Vulnerability Analysis, Attack Strategies and Countermeasures Design in Network Tomography

Shangqing Zhao, Zhe Qu, Zhuo Lu, Cliff Wang

1Department 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.

Vulnerability

Network tomography relies on a seeing-is-believing assumption, i.e., measurements indeed reflect the real performance aggregates over individual links, i.e., \( y \) 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.

Detection and Locating

1. Detection
   - mechanism: scapegoating
   - exists, if \( R \mathbf{x} \neq \mathbf{y} \);
   - does not exist, if \( R \mathbf{x} = \mathbf{y} \).
   - 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.

2. Locating
   - path 1: \( M_1 \rightarrow M_i \)
   - path 2: \( M_i \rightarrow M_i \)
   - path 3: \( M_i \rightarrow M_i \)

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.

Experimental Results

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

(i) Attack Presence vs. (a) Perfect Cut (b) Imperfect Cut
(ii) ISPs vs. (a) Perfect Cut (b) Imperfect Cut
(iii) 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: