When Seeing Isn’t Believing: On Feasibility and Detectability of Scapegoating in Network Tomography

Shangqing Zhao, University of South Florida

Zhuo Lu, University of South Florida

Cliff Wang, North Carolina State University

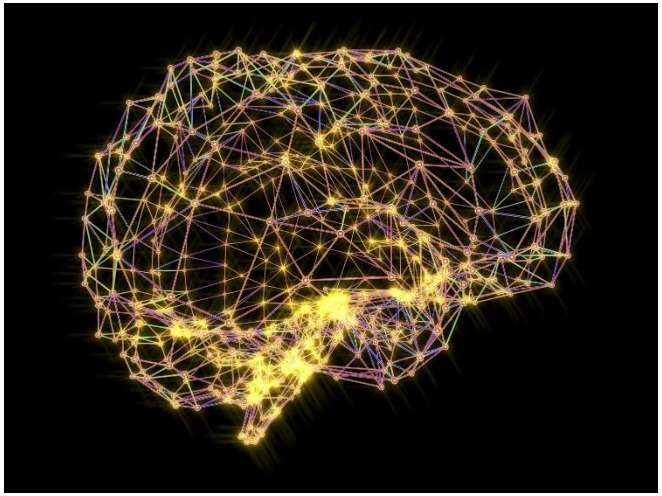
Move to Network Tomography

❖ Motivation:

If we can’t see what’s going on in a network directly, how to measure the network performance?

Directly access is difficult

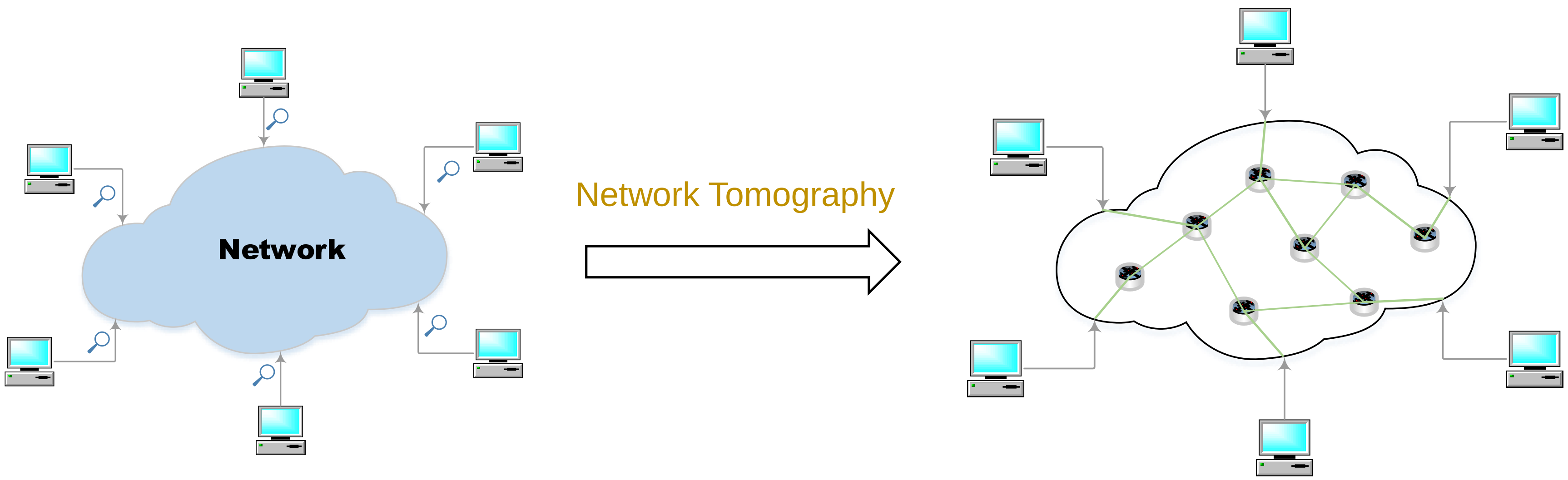
Brain Tomography



Move to Network Tomography

- **Motivation:**

If we can’t see what’s going on in a network directly, how to measure the network performance?



Directly access is difficult

Move to Network Tomography

❖ Definition:

Study internal characteristics (e.g. link delay) of the network from external measurements (e.g. path delay).

- infer the link performance from end-to-end path measurements.

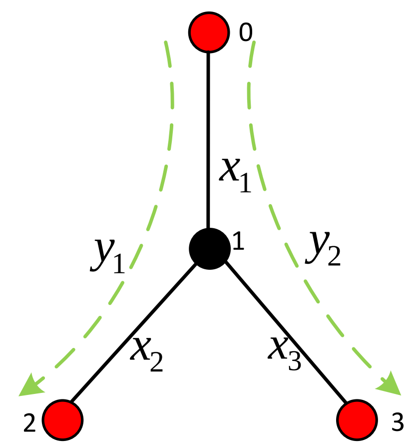
❖ Formulation:

Given

- $\mathbf{R}$: Routing matrix (e.g. $\mathbf{R}=\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$)
- $\mathbf{y}$: Observed path measurement metrics

Based on

$$\mathbf{y} = \mathbf{R}\mathbf{x}$$



Infer link metrics $\mathbf{x}$

$$\hat{\mathbf{x}} = (\mathbf{R}^T\mathbf{R})^{-1}\mathbf{R}^T\mathbf{y}$$

Security Concerns

- **Method of Network Tomography:**

Use the end-to-end path measurements to estimate the link metrics.

- **Assumption: seeing-is-believing**

Measurements indeed reflect the real performance aggregates over individual links.

  - Such assumption does not always hold in the presence of malicious nodes !!!

Traditional Attack

- **Packet dropping attack:**

Intentionally drop or delay packets routed to the malicious nodes.

  - Black hole attack
  - Grey hole attack

- **Weak Point**

Very easy to be detected.

  - Find out the links which always suffer bad performance under network tomography.

Scapegoating Attack

- **Key Idea:**

Attackers cooperatively delay or drop packets to manipulate end-to-end measurements such that a legitimate node is incorrectly identified by network tomography as the root cause of the problem.

- **Methodology**

1. Attacks only damage the path which contains the victim.
2. Attacks be cooperative (delay or drop no packets) on other paths.

