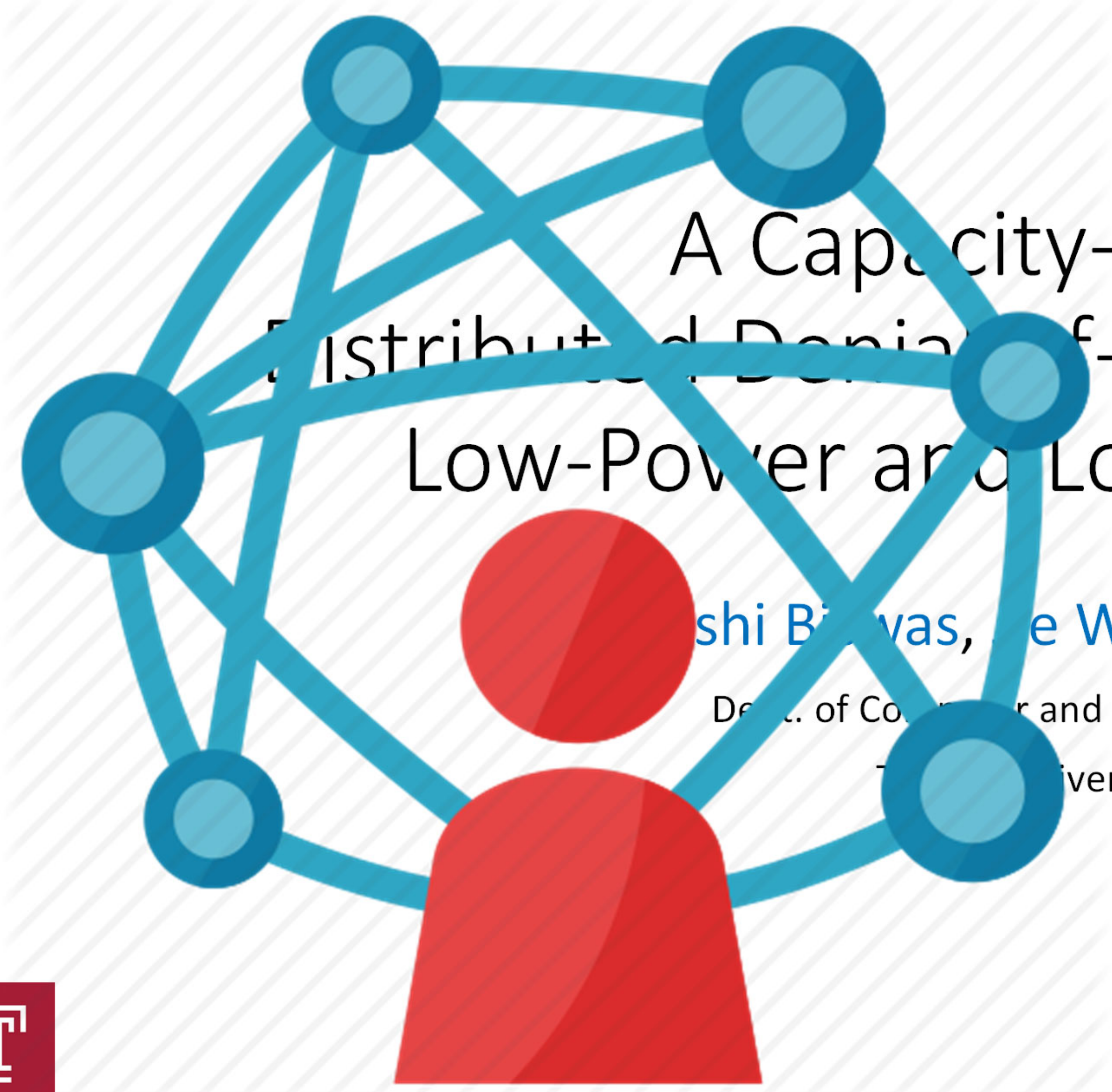


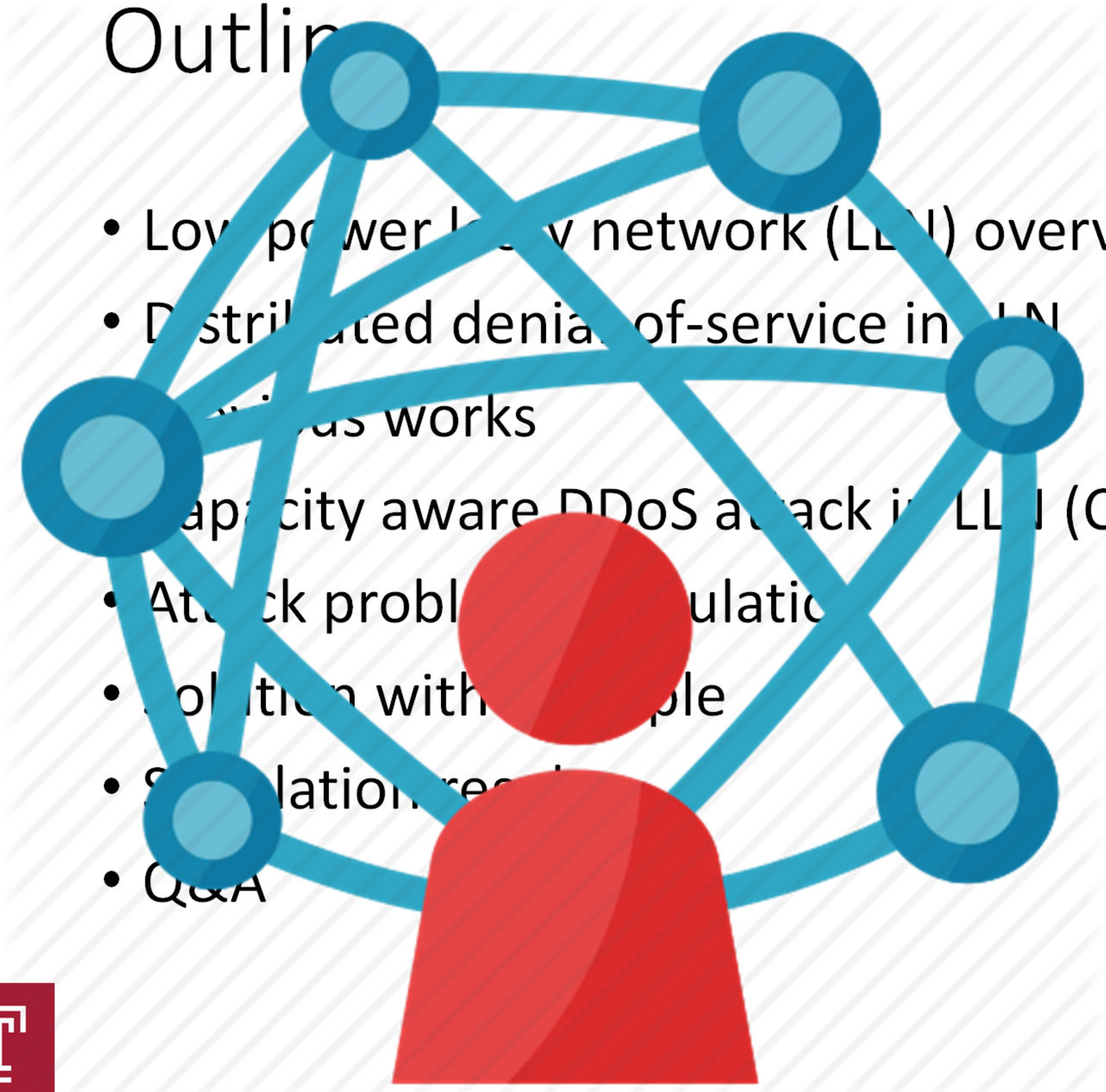
A Capacity-Aware Distributed Denial-of-Service Attack in Low-Power and Lossy Networks

…shi Bi…was, …e Wu, and Xiuqi Li

De…. of Co… …r and Info. Sciences

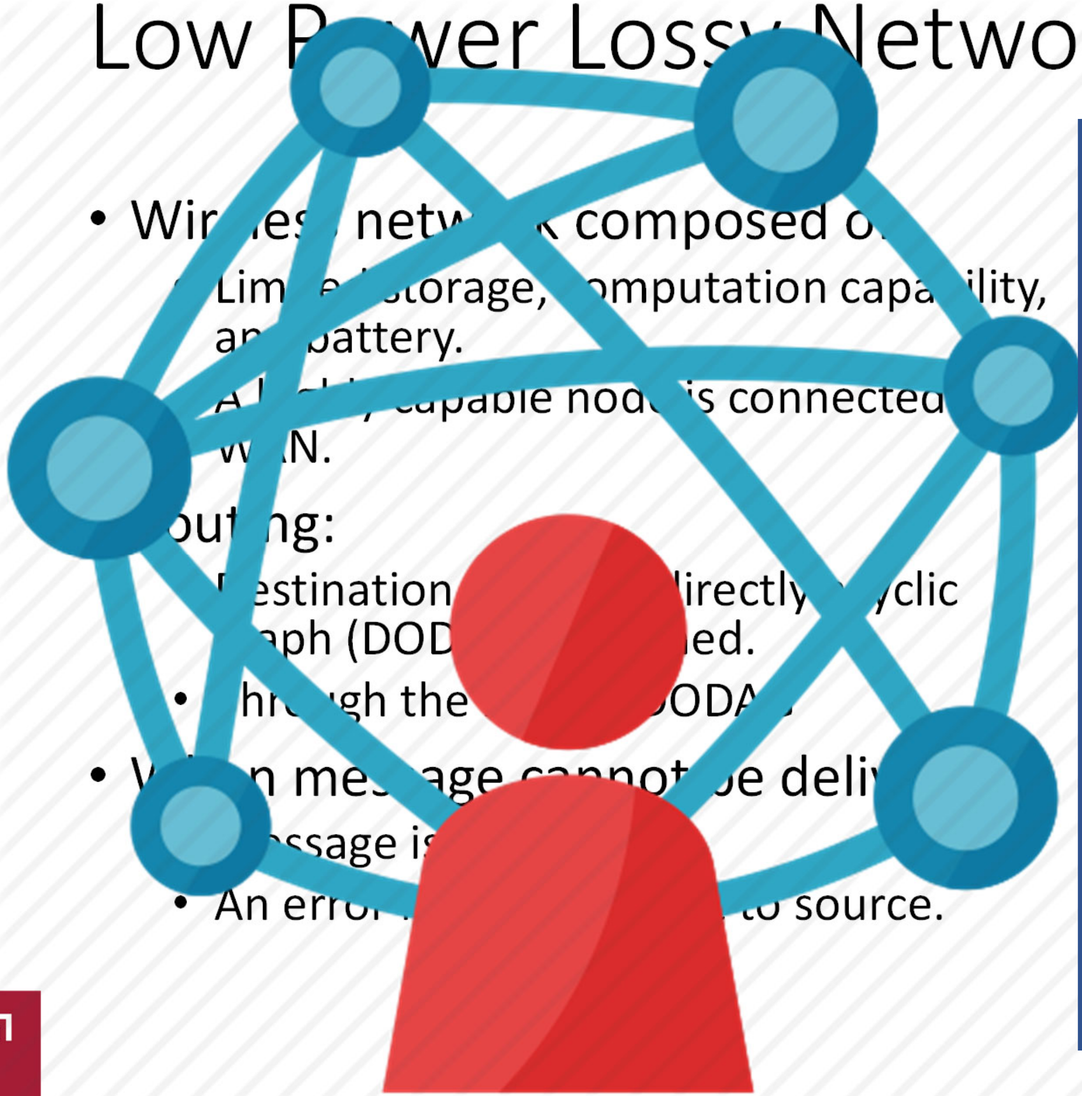
T… …iversity

Outline

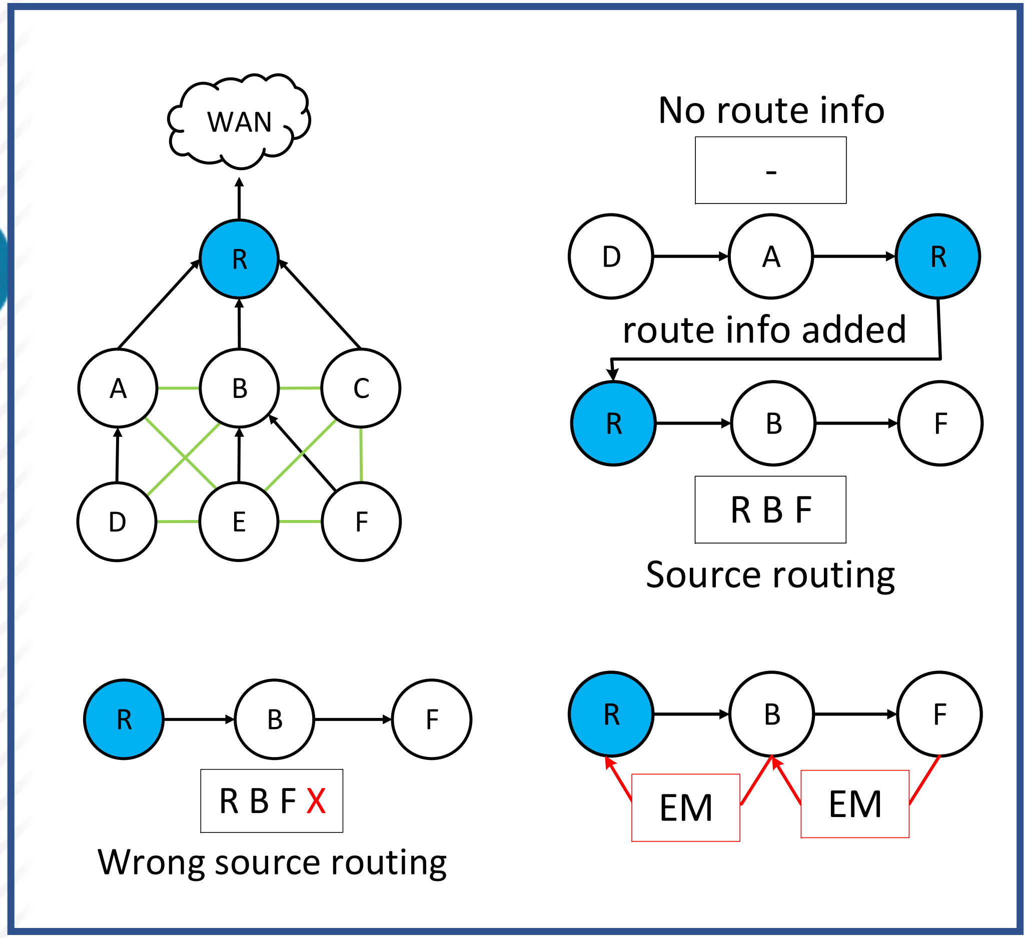


- Low power lossy network (LLN) overview
- Distributed denial-of-service in LLN
- Previous works
- Capacity aware DDoS attack in LLN (CADAL)
- Attack problem formulation
- Solution with example
- Simulation results
- Q&A

