Vulnerability Analysis, Attack Strategies and Countermeasures Design in Network Tomography

Shangqing Zhao, Zhe Qu, Zhuo Lu,
University of South Florida, Tampa, FL 33620
Emails: {shangqing@mail., zhequ@mail., zhuolu@}usf.edu

Cliff Wang
North Carolina State University, Raleigh, NC 27695
Email: cliffwang@ncsu.edu

***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 introduce our past and current research results to 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. We note that this poster abstract and the poster are excerpted from our recent and on-going papers.**

I. Introduction

Accurate and timely monitoring of network performance is vital to ensure a reliable and efficient network environment. However, directly measuring the performance of internal components is not always feasible due to some reasons, such as the lack of support functionality at network components or prohibition in autonomous systems. To this end, network tomography provides an alternative measurement algorithm (e.g., [1]–[3]). Specifically, in network tomography, monitoring nodes (also known as monitors) send probe packets between each other. A network link's quality metric, such as delay or packet loss, is inferred from the end-to-end measurements based on the knowledge of how probe packets are routed over end-to-end paths between these monitors.

There is limited study that considers network tomography from the security perspective. In this proposed poster, we plan to introduce our recent and current research results of security vulnerabilities in network tomography [4], [5]. In particular, the reliability of network tomography relies on an implicit assumption that measurements over end-to-end paths indeed reflect the real performance aggregates over individual links. However, this assumption does not always hold since probe packets may go through malicious nodes that can intentionally or maliciously cause negative impacts on end-to-end measurements, thereby rendering a potential security vulnerability that may jeopardize the major objective of network monitoring.

We describe an attack strategy, called *scapegoating*, taking advantage of this vulnerability in network tomography. The basic idea of scapegoating is to intentionally delay or drop packets at malicious nodes to manipulate end-to-end measurements between monitors in a way such that a legitimate node is incorrectly identified by network tomography as the root cause of the problem, thereby becoming a scapegoat.

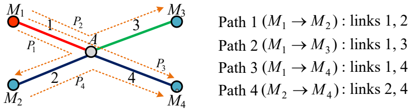
M_1
M_2
M_3
M_4
A
1
2
3
4
P_1
P_2
P_3
P_4
Path 1 ($M_1 \rightarrow M_2$) : links 1, 2
Path 2 ($M_1 \rightarrow M_3$) : links 1, 3
Path 3 ($M_1 \rightarrow M_4$) : links 1, 4
Path 4 ($M_2 \rightarrow M_4$) : links 2, 4

Fig. 1. Network example, where $M_1 - M_4$ are monitors, and M_1 is malicious.

In addition, we present three basic strategies to implement scapegoating attack, and demonstrate methods to detect and locate such attacks. We also use network datasets to perform simulation experiments to show the success possibility, damage, and the detectability and locatability of such attacks.

II. Attack, Detection and Localization

We first present the basic idea of scapegoating attack. Then we present three attack strategies to implement scapegoating. Finally, we introduce how to detect and locate such attack.

A. Basic Idea of Scapegoating

The basic idea of scapegoating is to damage the network and make a legitimate node scapegoat. To do so, instead of incurring damage on all paths, attackers only damage the path which contains the victim, and be cooperative (delay or drop no packets) on other paths. To demonstrate the idea of such an attack, we consider a naive scenario shown in Fig. 1, where nodes M_1, M_2, M_3 and M_4 are monitors, and M_1 is malicious. Let $\mathbf{x} = [x_1, x_2, x_3, x_4]^T$ and $\mathbf{y} = [y_1, y_2, y_3, y_4]^T$ be the link metric vector of links $l_1 - l_4$ and end-to-end path measurement vector of paths $P_1 - P_4$ respectively. Then we have the following linear system

$$\begin{aligned} P_1 : y_1 = x_1 + x_2, \quad P_2 :\ y_2 = x_1 + x_3, \\ P_3 : y_3 = x_1 + x_4, \quad P_4 :\ y_4 = x_2 + x_4. \end{aligned} \tag{1}$$

Now suppose an ideal case that the network is congestion free (i.e., almost 0ms delay on every link), and the attacker only damages path P_2 by inflicting extra 1000ms delay on link l_1 (i.e., $\mathbf{x} = [1000, 0, 0, 0]$). Then, we have the observed path measurement vector $\mathbf{y} = [0, 1000, 0, 0]^T$. The link metrics can be estimated from (1) as $\hat{\mathbf{x}} = [0, 0, 1000, 0]^T$. Thus, we know (i) the real attacker M_1 or its associated link l_1 can be successfully concealed by such an attack strategy against the network tomography; (ii) this misleads the network operator to believe that link l_3 or its end-node M_3 must have issues.

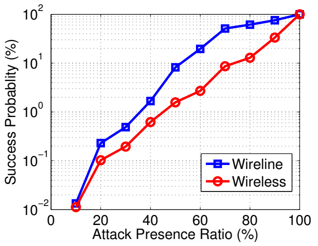

Fig. 3. The success probabilities of chosen-victim attacks.

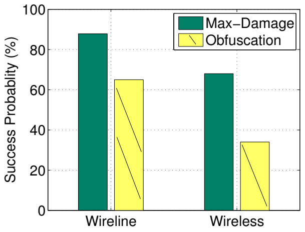

Fig. 4. The success probabilities of attack strategies 2 and 3.