Scapegoating Attack

- **Formulation:**
  - Definition: link state

$$S(l_i) = \begin{cases} \text{normal} & x_i < b_l \\ \text{uncertain} & b_l < x_i < b_u \\ \text{abnormal} & x_i > b_u \end{cases}$$

    - x_i is the performance of link i.
    - b_l and b_u are the lower and upper bound.
  - Definition: link set
    - $\mathcal{L}_s$ is the victim link set.

Scapegoating Attack

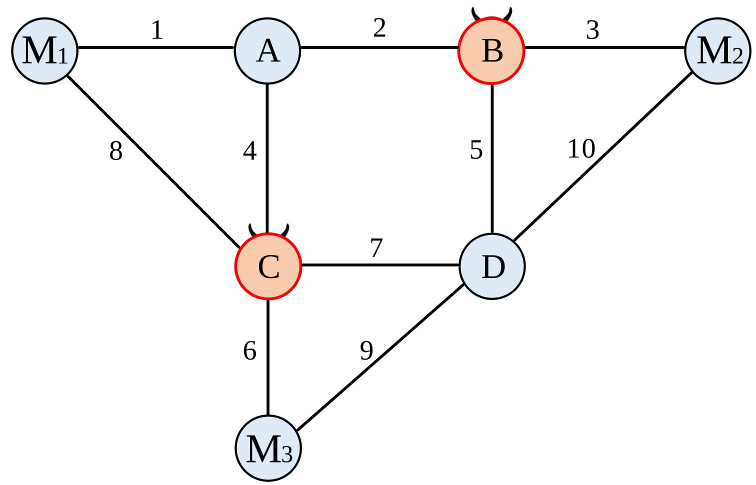
- **Formulation:**
  - Definition: damage

$$\mathbf{y}' = \mathbf{y} + \mathbf{m}$$

    - $\mathbf{y}'$ is the measurements with Scapegoating.
    - $\mathbf{y}$ is the measurements without Scapegoating.
    - $\mathbf{m}$ is the damage caused by attacker

Scapegoating Attack

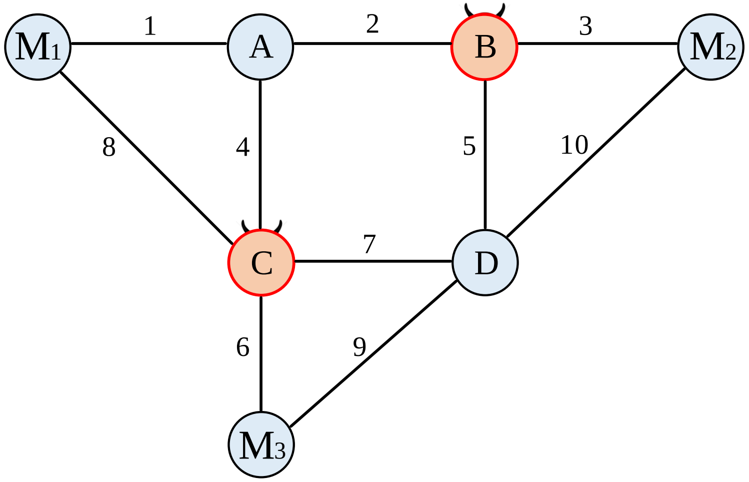
- **Strategies:**



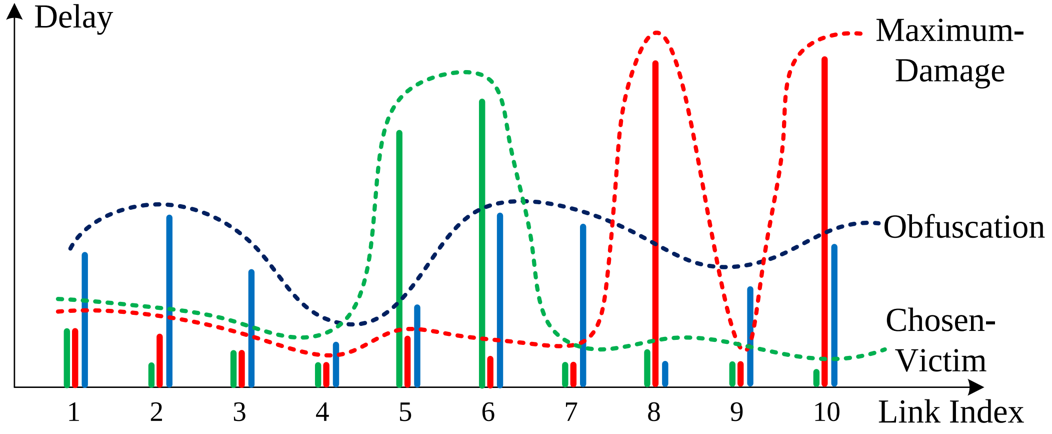
- <u>Chosen-Victim Attack</u>
  - Victim set $\mathcal{L}_s$ is already given.
- <u>Maximum-Damage Attack</u>
  - Maximum damage $\|\mathbf{m}\|_1$ to the network without knowing $\mathcal{L}_s$.
- <u>Obfuscation</u>
  - Make every link look mostly similar without evident outliers.

Scapegoating Attack

❖ **Strategies:**

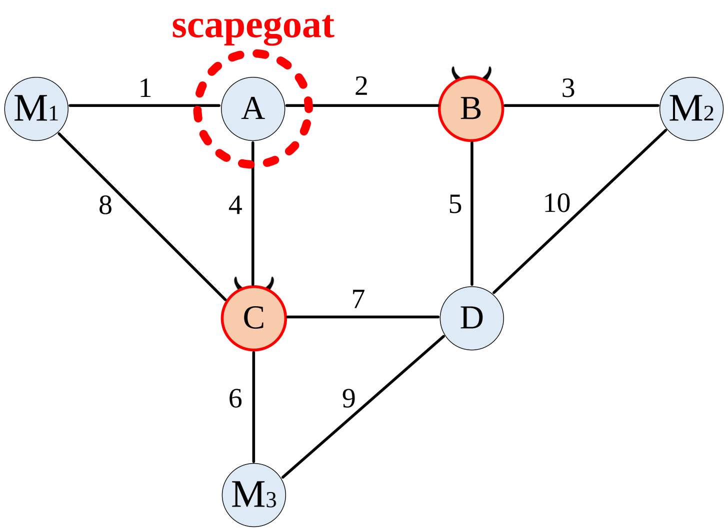


Example of three attacks



Scapegoating Attack

- **Chosen-Victim Attack:**



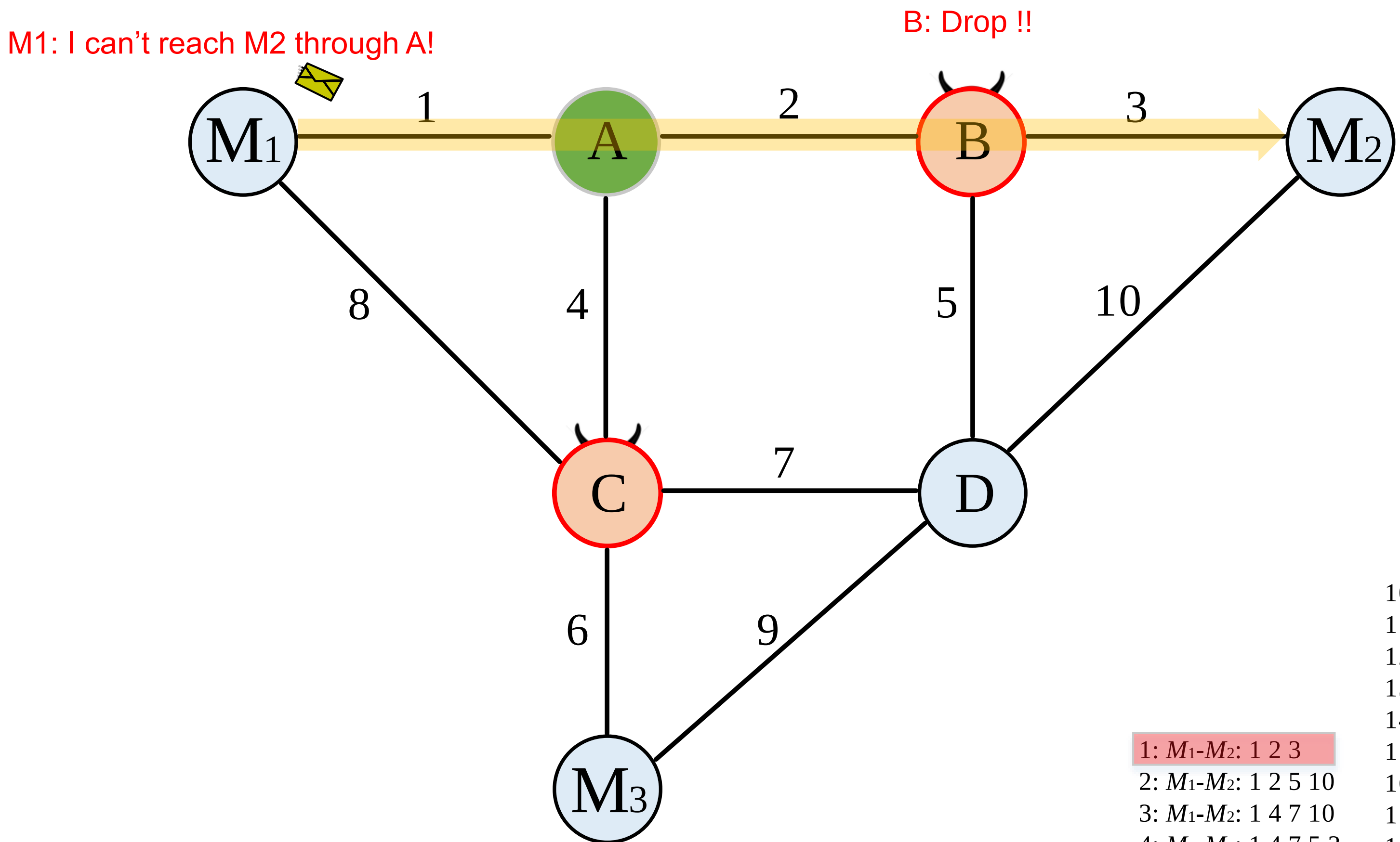
- Objective:

$$\max \|\mathbf{m}\|_1$$

- Subject to:

$$S(l_i) = \begin{cases} \text{abnormal} & i = 1 \\ \text{normal} & others \end{cases}$$