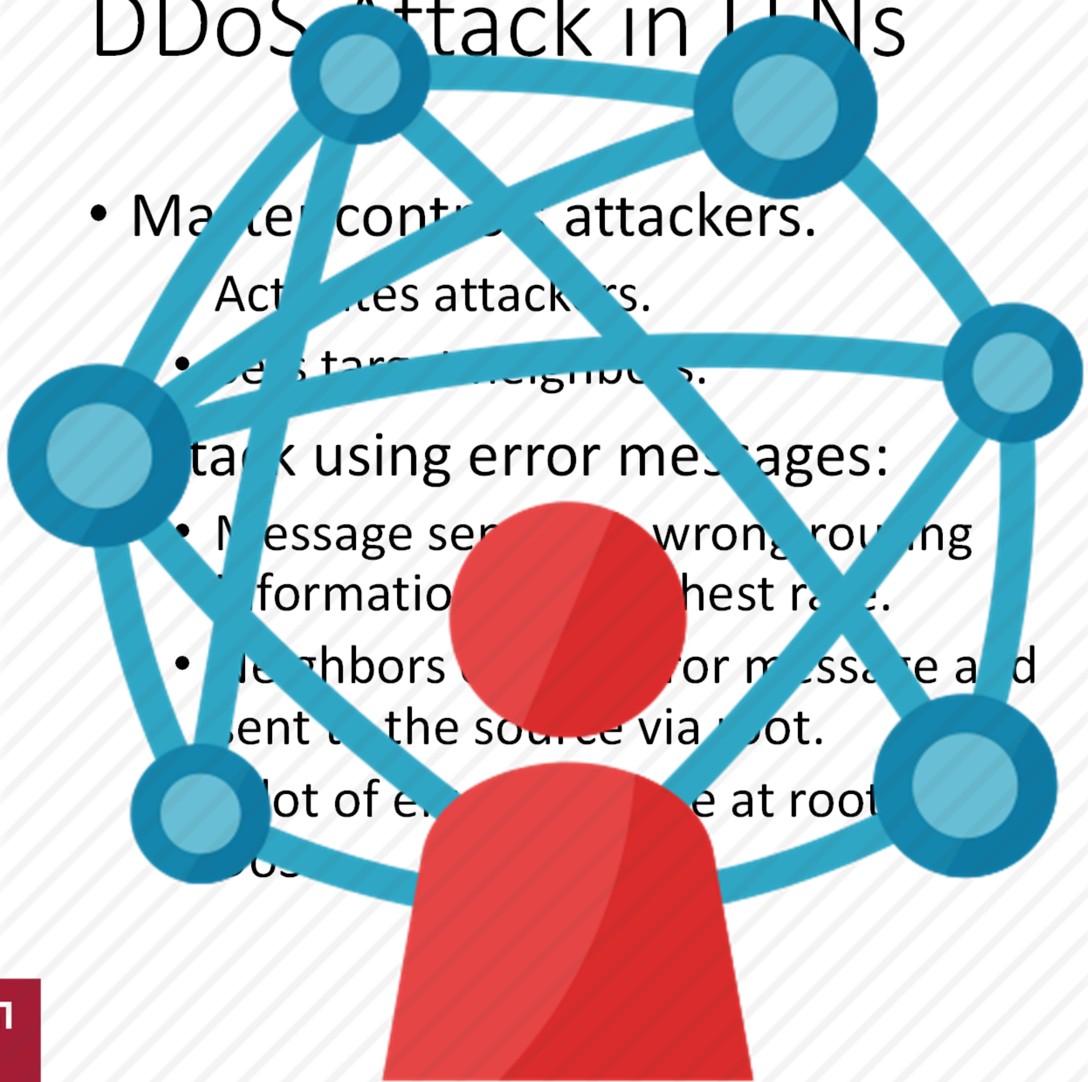
Low P wer Loss Network (LLN) Overview



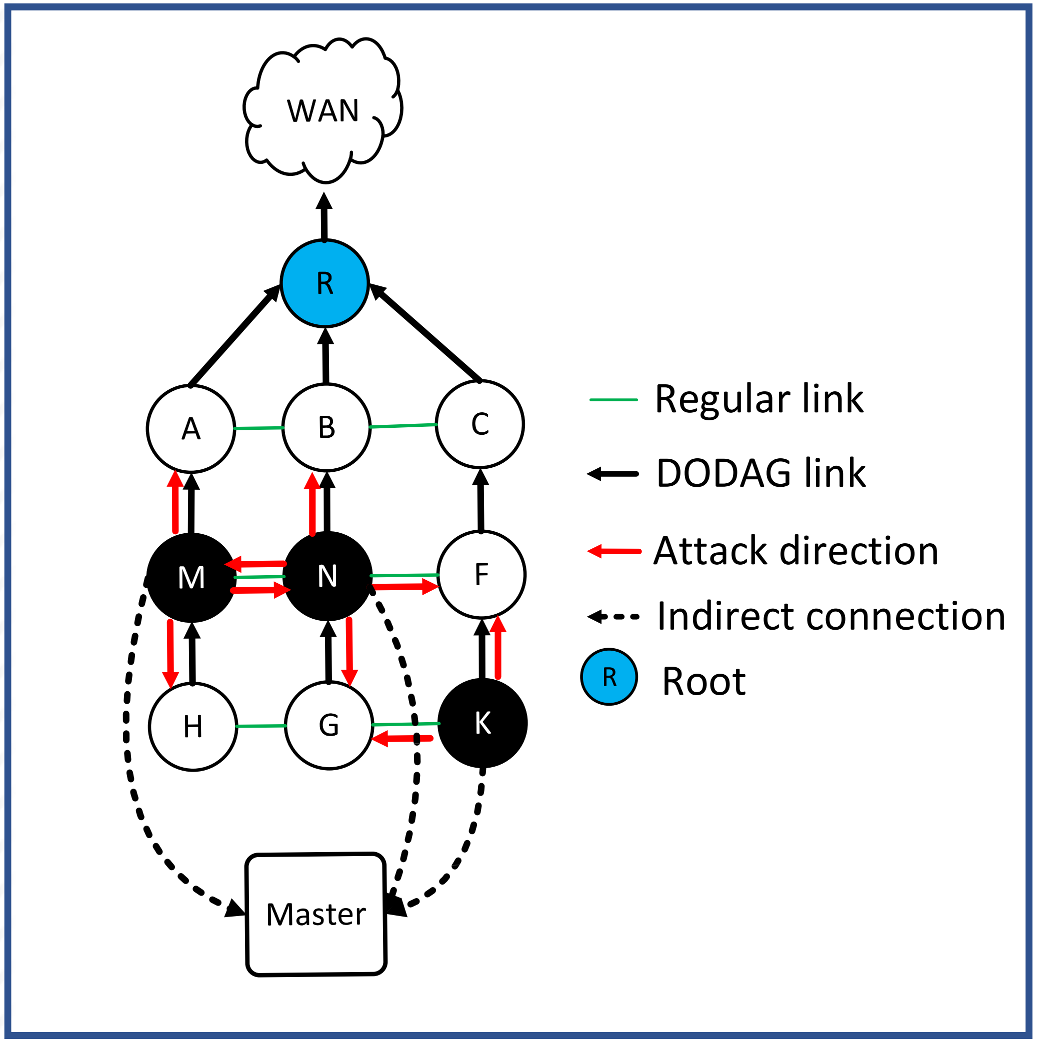
- Wir les netw k composed o
  - Lim e storage, omputation capa ility, an battery.
  - A capable nod is connected W N.
- out ng:
  - estination irectly yclic aph (DOD ed.
    - hr gh the ODA
- n me age cannot e deliv
  - ssage is
  - An erro o source.



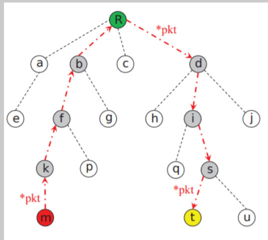
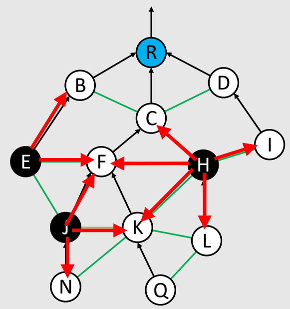
DDoS ttack in L Ns



- Ma te cont attackers.
  - Act tes attack rs.
  - e s tar eighb s.
- ta k using error me ages:
  - essage se wron rou ing formatio hest ra .
  - e ghbors or messa e a d ent the source via oot.
  - lot of e e at root

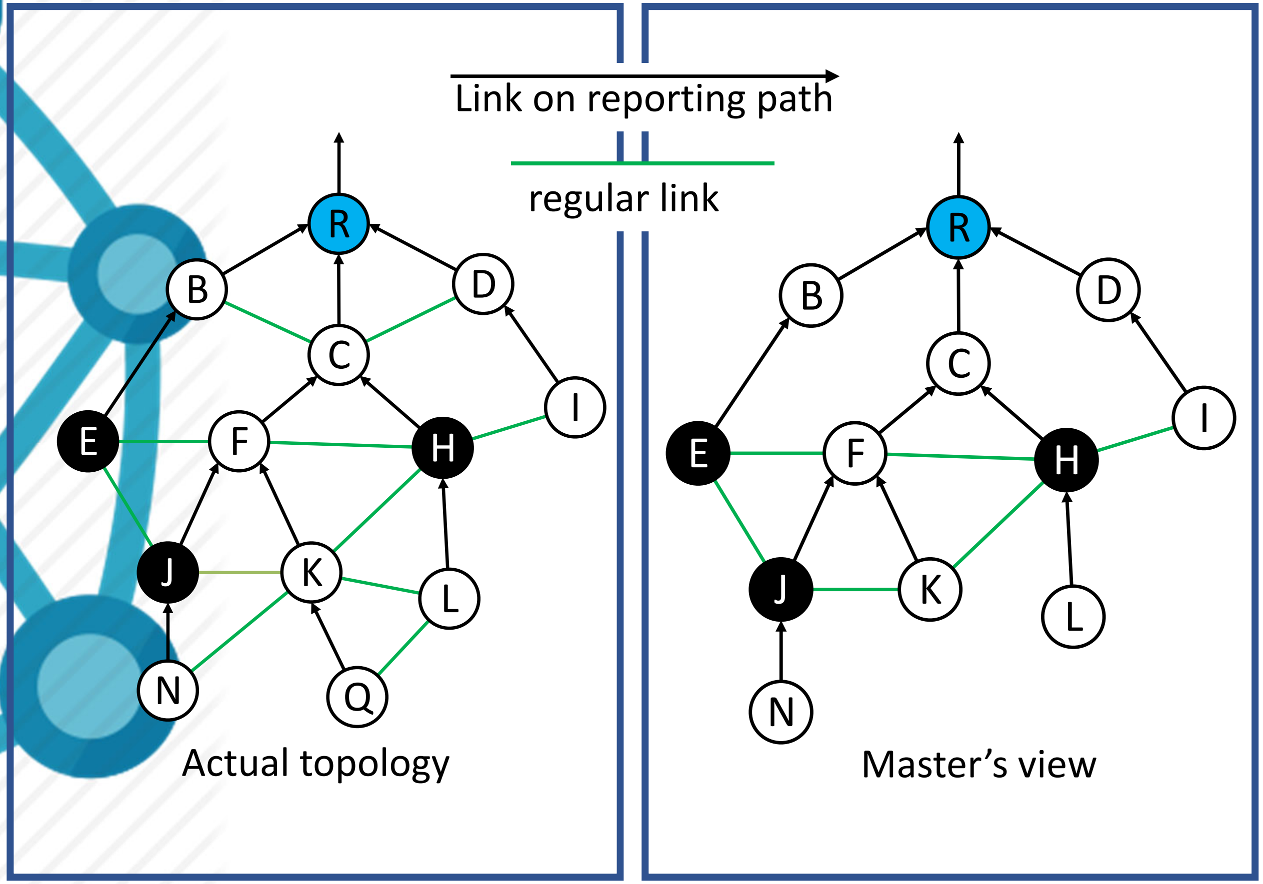


Previous Work

Systems	Limitations
Energy depletion attack Attackers send a lot of packets to a target node to exhaust its battery.  C. Pu, "Energy Depletion Attack Against Routing Protocol in the Internet of Things," in 2019 16th IEEE Annual Consumer Communications & Networking Conference, Jan 2019.	• The whole network does not suffer.
Hatchetman attack All attackers send packets with wrong routing information to their neighbors.  C. Pu and T. Song, "Hatchetman attack: A denial of service attack against routing in low power and lossy networks," in 5th IEEE International Conference on Cyber Security and Cloud Computing, Jun 2018.	• No coordination among attackers. • Does not select the target neighbors optimally.