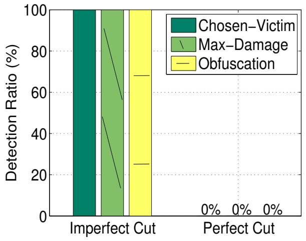

Fig. 5. The detection ratios of three different attackers.

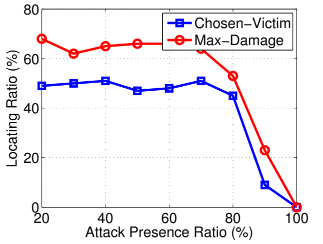

Fig. 6. The locating ratios for of attack strategies 1 and 2.

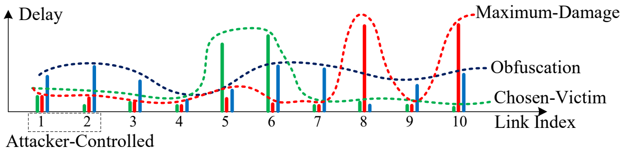

Fig. 2. Examples of three attack strategies.

B. Attack Strategy

Scapegoating aims to do the damage to the network, and at the same time hide the true malicious node or link set. We propose three different strategies to hide themselves and inflict the damage: 1) Chosen-victim scapegoating, in which attackers target one or more given victims in the network; 2) Maximum-damage scapegoating, in which attackers find a number of victims among all nodes to inflict the maximum damage to the network; 3) Obfuscation, by which network tomography is tricked to produce a substantial amount of link estimates beyond the normal status to confuse a network operator.

C. Detection and Localization

1) Detection: We then introduce a method to detect if scapegoating is launching in a network, i.e.,

$$\text{scapegoating} \begin{cases} \text{exists}, & \text{if } \mathbf{R}\hat{\mathbf{x}} \neq \mathbf{y}', \\ \text{does not exist}, & \text{if } \mathbf{R}\hat{\mathbf{x}} = \mathbf{y}', \end{cases} \tag{2}$$

where $\mathbf{R}$ and $\mathbf{y}'$ are the routing matrix and the measurements with attacks respectively. $\hat{\mathbf{x}}$ is the estimated value of $\mathbf{x}$.

2) Locatability: The key idea of scapegoating is that attackers only damage the paths that contain victim links and do nothing to other paths. Therefore, a malicious link used by attackers to cause damages should present on multiple paths, i.e., some of them contain victim links and others do not. However, if the link controlled by a attacker is the only shared link in a network, then the only explanation for the inconsistency in (2) is that this shared link is malicious, because it is the only link that can really inflict the traffic differentiation among different paths.

III. Experimental Evaluation

We conduct our experiments based on the Rocketfuel datasets [6] and random geometric graph for wireline and wireless network topologies respectively.

1) Attack Evaluation: We first evaluate the success probabilities of three attack strategies in both wireline and wireless topologies. Fig. 3 depicts the success probabilities of chosen-victim scapegoating over different attack presence ratios, defined as the ratio of the number of measurement paths including at least one victim and at least one attacker over the number of total measurement paths including any victim. We see that from both types of networks, the success probability increases as the attack presence ratio increases. Fig. 4 shows the success probabilities of maximum-damage and obfuscation attacks. It is noted from Fig. 4 that even one single attacker is likely to succeed, verifying that scapegoating is feasible in both networks.

2) Detectability and Locatability Evaluation: Fig. 5 shows the detection ratios over all three scapegoating attacks in the perfect cut and imperfect cut cases, where perfect cut case means for any measurement path containing a victim link, there always exists a malicious node present on that path, and imperfect cut case denotes for at least one path containing a victim link, there is no malicious one present on that path. From Fig. 5, the detection ratio in the presence of all three attacks is 100% when attackers can perfectly cut victim links, and 0% otherwise. Fig. 6 shows the relationship between the locating performance. We can see, when the attack presence ratio reaches 90%, the locating ratio decreases sharply, since almost all links are controlled by attackers, and the numbers of normal links and victim links decrease dramatically, which are necessary to locate attack links.

Acknowledgement: The work at USF was supported in part by NSF CNS-1717969.

References

[1] A. Krishnamurthy and A. Singh, "Robust multi-source network tomography using selective probes," in *Proc. of IEEE INFOCOM*, 2012.

[2] T. He, L. Ma, A. Gkelias, K. K. Leung, A. Swami, and D. Towsley, "Robust monitor placement for network tomography in dynamic networks," in *Proc. of IEEE INFOCOM*, 2016.

[3] L. Ma, T. He, K. K. Leung, A. Swami, and D. Towsley, "Monitor placement for maximal identifiability in network tomography," in *Proc. of IEEE INFOCOM*, 2014.

[4] S. Zhao, Z. Lu, and C. Wang, "When seeing isn't believing: On feasibility and detectability of scapegoating in network tomography," in *Proc. of IEEE ICDCS*, May, 2017.

[5] ——, "Measurement integrity in network tomography: Measurement integrity attacks against network tomography: Feasibility and defense," in *Submitted for Publication*, 2018.

[6] "Rocketfuel," www.cs.washington.edu/research/networking/rocketfuel/.