Protecting Resources Against Volumetric and Non-volumetric Network Attacks

Rajorshi Biswas
Information Sciences and Technology,
Penn State Berks, Reading, PA, USA

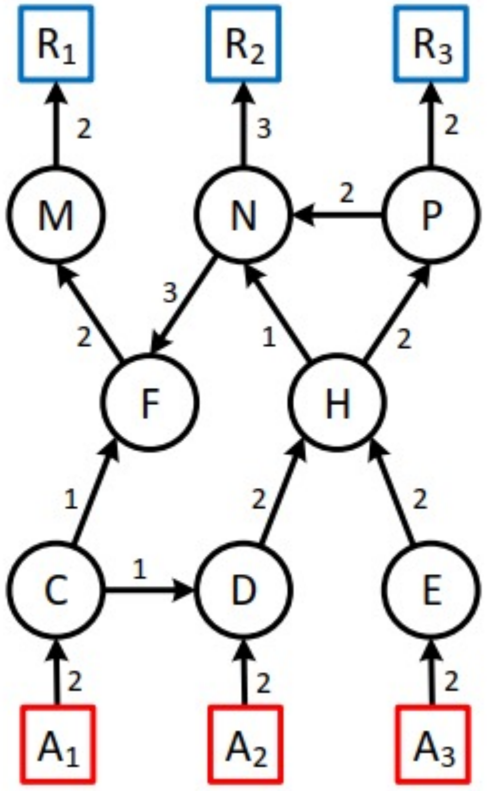
Jie Wu
Department of Computer and Information Sciences,
Temple University, Philadelphia, PA, USA

Outline

- Volumetric and Non-volumetric Attacks
- Filter Router and Moving Target Defense
- Problem Definitions
- Greedy and Dynamic Programming Solutions
- Simulation Results
- Q&A

Volumetric and Non-volumetric Attacks

- Volumetric
  - The damage of victim depends on the amount of attack traffic.
  - Example: DDoS, LFA
  - Does not require to block all traffic
  - Defense: Filter router and filter
- Non-volumetric
  - The damage of victim does not depend on the amount of traffic.
  - Example: password stealing
  - Requires to block all paths to the resources
  - Defense: Moving target defense



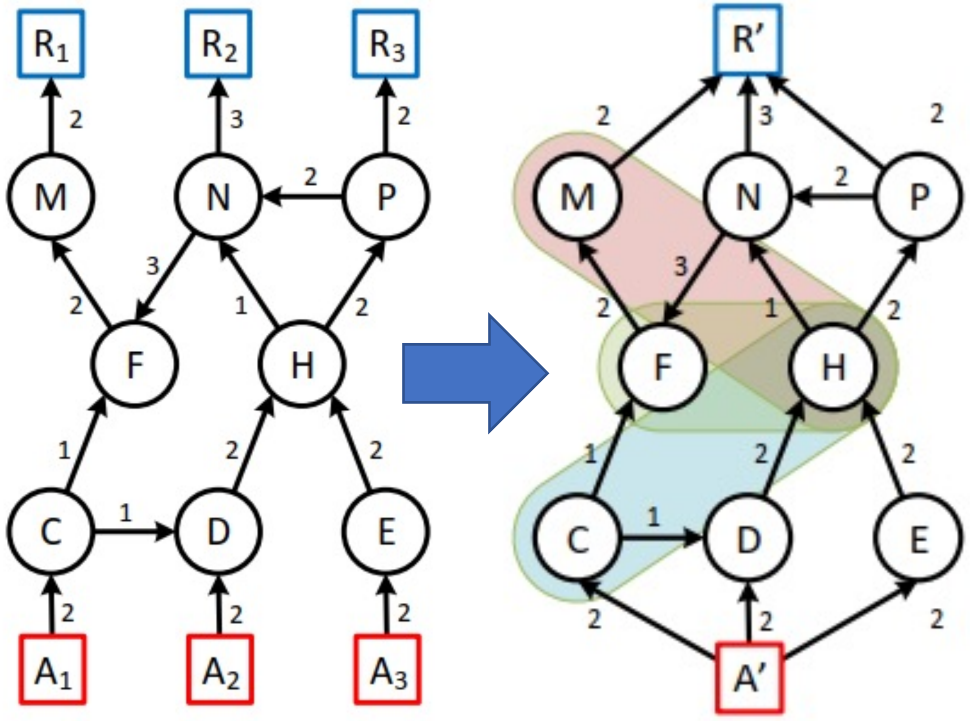
Filter Router and Moving Target Defense

- Filter
  - Simple blocking rules
  - Source-based, dest-based
  - “if source=X, drop the packet”
  - “if dest=Y, drop the packet”
- Filter Router
  - Accepts filters
  - Drop packets according to filters
- Each filter costs a certain amount to the victim.

