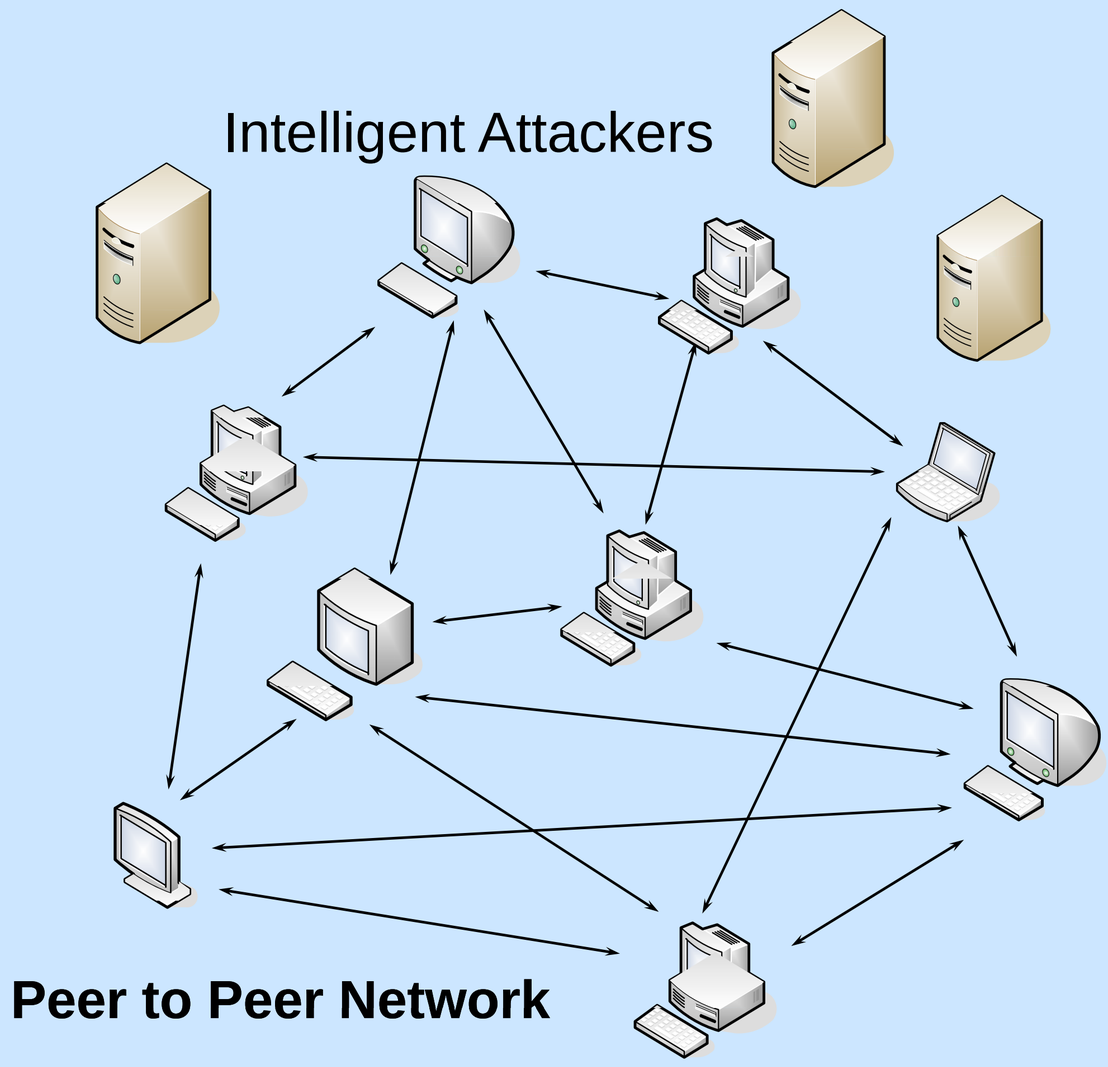
- P2P network with processing constraints at the nodes
- We consider both single malicious attacker and small botnet situations
- Fair use passive DoS defense mechanism

DoS Defense Mechanism

Constrained resource is at the application layer; this provides the opportunity for some DoS defense. Differentiating malicious queries may not be possible, so consider passive fair use policies.

Complexity

Vertex cover reduces to special case of damage maximization problem. NP-Complete, APX-Complete.



