Vulnerability Analysis, Attack Strategies and Countermeasures Design in Network Tomography

Shangqing Zhao[†], Zhe Qu[†], Zhuo Lu[†], Cliff Wang[‡]

[†] Department of Electrical Engineering, College of Engineering, University of South Florida, Tampa, FL 33630;

[‡] Department of Electrical & Computer Engineering, College of Engineering, North Carolina State University, Raleigh, NC 27695

Abstract

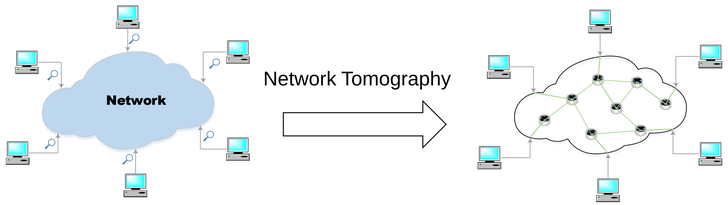
Network tomography is a vital tool to estimate link metrics from end-to-end measurements. However, simply trusting end-to-end measurements leads to measurement integrity vulnerabilities when attackers occur in a network because they can intentionally manipulate link metrics via delaying or dropping packets to affect measurements.

In this proposed poster, we show that the vulnerability in network tomography is real and describe our attack strategy, called ***scapegoating***. We present three basic scapegoating approaches and show the conditions that attacks can be successful. In addition, we show how to detect and locate such attacks in a network.

Background

Network Tomography

- Motivation: if we can't see what's going on in a network directly, how to measure the network performance?



- 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:

  x_i : link performance (e.g., link delay)

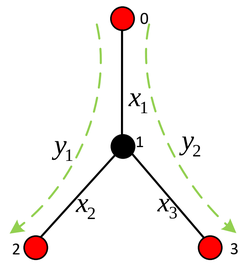
  y_i : path performance (e.g., path delay)

  linear system: $y_1 = x_1 + x_2$

  $y_2 = x_1 + x_3$

  matrix form: $\mathbf{y} = \mathbf{R}\mathbf{x}$ where $\mathbf{R} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$

  Given $\mathbf{y}$ and $\mathbf{R}$, network tomography wish to infer link metrics $\mathbf{x}$



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

Vulnerability and Attacks

Vulnerability

Network tomography relies on a *seeing-is-believing* assumption, i.e., measurements indeed reflect the real performance aggregates over individual links, i.e., y_i is true.

However, Such assumption does not always hold in the presence of malicious nodes.

Existing Attacks

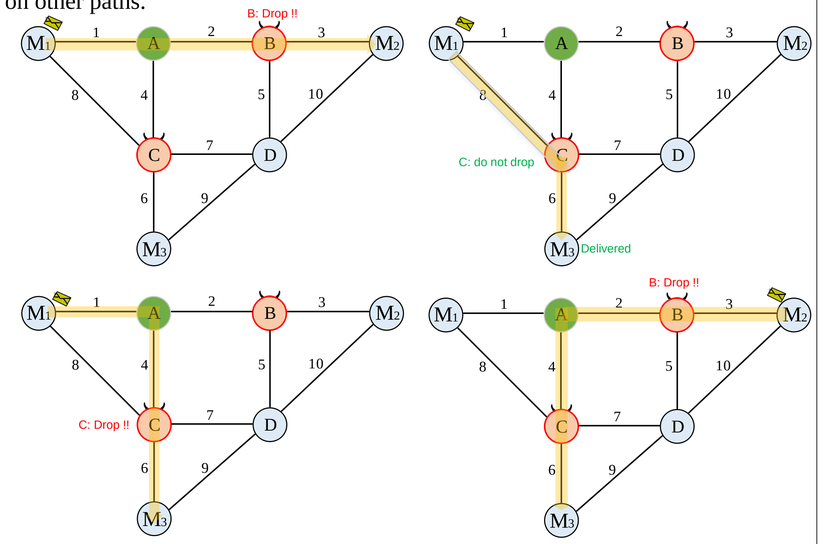
- Black hole attack: attackers drop all packets passing through it.
- Grey hole attack: attackers drop partial packets passing through them.

But they are very easy to be detected by network tomography!

Scapegoating Attack

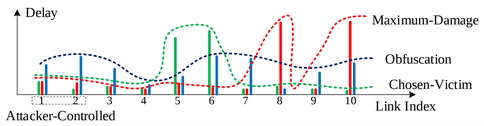
Idea: attackers cooperatively delay or drop packets to manipulate end-to-end measurements such that a legitimate node is incorrectly identified by network tomography as the root cause of the problem.

Methodology: attackers only damage paths which contain victims, and do nothing on other paths.



All packets going through A are blocked, and packets do not pass A are delivered. Therefore, A or link 1 must have problems. A is a scapegoat!

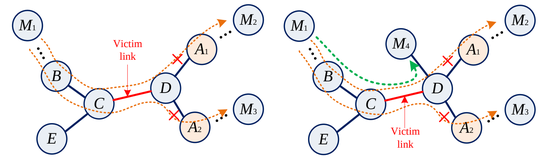
Attack strategies:



Detection and Locating

1. Detection

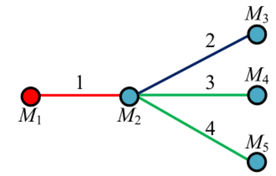
mechanism: $\text{scapegoating} = \begin{cases} \text{exists}, & \text{if } R\hat{x} \neq y', \\ \text{does not exist}, & \text{if } R\hat{x} = y'. \end{cases}$



(a) Perfect Cut — Not detectable

(b) Imperfect Cut — Detectable

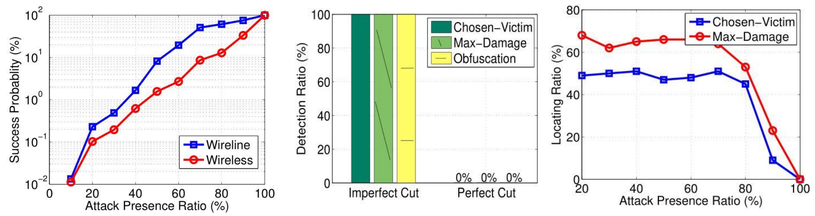
2. Locating



Link 1 is the only shared link among these 3 paths. So once attack is detected, the only explanation is that link 1 is malicious.

Experimental Results

Dataset: We use Rockfuel dataset for wireline network topology, and random geometric graph for wireless network topology.



Conclusion & Acknowledgment

(i) All three attack strategies are practical threats in network tomography scenarios.

(ii) We should not simply trust the measurements.

(iii) Existing network tomography methods in various applications need to be revisited to increase attack resilience.

(iv) This work at University of South Florida in this paper was supported in part by NSF CNS-1717969.