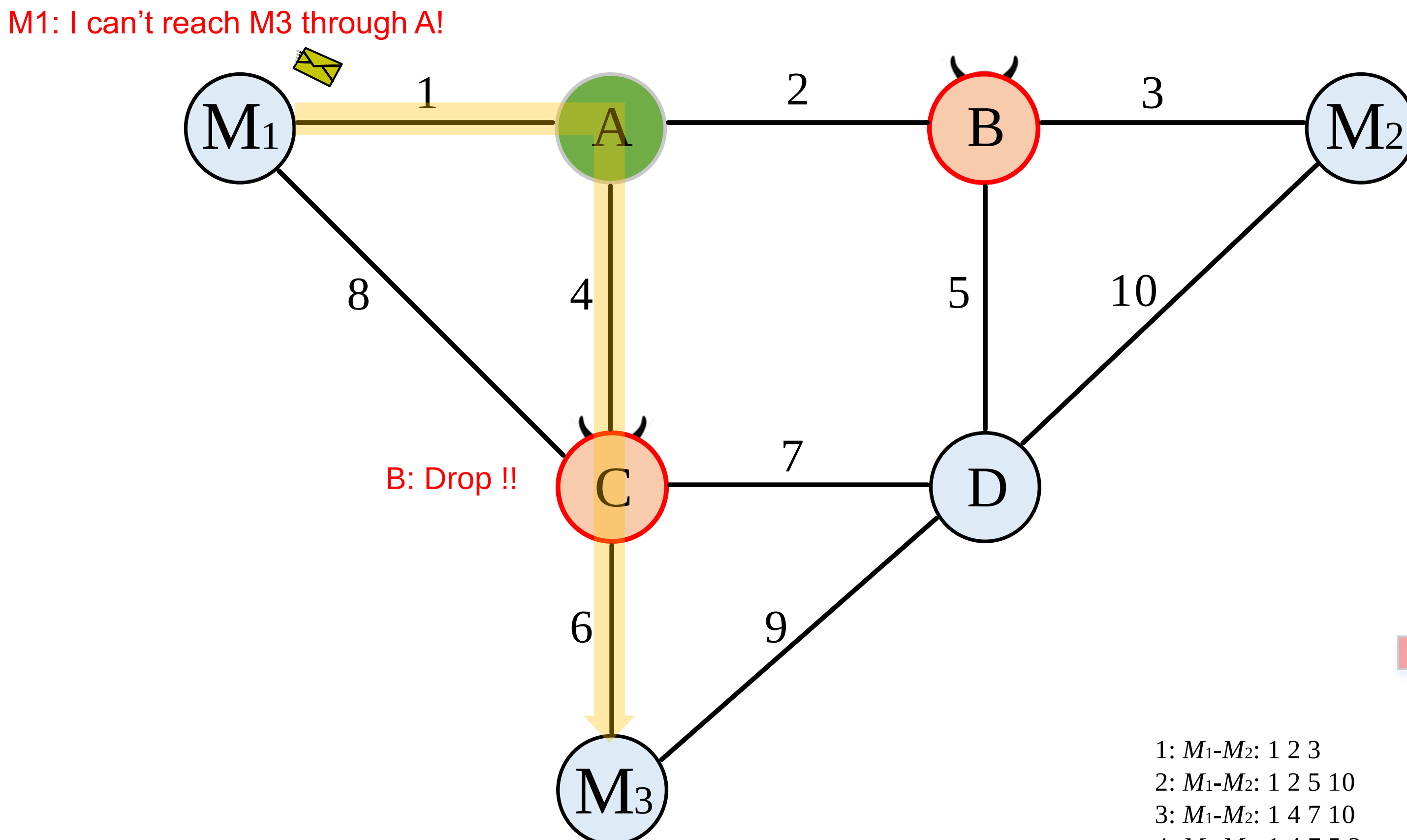
Scapegoating Attack



1: M_1-M_2: 1 2 3
2: M_1-M_2: 1 2 5 10
3: M_1-M_2: 1 4 7 10
4: M_1-M_2: 1 4 7 5 3
5: M_1-M_2: 1 4 6 9 10
6: M_1-M_2: 8 7 10
7: M_1-M_2: 8 7 5 3
8: M_1-M_2: 8 6 9 10
9: M_1-M_2: 8 6 9 5 3
10: M_1-M_3: 8 6
11: M_1-M_3: 8 7 9
12: M_1-M_3: 1 4 6
13: M_1-M_3: 1 4 7 9
14: M_1-M_3: 1 2 5 9
15: M_1-M_3: 1 2 5 7 6
16: M_1-M_3: 1 2 3 10 9
17: M_2-M_3: 10 9
18: M_2-M_3: 10 7 6
19: M_2-M_3: 3 5 9
20: M_2-M_3: 3 5 7 6
21: M_2-M_3: 3 2 4 6
22: M_2-M_3: 3 2 4 7 9
23: M_2-M_3: 3 2 1 8 6