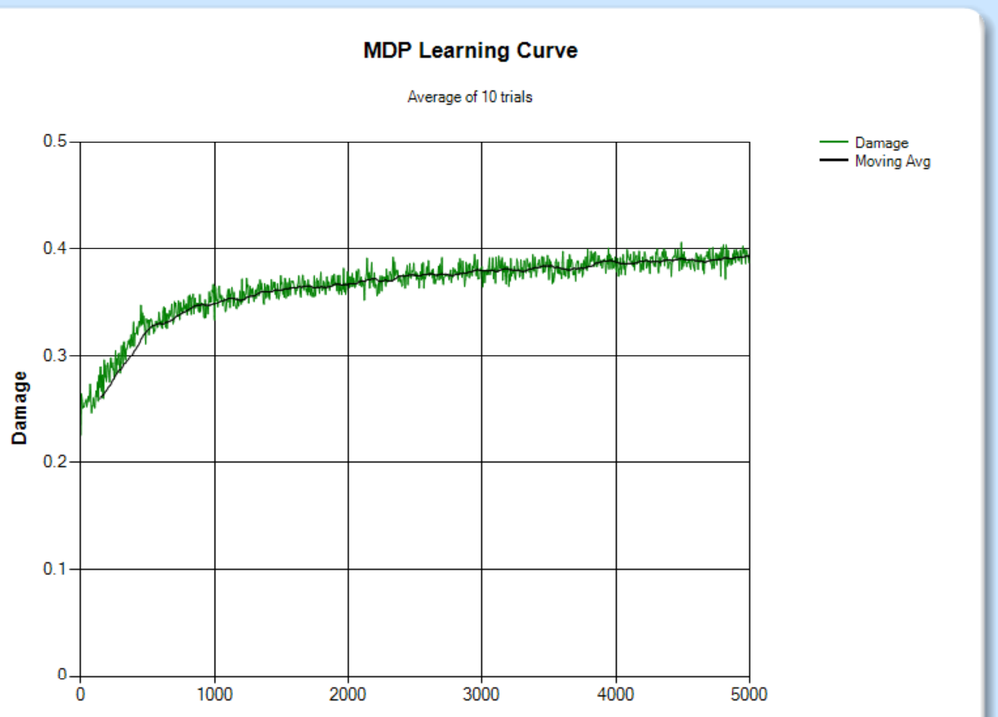
Approach and Impact

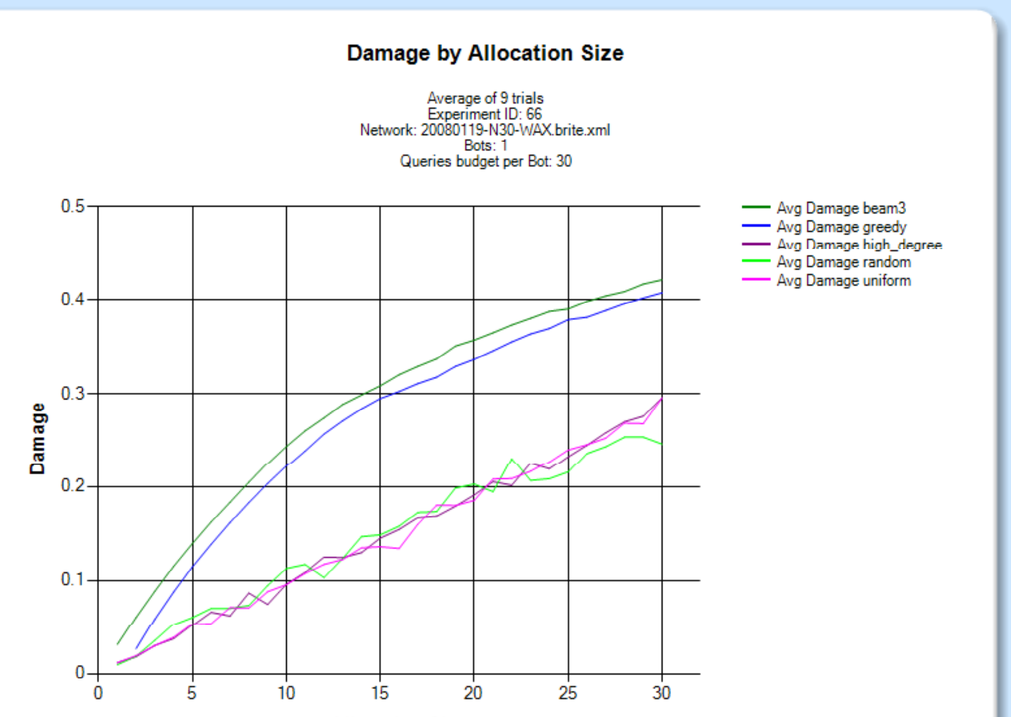
New approach

- Consider worst-case scenario where attacker has complete knowledge of the network topology and dynamics
- Compare realistic scenario where attacker has a noisy reward signal and directly optimizes using policy gradient

Research Impact

- Early results have shown success on small networks
- We can compute the stochastic policy gradient and use a POMDP for direct optimization
- Work in progress includes variations on the RL formulation and larger botnet simulations





Approximation Algorithms

Memoryless model

- Damage function is monotonic and submodular; greedy algorithm achieves a $1 - 1/e$ approximation.

Caching model

- Damage function is neither monotonic nor submodular. Networks exist for which the greedy algorithm performs arbitrarily poorly. This is achieved by reducing available entropy at certain nodes. Nodes with high fan-out are attractive when few queries are allocated, but effectively decrease total entropy when more queries are added.
- Within the caching model, we compare naïve strategies with very limited knowledge, strategies with full knowledge, and policy gradient with “reasonable” knowledge.

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT

Oregon State University OSU