Capacity-Aware DDoS Attack in LLN (CADAL)

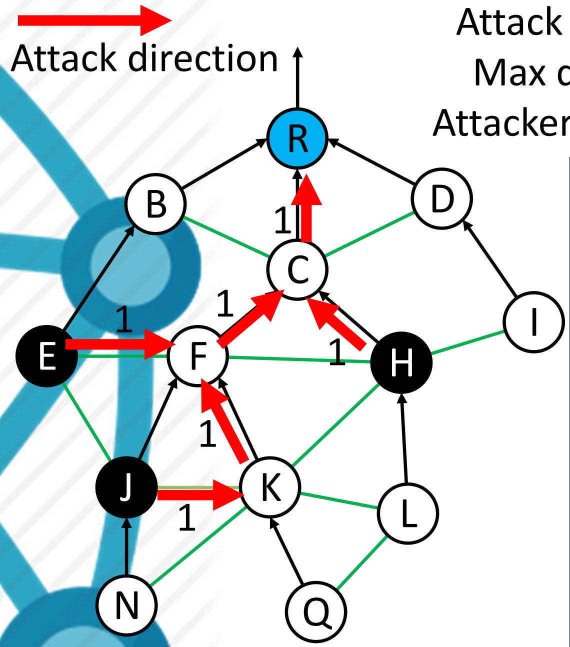
- Attackers
  - Get reporting paths of neighbors by eavesdropping on their packets.
  - Send neighbors’ reporting paths to the master.
  - Can attack a limited number of neighbors at the highest rate.
- Master
  - Formulate partial topology from reporting paths.
  - Selects a set of attackers and target neighbors to maximize attack strength.



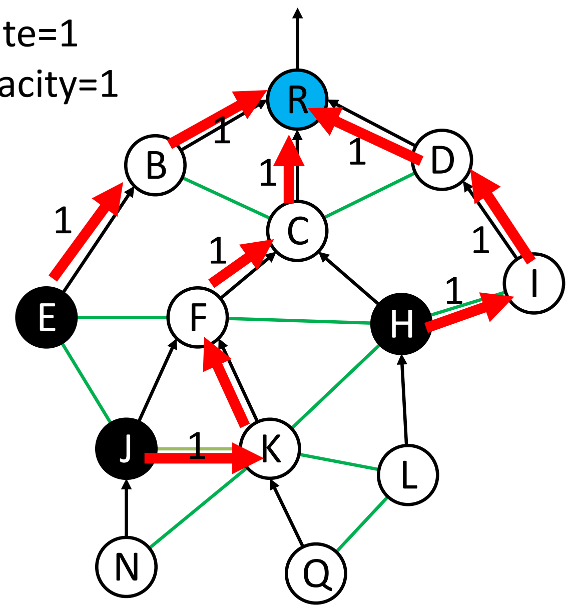
Problem Formulation

- Attack Strength:
  - Attack data receiving rate at root.
- Problem:
  - Find the smallest set of target neighbors.
- Constraint:
  - Attack strength must be the maximum.
  - Number of target neighbors of each attacker < attacker's capacity.

Attack data rate=1
Max data rate=1
Attacker's capacity=1



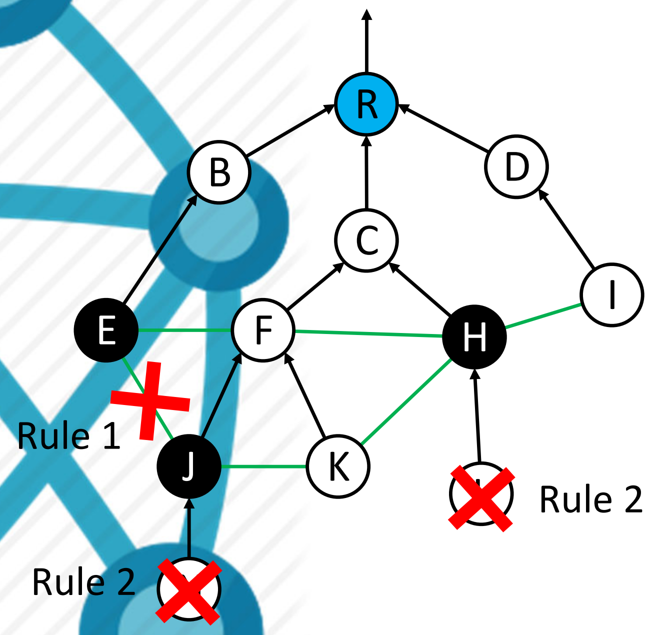
Attack strength =1
(not maximum)



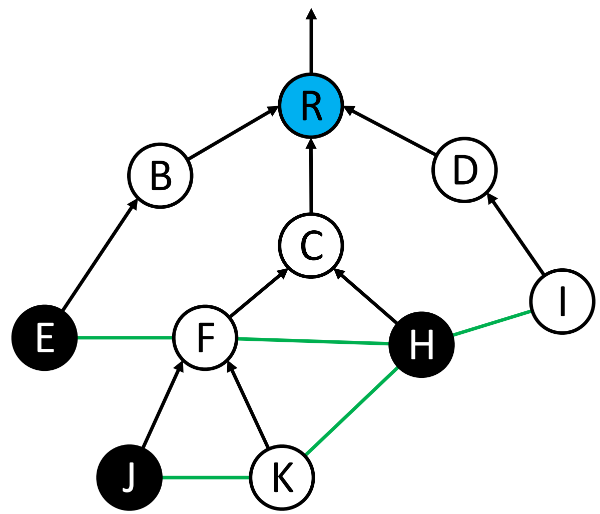
Attack strength =3
(maximum)

Solution

- Step 1: Neighbor Pruning
  - Rule 1: Remove attacker neighbors
  - Rule 2: Remove neighbors having attacker on reporting path
- Step 2: Flow Graph Creation
  - Add virtual source node
  - Add edges from S to all attacker
  - Set link capacity
- Step 3: Optimal Target Set Computation
  - Max flow problem solving



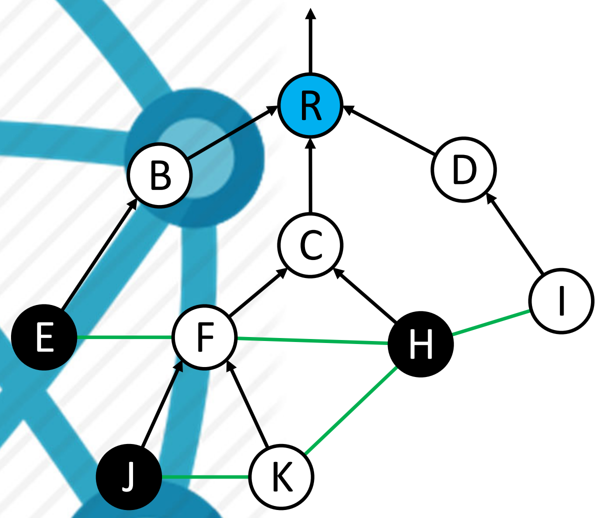
Master's view



After pruning

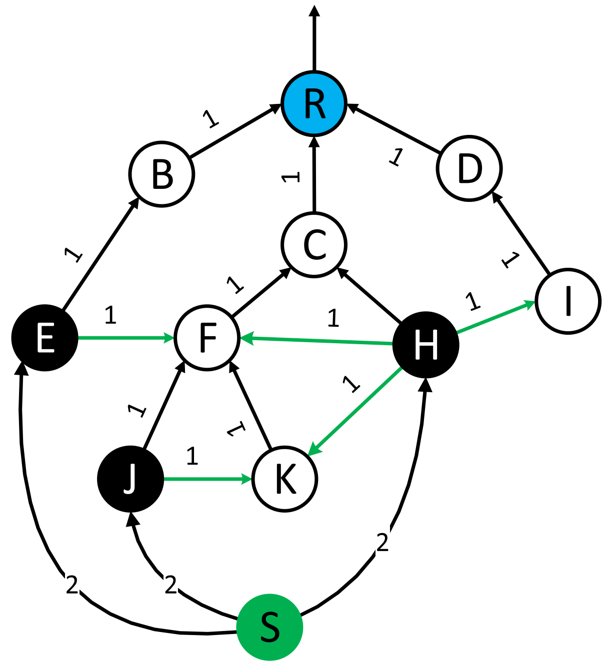
Solution

- Step 1: Neighbor Pruning
  - Rule 1: Remove attacker neighbors
  - Rule 2: Remove neighbors having attacker on reporting path
- Step 2: Flow Graph Creation
  - Add virtual source node
  - Add edges from S to all attacker
  - Set link capacity
- Step 3: Optimal Target Set Computation
  - Max flow problem solving



