POSTER: Packet Conductance for Statistical Intrusion Detection in Anonymous Networks

Arjun P. Athreya (Student), Yu Seung Kim (Student), Xiao Wang (Student), Yuan Tian (Student)
and Patrick Tague (Faculty)
Carnegie Mellon University, USA

***Abstract*—Intrusion detection systems have been widely studied for various types of networks and applications. In applications where end-hosts of a network seek anonymity, the communication between such hosts behind secured gateways are supported by a heterogeneous, mixed wired/wireless network core. The secured gateway fully encrypts and anonymizes all data packets sent through the network core. While attacks on data itself is possible via crypt-analysis, real-time intrusion detection by studying packet header information is not possible as these packets are fully encrypted. In this paper we propose a distributed intrusion detection system for such anonymized networks. Our system monitors the behavior of the network bandwidth consumption in real-time and uses a statistical inference system to classify anomalies in bandwidth consumption of the network.**

I. Introduction

Intrusion detection system (IDS) aims to protect information systems and networks from intruders. The seminal work of intrusion detection relied on audits and forensics on logs and other available labeled data to the detectors [1]. Typically, intrusion detection systems model the operating environment to understand the normal behavior (absence of intruders or attacks) and then look to monitor the same system for deviation from the normal behavior to detect and classify the attacks or intrusion's severity. Intrusion detection can be host based or network based. Host based IDS looks at logs made by the host for the specified set of operations and looks for rule violations. Network based IDS monitors network parameters and meta-data of network packets (IP addresses, packet sequence numbers, packet sizes) and then looks for their anomalies behavior to raise intrusion alarms [2].

For numerous reasons such as confidentiality, political restraint evasion or sensitive communications, anonymity is desired. While data anonymity is used to protect the identity of creator of the data, network anonymity protects against traceability of end-hosts of networks even though their data traverses through the network in the presence of adversaries. Thus in a fully anonymized network using services such as The Onion Router (TOR) [3], all the packet's contents and the packet's meta data are fully protected by cryptographic techniques. This makes the very input to the traditional network IDS unavailable to raise intrusion alarms. Additionally, real-time IDS for anonymous networks is challenging because cryptanalysis of anonymized data packets needs time in the absence of not knowing the cryptographic keying information. Hence, developing real-time intrusion systems is a hard problem and to our best knowledge remains unsolved.

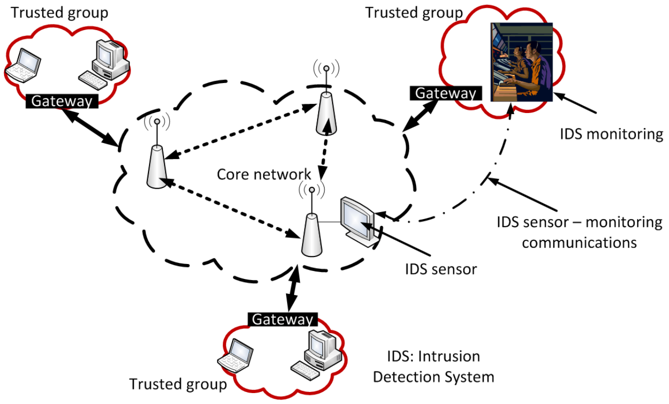

Fig. 1: This figure shows the anonymous communication core network supporting communications between end-hosts seeking anonymity based in trusted enclaves. The intrusion detection sensors in the core report to intrusion monitoring centers in the trusted groups.

In this paper we propose an IDS for anonymized networks using observable network statistics. In particular, our focus is on the military communications networks shown in Figure 1. These networks involve end-hosts of different secure conclaves trying to communicate with each other using the network core. The network core in this work is a wireless network consisting of wireless routers which could support multiple wireless local area networks (WLAN) in the context of wireless mesh networks or ad hoc networks. Considering the sensitive nature of communications, the data packets are fully encrypted before being sent to the core network to achieve anonymity. We assume that attackers (intruders) will not always be successful in obtaining any meaningful information from breaking the security offered by cyptographic techniques used to protect the packets. However attackers can launch attacks that affects the bandwidth of target WLAN without needing to modify packet contents, thereby leading to Denial of Service (DoS) in the core network. Attackers could be distributed in the network and thus a distributed DoS (D-DoS) attack can be launched in the core network. Thus we detect the presence of intruders and the attack by monitoring the network bandwidth consumption for anomalous behavior. The presence of intruders in the core is reported to the intrusion monitoring center in the trusted groups. This allows for the trusted groups to identify sections of the core under attack. We discuss our proposed detection framework for anonymous networks in the following section.