- Monitors: M_1, M_2,M_3
- Attackers: B, C
- Victim: A

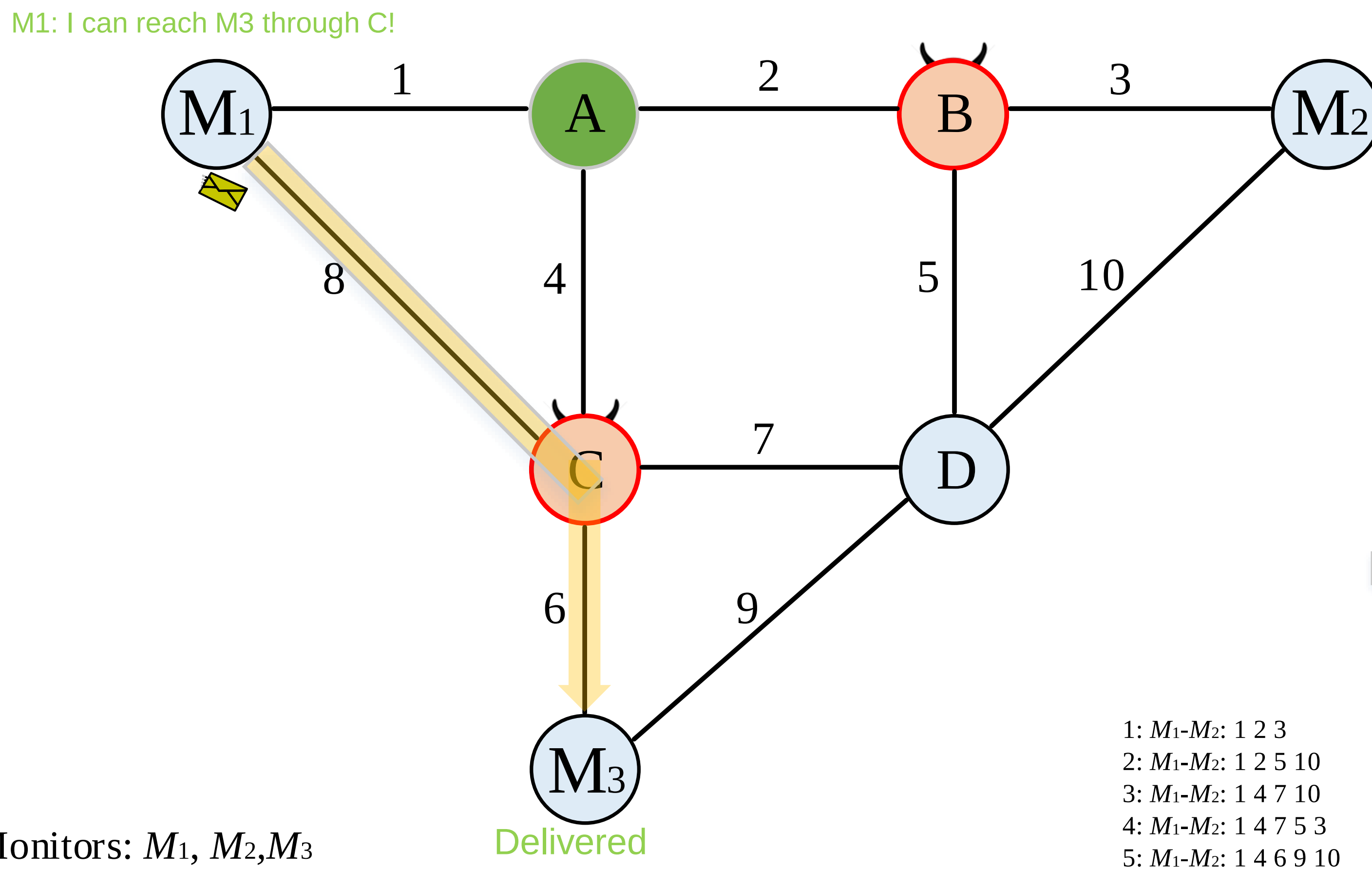
Scapegoating Attack



1: M_1-M_2: 1 2 3
2: M_1-M_2: 1 2 5 10
3: M_1-M_2: 1 4 7 10
4: M_1-M_2: 1 4 7 5 3
5: M_1-M_2: 1 4 6 9 10
6: M_1-M_2: 8 7 10
7: M_1-M_2: 8 7 5 3
8: M_1-M_2: 8 6 9 10
9: M_1-M_2: 8 6 9 5 3
10: M_1-M_3: 8 6
11: M_1-M_3: 8 7 9
12: M_1-M_3: 1 4 6
13: M_1-M_3: 1 4 7 9
14: M_1-M_3: 1 2 5 9
15: M_1-M_3: 1 2 5 7 6
16: M_1-M_3: 1 2 3 10 9
17: M_2-M_3: 10 9
18: M_2-M_3: 10 7 6
19: M_2-M_3: 3 5 9
20: M_2-M_3: 3 5 7 6
21: M_2-M_3: 3 2 4 6
22: M_2-M_3: 3 2 4 7 9
23: M_2-M_3: 3 2 1 8 6

- Monitors: M_1, M_2,M_3
- Attackers: B, C
- Victim: A

Scapegoating Attack

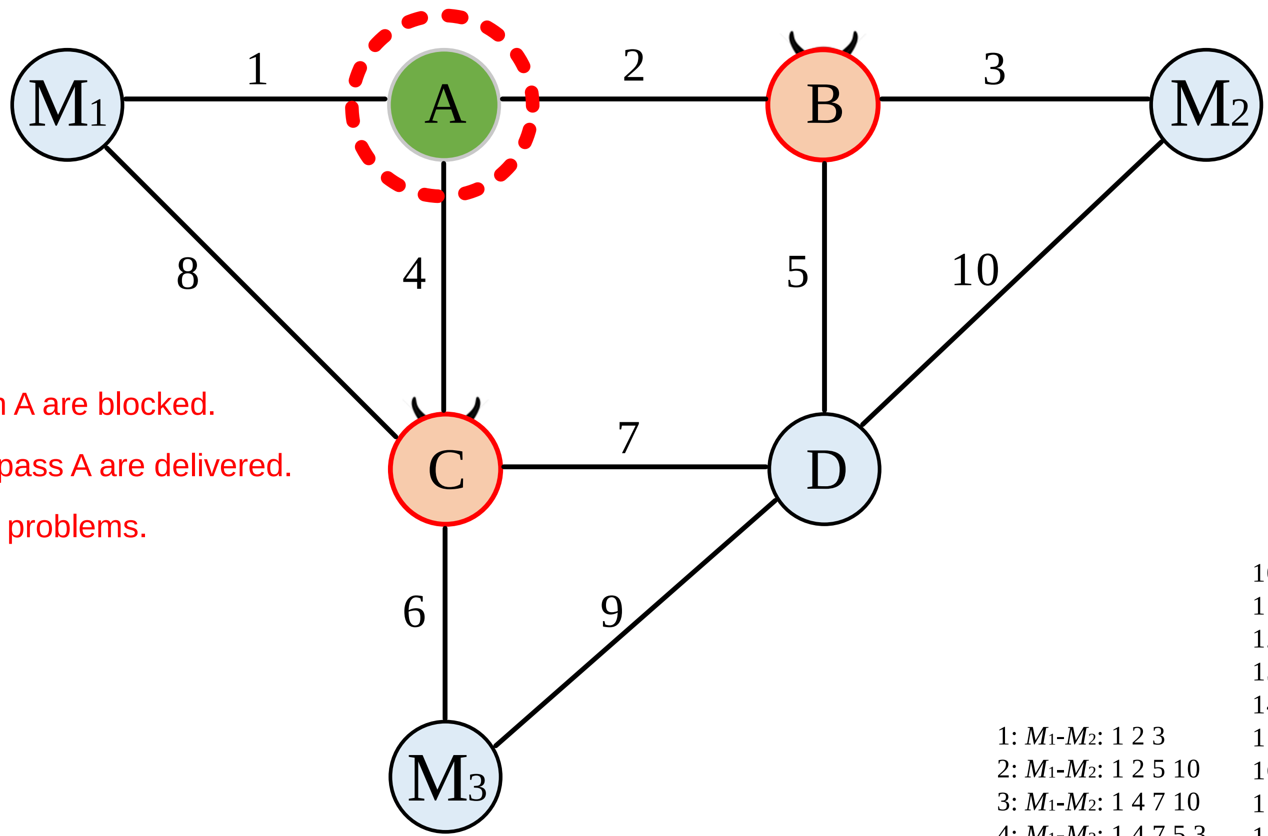


10: M_1-M_3: 8 6
11: M_1-M_3: 8 7 9
12: M_1-M_3: 1 4 6
13: M_1-M_3: 1 4 7 9
14: M_1-M_3: 1 2 5 9
15: M_1-M_3: 1 2 5 7 6
16: M_1-M_3: 1 2 3 10 9
17: M_2-M_3: 10 9
18: M_2-M_3: 10 7 6
19: M_2-M_3: 3 5 9
20: M_2-M_3: 3 5 7 6
21: M_2-M_3: 3 2 4 6
22: M_2-M_3: 3 2 4 7 9
23: M_2-M_3: 3 2 1 8 6

1: M_1-M_2: 1 2 3
2: M_1-M_2: 1 2 5 10
3: M_1-M_2: 1 4 7 10
4: M_1-M_2: 1 4 7 5 3
5: M_1-M_2: 1 4 6 9 10
6: M_1-M_2: 8 7 10
7: M_1-M_2: 8 7 5 3
8: M_1-M_2: 8 6 9 10
9: M_1-M_2: 8 6 9 5 3

- Monitors: M_1, M_2,M_3
- Attackers: B, C
- Victim: A

Scapegoating Attack



All packets through A are blocked.

All packets do not pass A are delivered.

A must have some problems.