After pruning

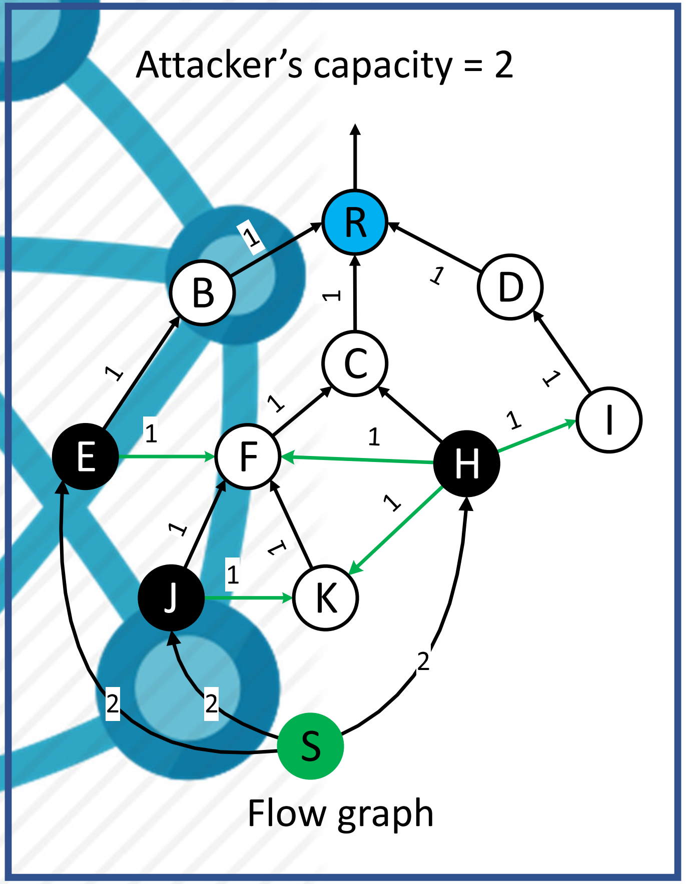
Attacker's capacity = 2

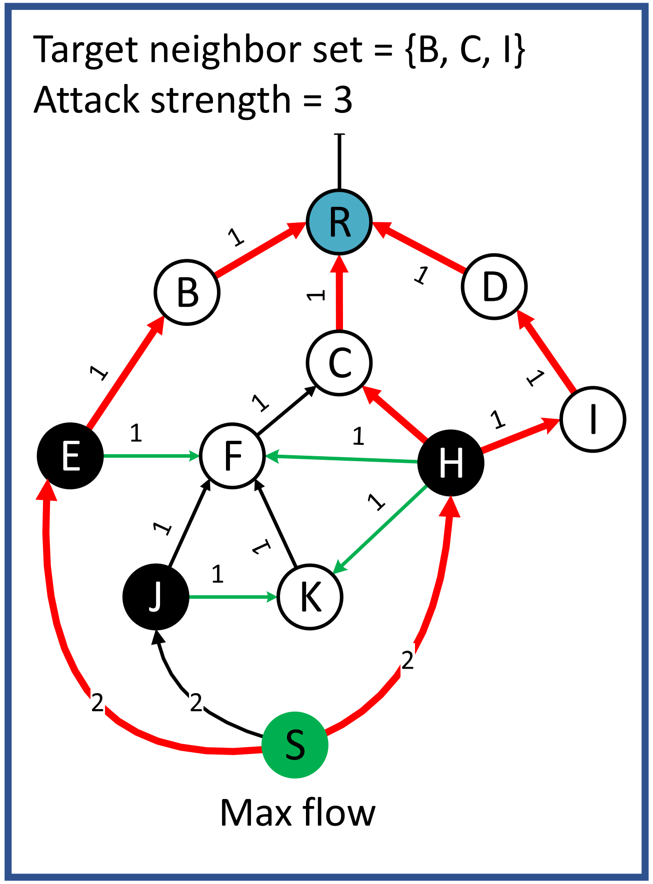


Flow graph

Solution

- Step 1: Neighbor Pruning
  - Rule 1: Remove attacker neighbors
  - Rule 2: Remove neighbor having attacker on reporting path
- Step 2: Flow Graph Creation
  - Add virtual source node
  - Add edges from S to all attacker
  - Set link capacity
- Step 3: Optimal Target Set Computation
  - Max flow problem solving



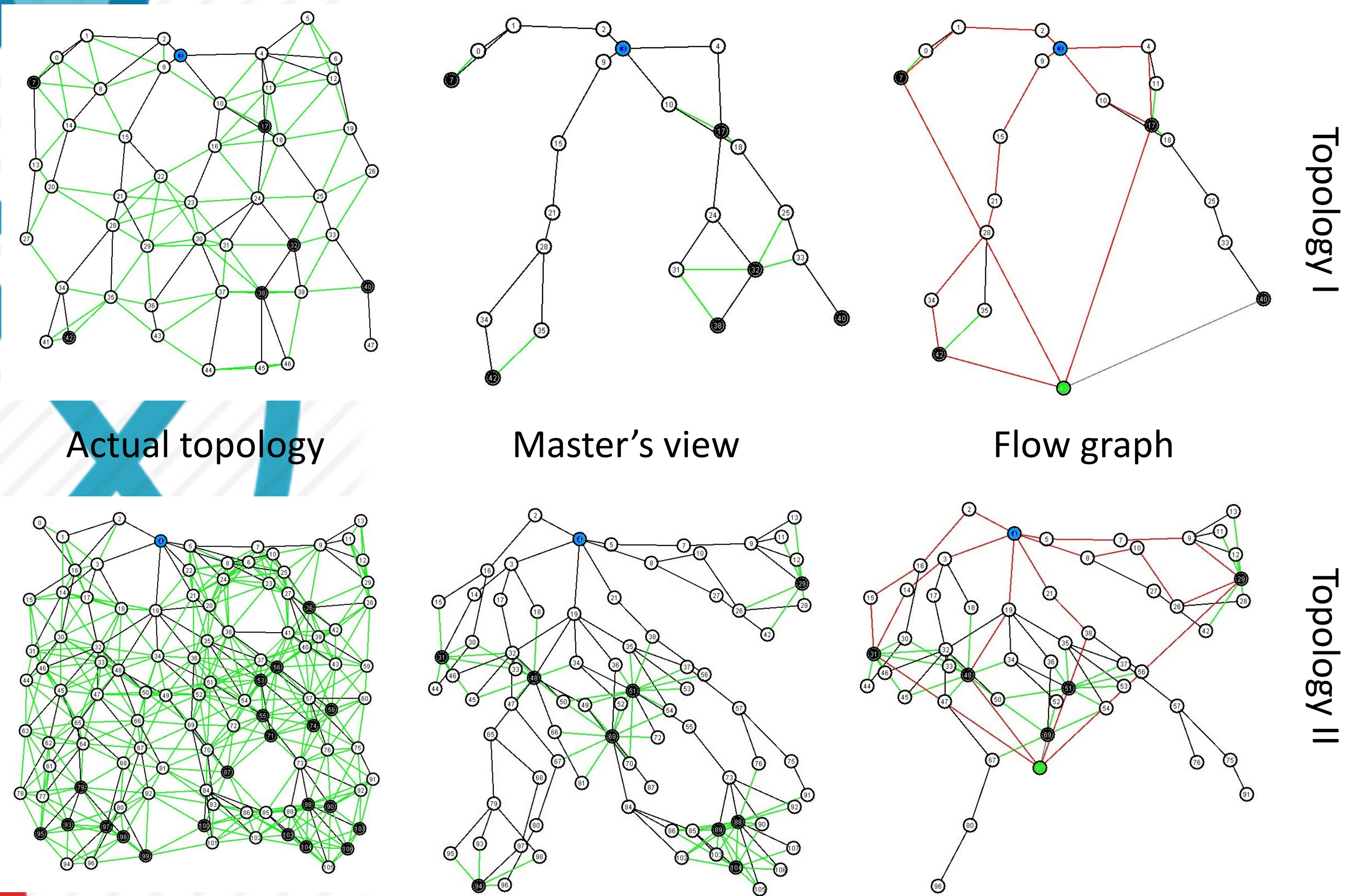


Assignment: E->B, H->C, H->I

Simulation: Random Tree Generation

Topology I
Nodes:47
Attackers: 6
Edges: 131
Degree: 1-8

Topology II
Nodes:107
Attackers: 9
Edges: 558
Degree: 2-17

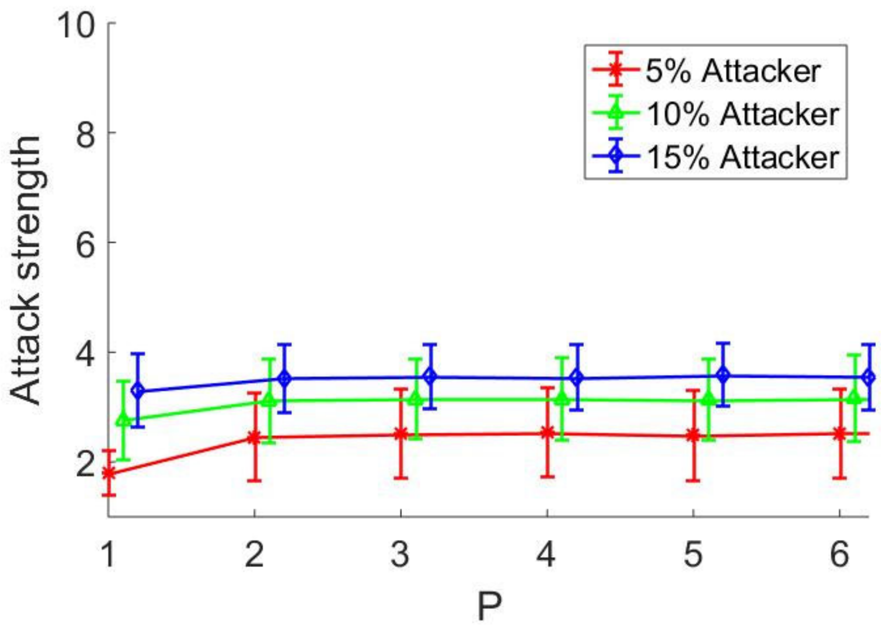


Unite disk graph
Randomly placed nodes (uniform)