- Moving Target Defense
  - Change the system parameters dynamically so that the attacker needs to start over on each change.
  - IP, port, password, system settings, etc.

Problem: Find K number of nodes to apply Filters

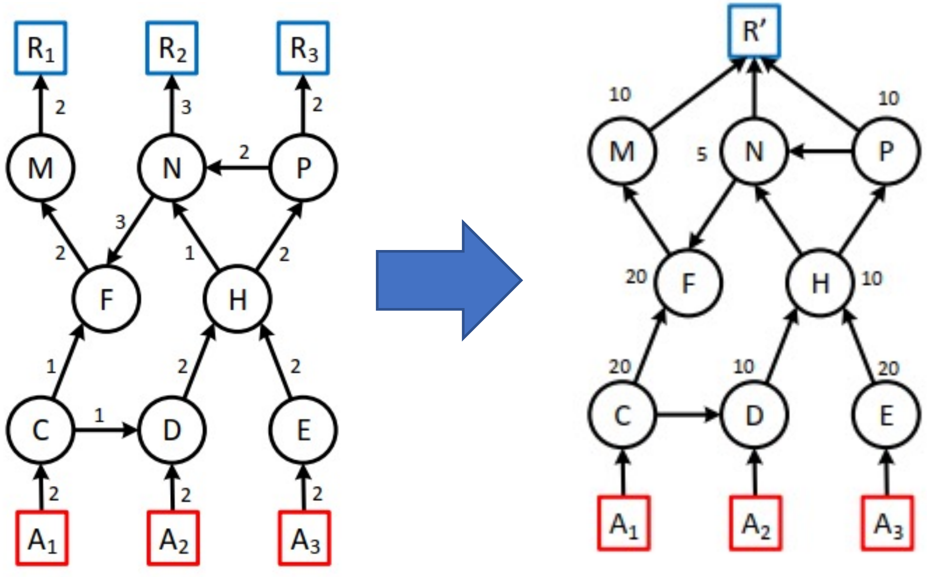
- Minimize:
  - Traffic reaching the resources.
- Constraints:
  - The number of filters cannot be more than K.
- Greedy Solution:
  - Combine recourses and attackers.
  - Find all min-cuts using Kanevsky methods.
  - Calculate contribution of each node in max flow.
  - Pick the most contributed node.
- Complexity: $O(|S_c||V|\,(|V|+|E|f))$
- Approximation Ratio: $1-\frac{1}{e}$



Volumetric attack

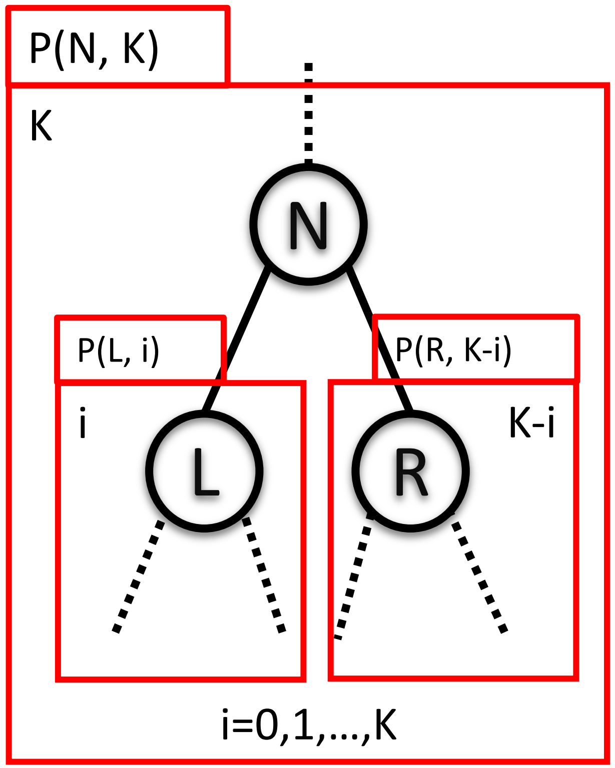
Problem: Find K number of MTD deployments

- Minimize:
  - Damage: the amount of steps passed by the attackers.
- Constraints:
  - The attacker must be blocked before reaching resources.
  - The number of deployed MTD must be less than budget K.
- Solution: Dynamic Programming