- Monitors: M_1, M_2,M_3
- Attackers: B, C
- Victim: A

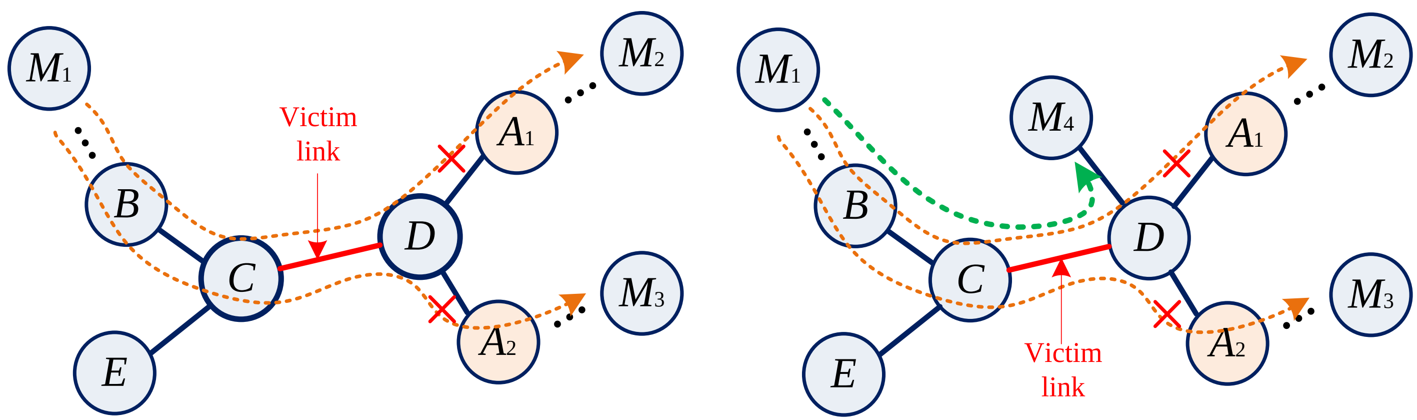
1: M_1-M_2: 1 2 3
2: M_1-M_2: 1 2 5 10
3: M_1-M_2: 1 4 7 10
4: M_1-M_2: 1 4 7 5 3
5: M_1-M_2: 1 4 6 9 10
6: M_1-M_2: 8 7 10
7: M_1-M_2: 8 7 5 3
8: M_1-M_2: 8 6 9 10
9: M_1-M_2: 8 6 9 5 3

10: M_1-M_3: 8 6
11: M_1-M_3: 8 7 9
12: M_1-M_3: 1 4 6
13: M_1-M_3: 1 4 7 9
14: M_1-M_3: 1 2 5 9
15: M_1-M_3: 1 2 5 7 6
16: M_1-M_3: 1 2 3 10 9
17: M_2-M_3: 10 9
18: M_2-M_3: 10 7 6
19: M_2-M_3: 3 5 9
20: M_2-M_3: 3 5 7 6
21: M_2-M_3: 3 2 4 6
22: M_2-M_3: 3 2 4 7 9
23: M_2-M_3: 3 2 1 8 6

Feasibility Analysis

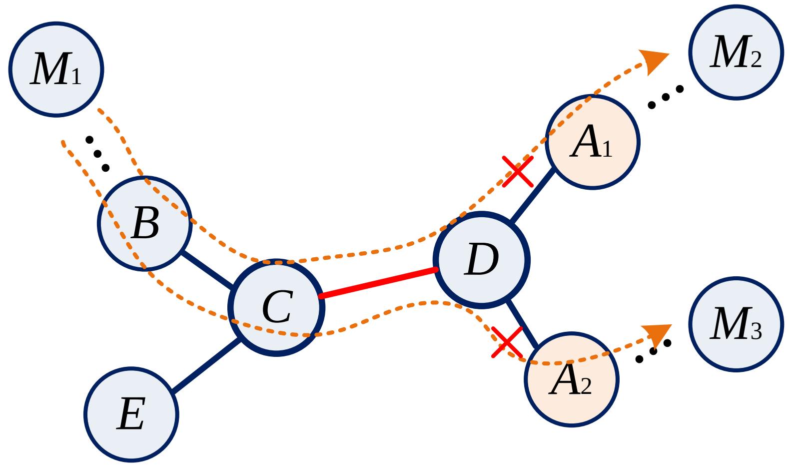
❖ Definition

- Perfect cut: For any measurement path *P* containing a victim link, there always exists at least one malicious node present on *P*.
- *Imperfect cut:* For at least one path *P* containing a victim link, there is no malicious one present on *P*



(a) Perfect Cut (b) Imperfect Cut

Feasibility Analysis

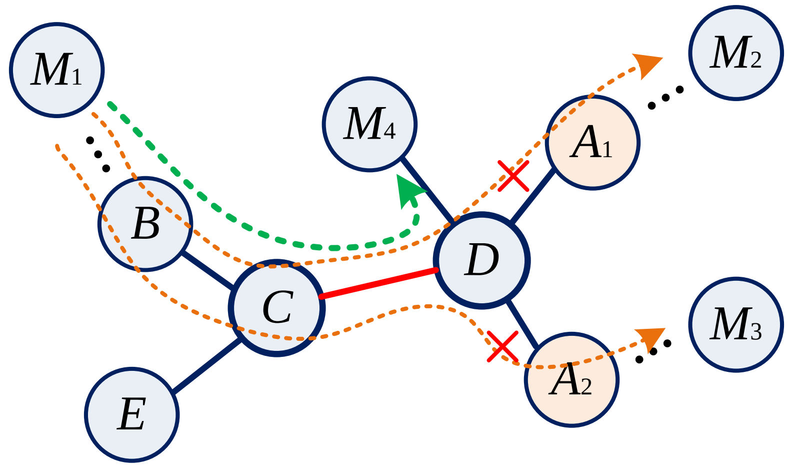


(a) Perfect Cut

Theorem 1 (Feasibility under perfect cut):

Scapegoating is always feasible if the set of malicious nodes can perfectly cut the set of victim links from all measurements paths.

Feasibility Analysis



(b) Imperfect Cut

Theorem 2 (Scapegoating Success Probability under Imperfect Cut):

> Under generic random assumptions, the scapegoating success probability is an increasing function of the number of measurement paths that include at least one victim link and at least one attacker.