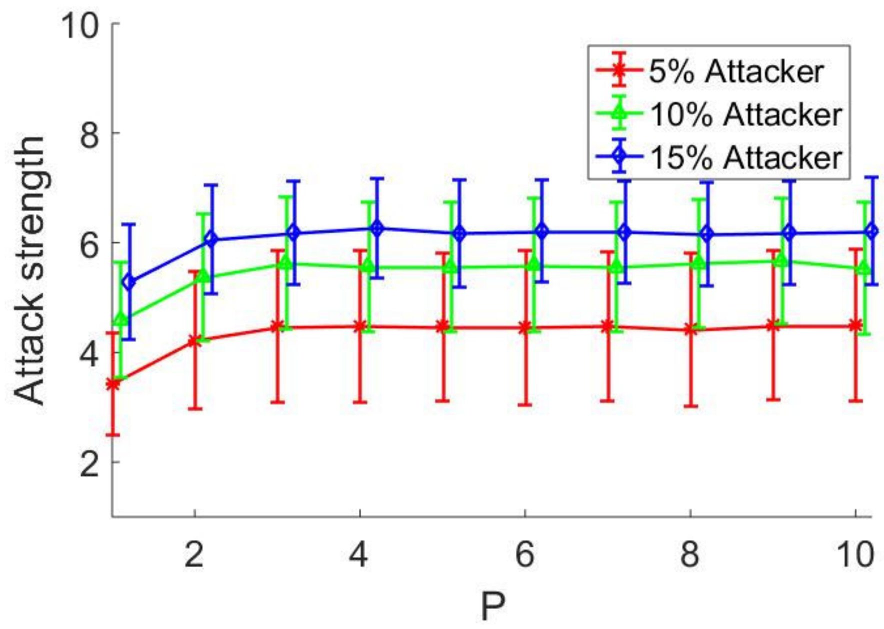
Area: 500x500
Neighborhood radius: 70
Attacker capacity: 2
Attacker ratio: 10%

Simulation: Different Attacker Capacities

Topology I

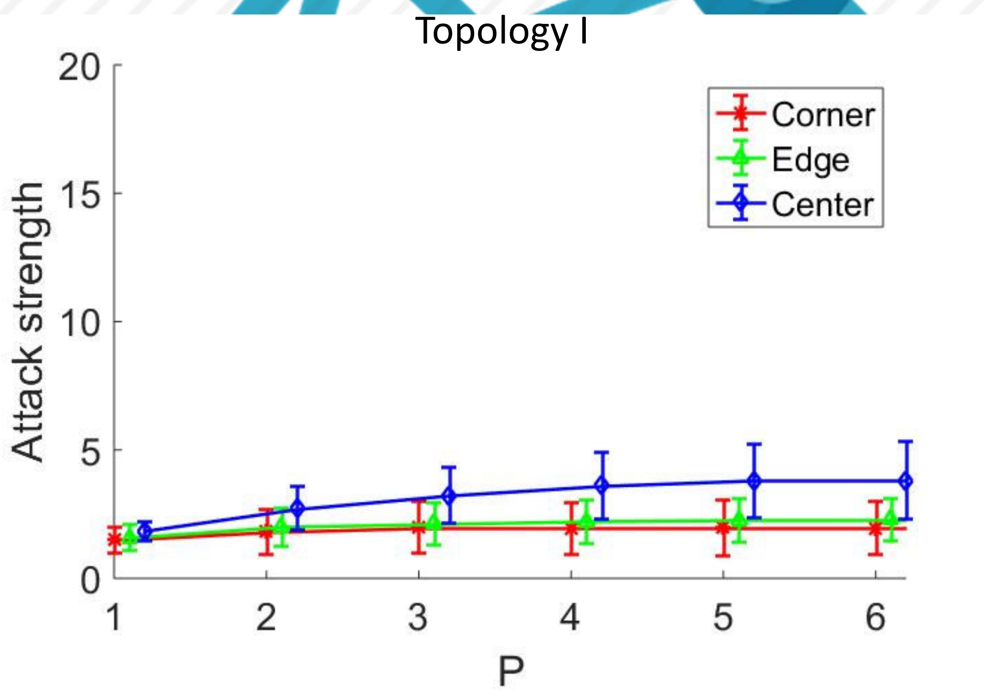


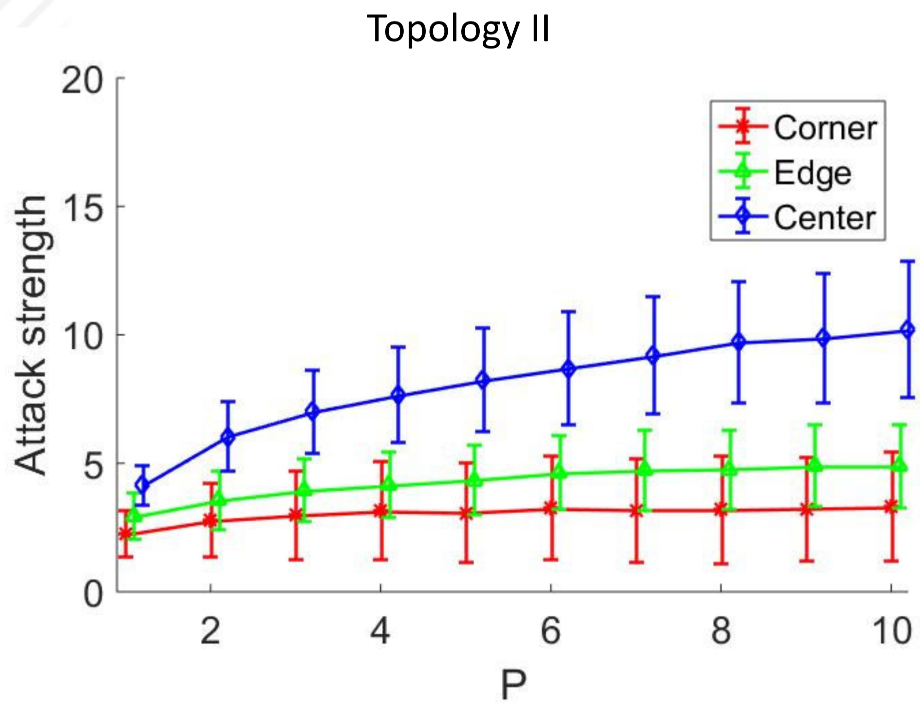
Topology II



Attack strength becomes stable after a certain attacker capacity

Simulation: Different Root Location

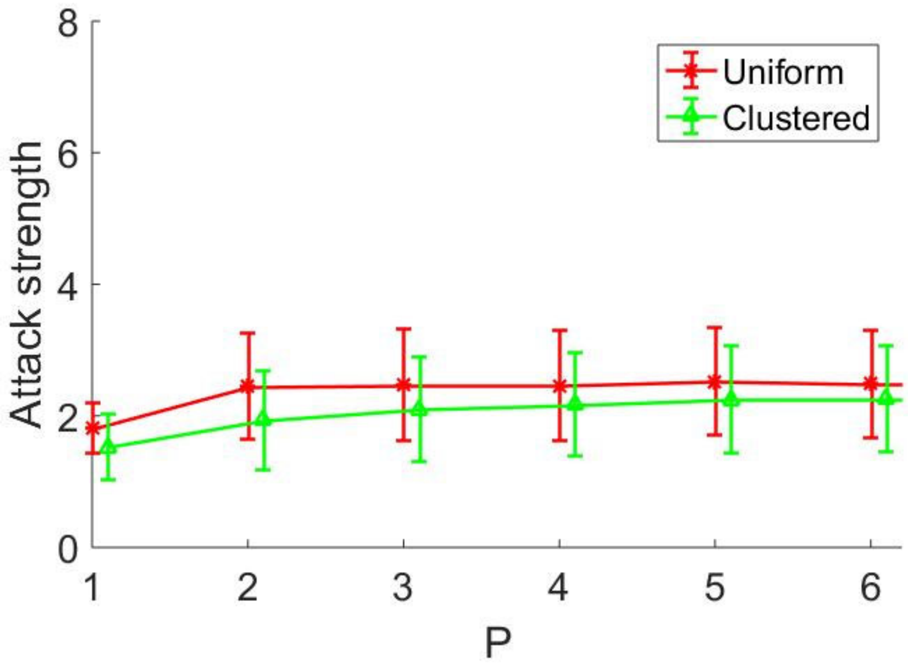




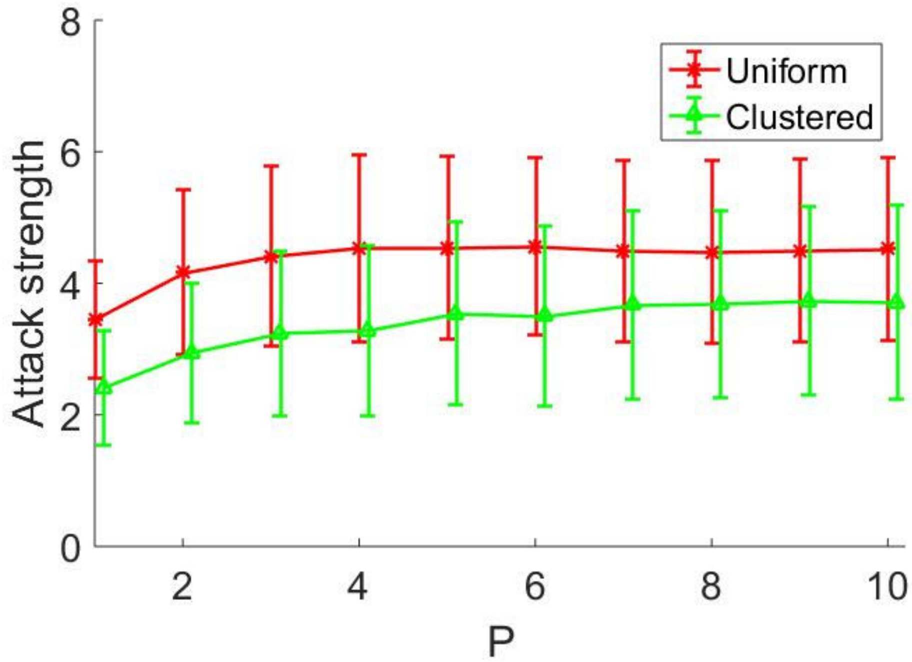
Root at center is more vulnerable than edge and corner.