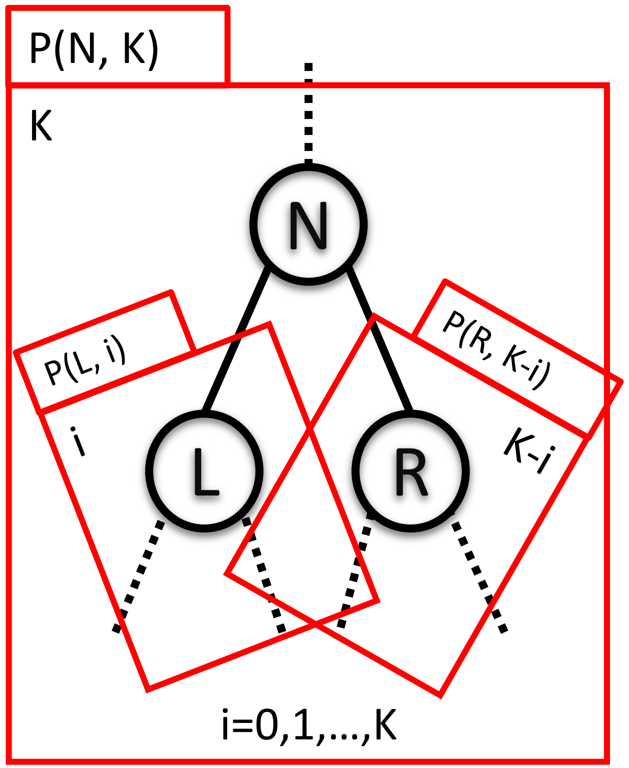


Non-volumetric attack

A Dynamic Programming Solution



Tree topology: No overlap



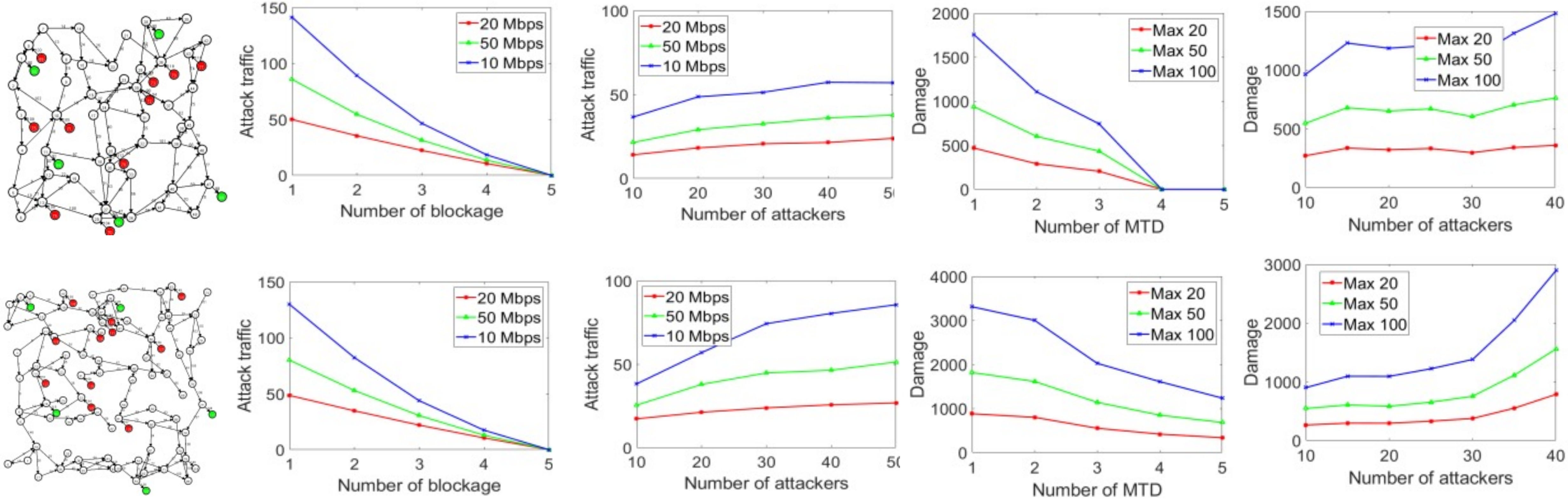
Tree topology: overlap

Solution: Keep tracking of, protected and damaged nodes

Protected
+
Unprotected
=
Protected

Complexity: $O(|V|^2K^2\Delta)$

Simulation Results



Volumetric

Non-volumetric

Thank You !!

Please send your questions to

rajorshi@temple.edu