Detectability Analysis

❖ Detection mechanism

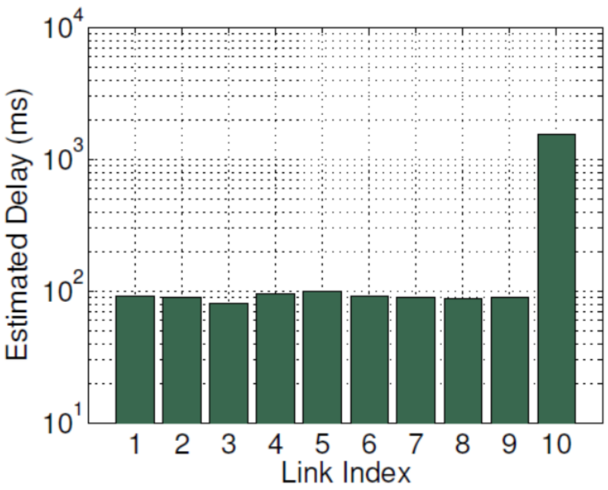
$$\text{scapegoating} = \begin{cases} \text{exists}, & \text{if } R\hat{x} \neq y', \\ \text{does not exist}, & \text{if } R\hat{x} = y'. \end{cases}$$

➢ Theorem 3 (Detectability):

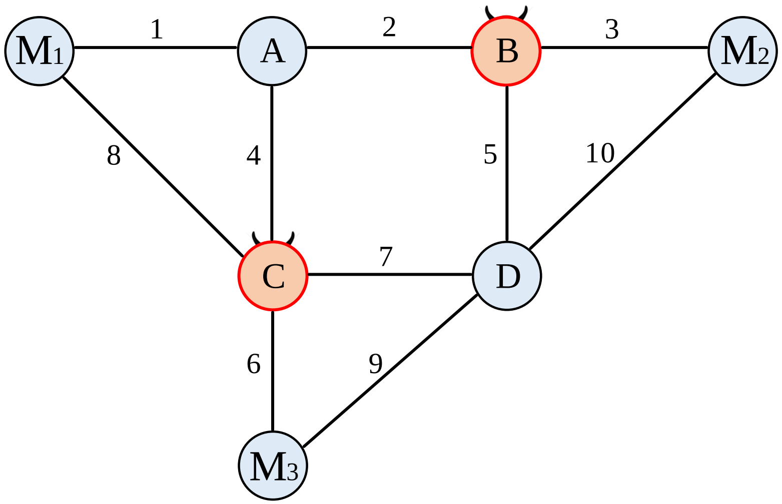
Scapegoating is undetectable if attackers can perfectly cut victim links from measurement paths or $\mathbf{R}$ is a square matrix; and is detectable otherwise.

Experimental Evaluation

❖ Feasibility evaluation



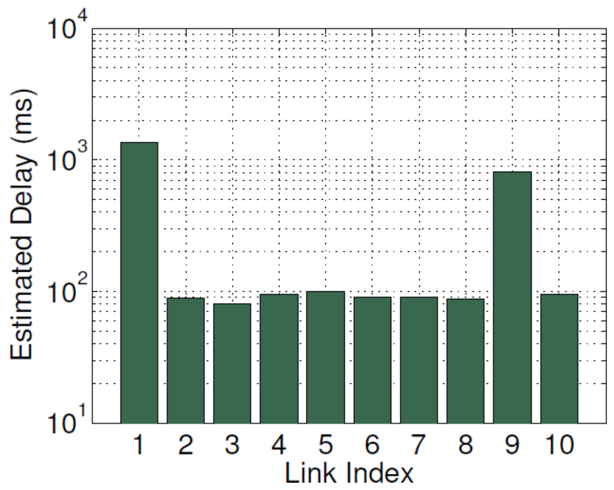
Chosen-Victim Attack



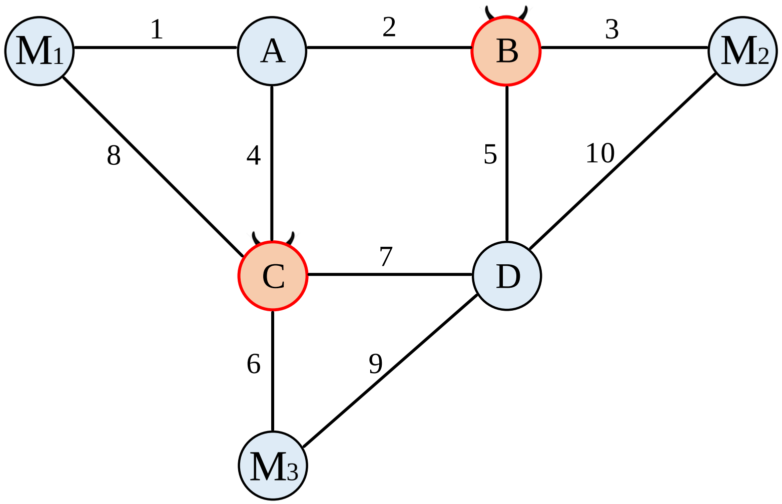
➢ Link 10 has a very high delay.

Experimental Evaluation

❖ Feasibility evaluation



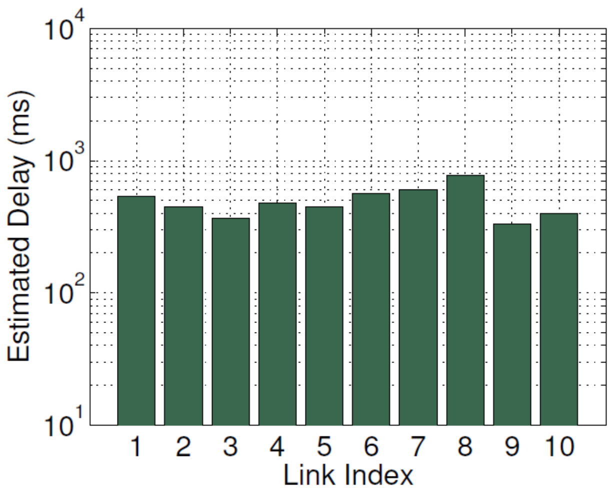
Maximum-Damage Attack



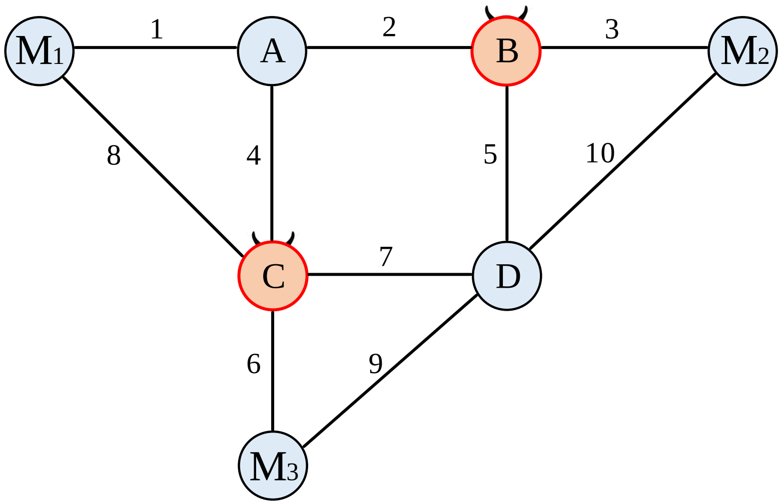
➢ Delay of both link 1 and 9 are high.