Simulation: Different Attacker Distribution

Topology I



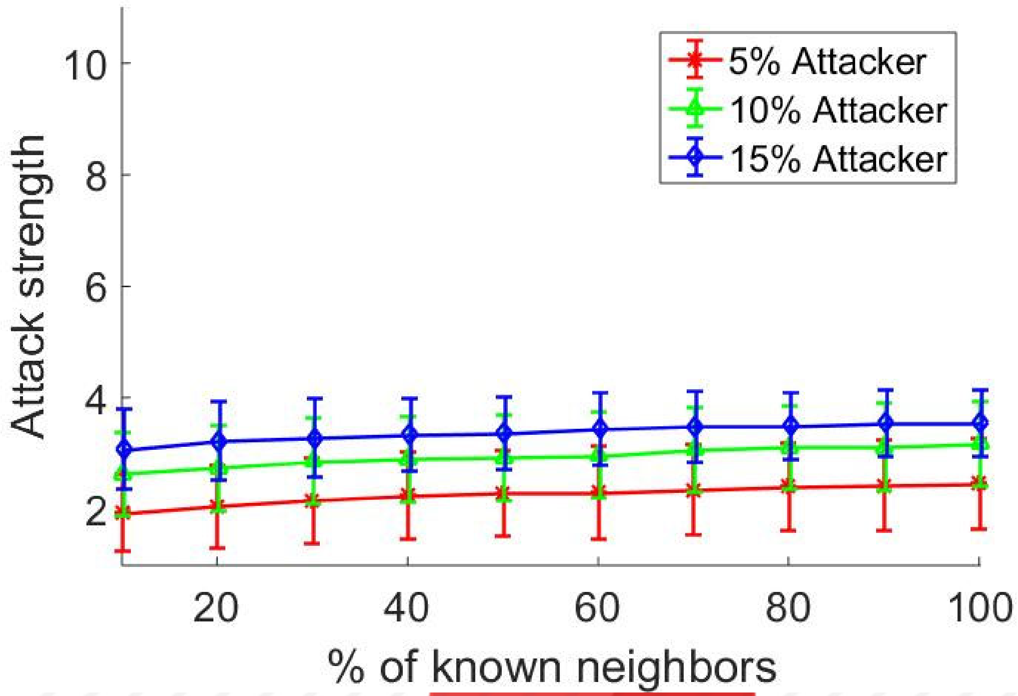
Topology II



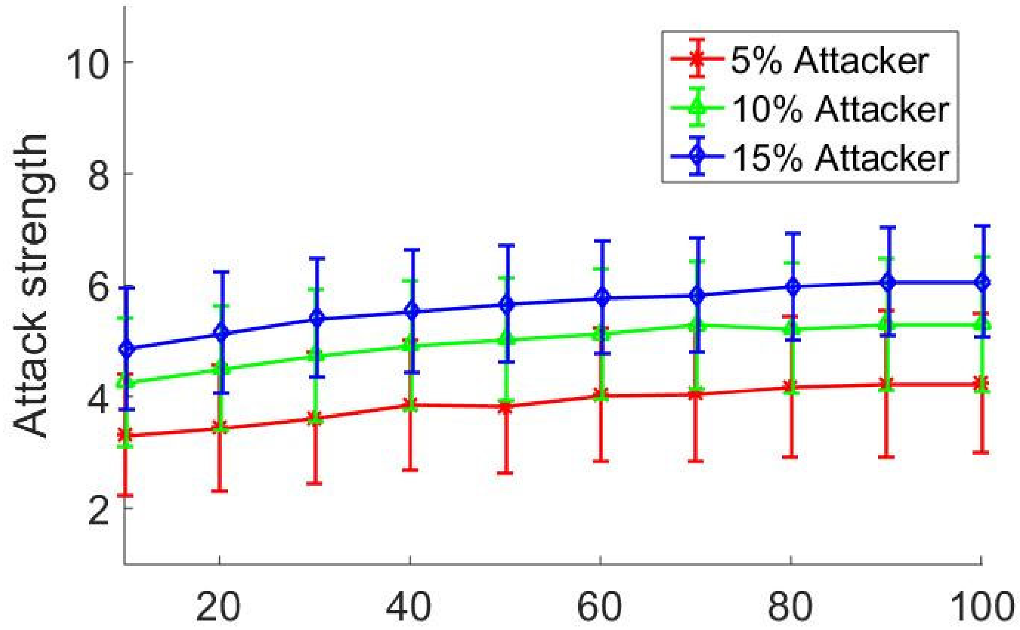
Distributed attackers are more powerful than clustered attackers.
Attacker ratio =10%

Simulation: Different Neighborhood Knowledge

Topology I



Topology II



AY8

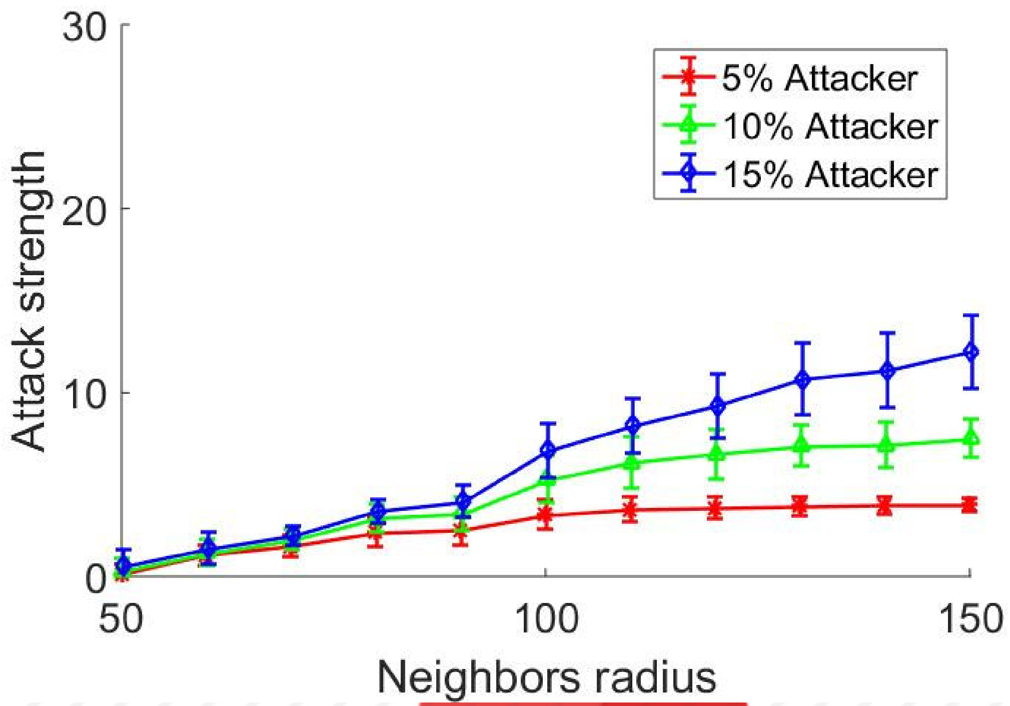
More knowledge about the neighborhood results in more powerful attack