Experimental Evaluation

❖ Feasibility evaluation



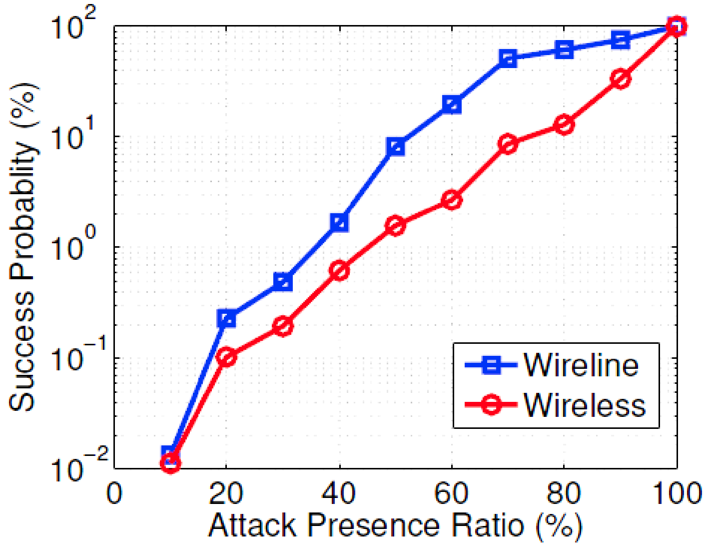
Obfuscation



➢ Delay of all links are similar.

Experimental Evaluation

- **Success probabilities evaluation**
  - Use the Rocketfuel datasets as topologies for wireline networks.
  - Use random geometric graph to generate wireless network topologies.

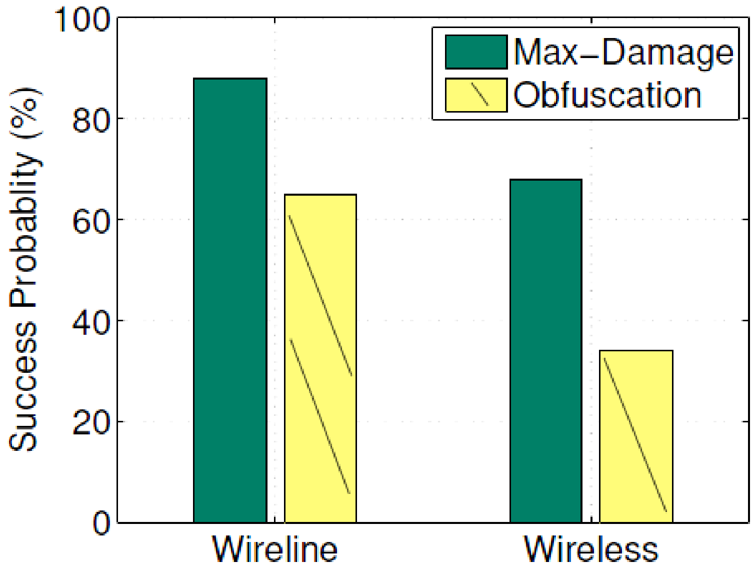


The success probability increases as the attack presence ratio increases under Chosen-victim scapegoating.

Experimental Evaluation

❖ **Success probabilities evaluation**

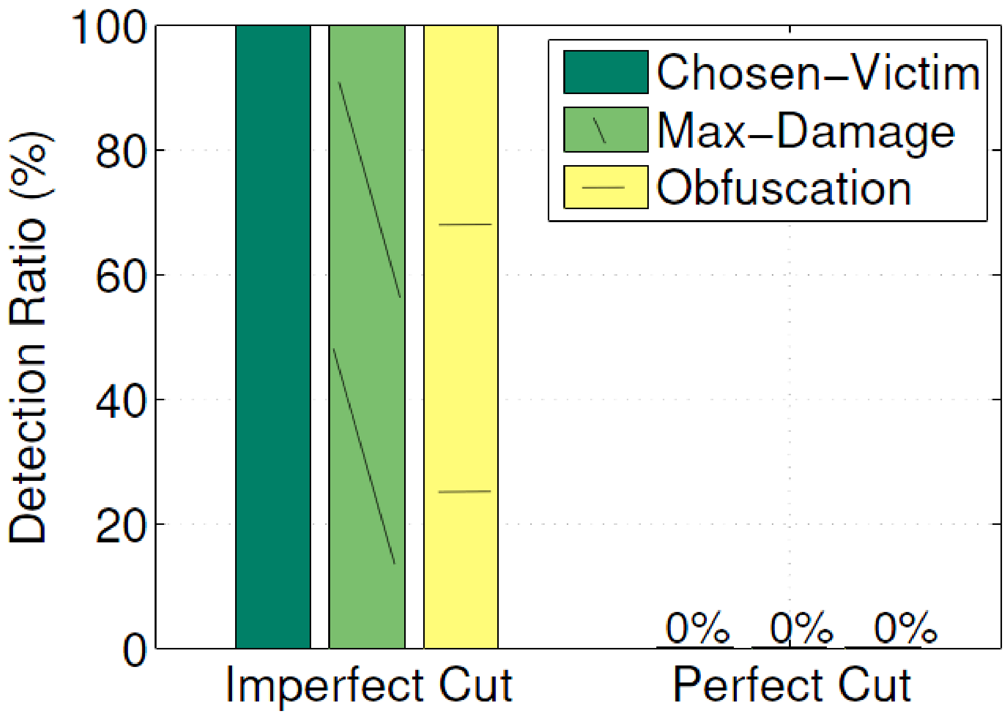
- ➢Use the Rocketfuel datasets as topologies for wireline networks.
- ➢Use random geometric graph to generate wireless network topologies.



Even one single attacker is likely to succeed, and maximum-damage attacks are always more likely than chosen-victim attacks.

Experimental Evaluation

- **Detection evaluation**



Perfect attack is undetectable.

Summary

- All three attack strategies are practical threats in network tomography scenarios.

- Perfect cut scenario is undetectable.

- We should not simply trust measurements.

Q&A

Thanks