Attacker power (P)= 2

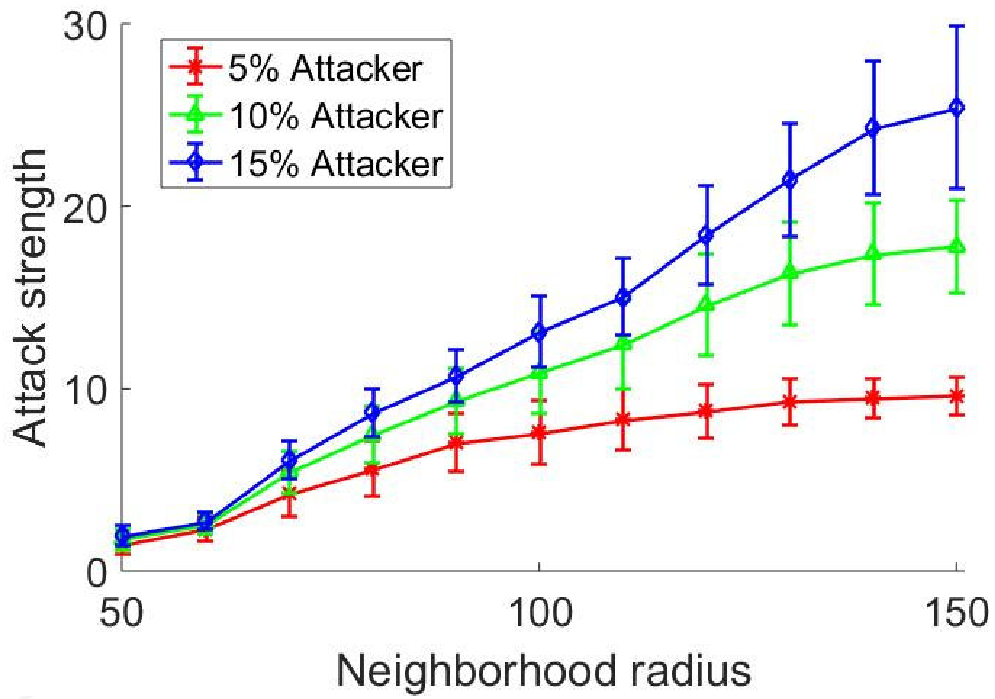
AY8 ...about the neighborhood results in a more powerful attack.
Allison Yu, 9/17/2019

Simulation: Different Neighborhood Radius

Topology I



Topology II

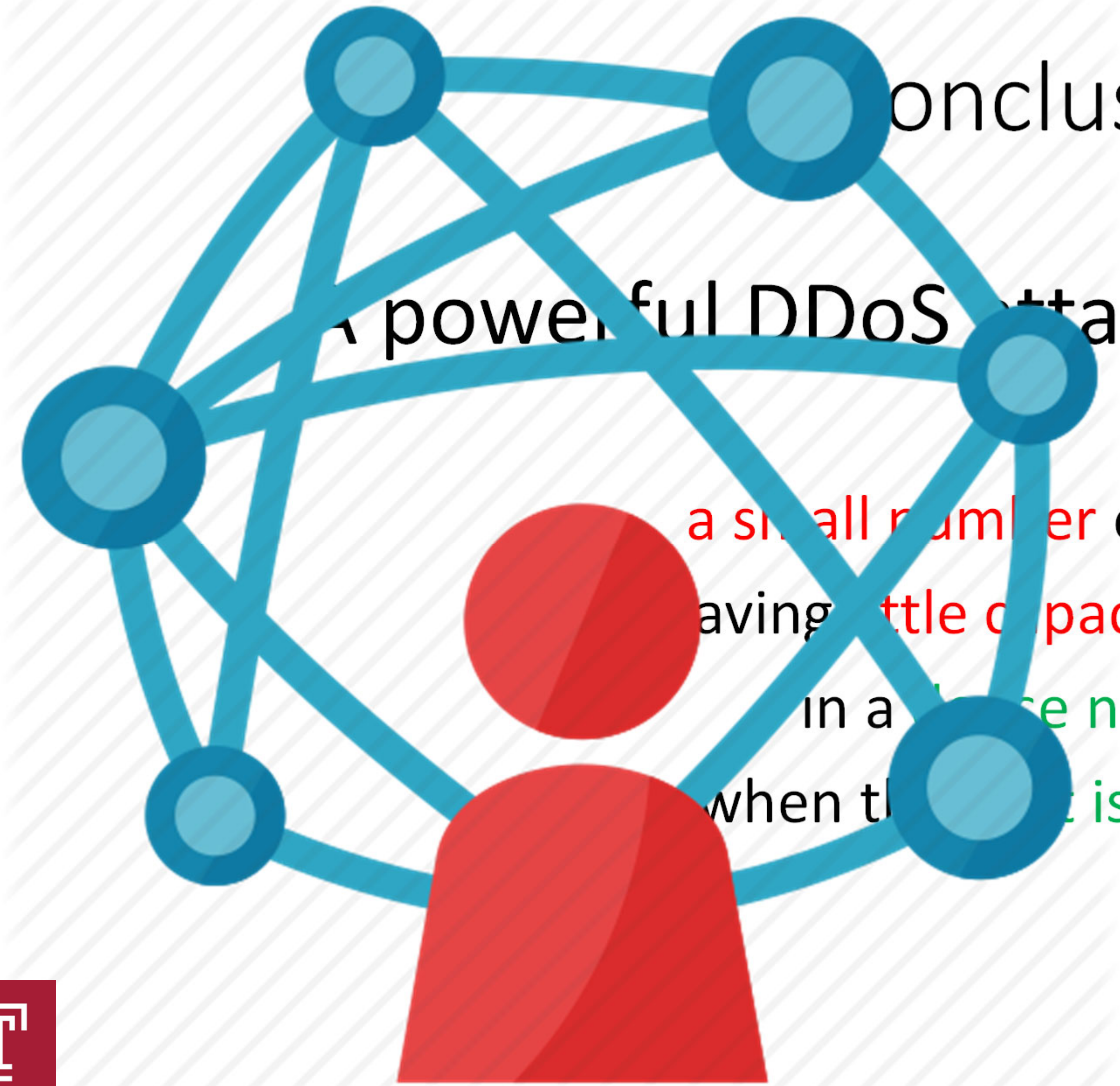


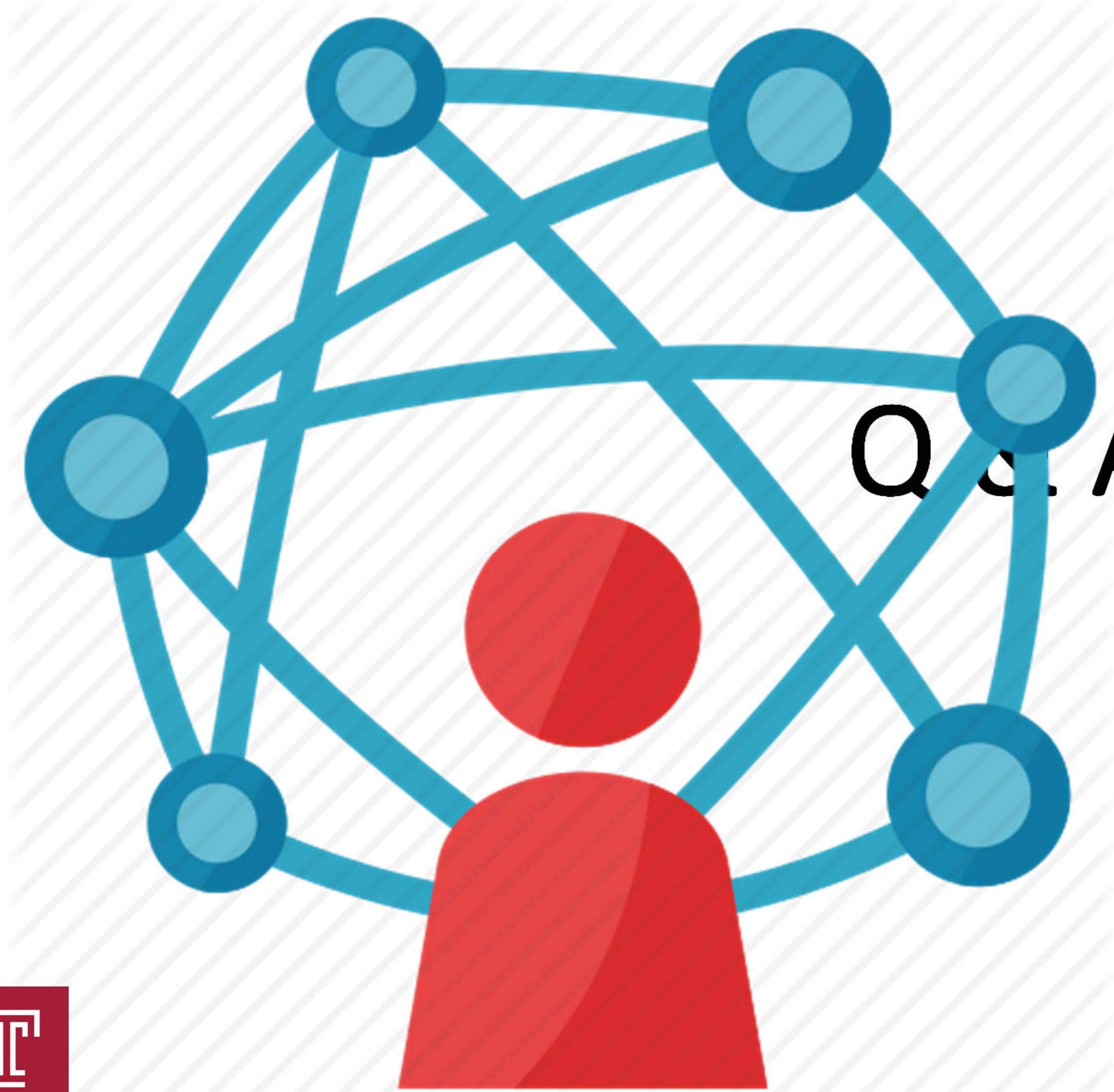
The greater the neighborhood radius, the more the degree and attack strength
Attacker power (P)= 2

[illegible]onclusion

[illegible] powe[illegible]ful DDoS [illegible]ttack is possible with

- a s[illegible]all [illegible]um[illegible]er of attackers
- [illegible]aving [illegible]ttle c[illegible]pacity of attack
- in a [illegible]e network
- when t[illegible] is in middle.





Q & A ???