II. Statistical Intrusion Detection Framework

We first propose a metric for capturing anomalies in network bandwidth in anonymous networks. Then we describe our intrusion detection model using the proposed metric. Finally we discuss the challenges in using aggregate statistics to make decisions on intrusion detection in anonymous networks.

A. Packet Conductance

In device Physics, *conductance* of a conductor is defined as the ease with which electric current passes through it. In our work we define *packet conductance* as the ease with which incoming forwarding traffic leaves the router, which is a ratio of outgoing data rate (packets per unit time) over the incoming data rate at a router. This metric will help us understand the dynamics of channel's bandwidth behavior on the incoming links and the outgoing links at a wireless router.

For normal operations, this metric should ideally be equal to 1.0. This means that accounting for queuing and other delays, the net incoming and outgoing rates must be equal. However, when attackers target a link to reduce its traffic transportation capacity, this metric will indicate the presence of an attack on the bandwidth because the value of the metric will be lesser than 1.0. Apart from the fact that the metric indicates the presence of bandwidth related attacks, it has many advantages for anonymous networks IDS design. Firstly, this metric is non-invasive. Packets need not be inspected at all for any flow related information because we are purely looking at aggregated bandwidth measurement at each interface. Secondly, as no inspection is needed, metric's performance can be captured in real-time. Finally, the metric captures all the links that get affected because of certain subset of links being affected in a WLAN. This is because, the WLAN bandwidth is shared and thereby if the attacker consumes the common resource, the metric on all affected nodes will indicate the attack's presence.

B. Attacker and Intrusion Detection Model

In this work we focus on bandwidth flooding attacks. In particular we assume that the attackers will flood the core network. We study two instances of attacks which will result in a DoS in the affected WLAN. First instance of the attack is when the attackers flood a link or a router of the WLAN at a data rate higher than mandated by the wireless standard supported in the WLAN. Thus the router receiving this traffic will not be able to forward the traffic at the same rate which will be reflected by drops in the packet conductance metric. Another instance of the attack results from medium access misbehavior which results in bandwidth exhaustion of the WLAN. Thus the packet conductance metric on all the affected routers and clients in a WLAN will indicate the presence of this attack due to drops in the metric's performance.

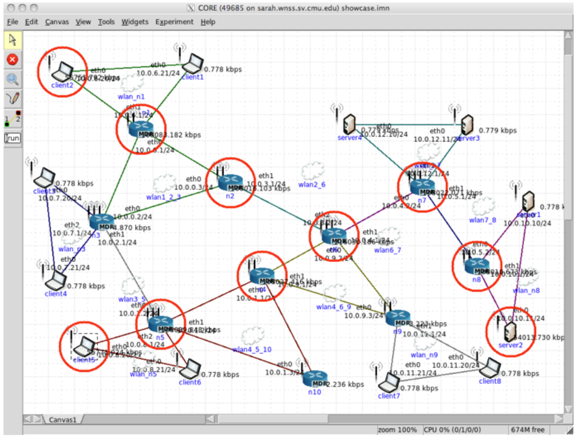

Fig. 2: This figure shows the simulation setup of the core network which implements our detection model using packet conductance metric. The red circles in the figure indicate the routers detecting intrusion in the core network.

Our detection framework involves with each router being trained initially by monitoring our metric's performance for normal operations. Then, with moving window of time, each router compares the performance of the metric in the respective time window with historic performance of the metric. Anomalous behavior of the metric in the current window of observation is captured by thresholds network managers can set based on historic performance of the metric and knowledge of attack's presence. This could also depend on sensitivity needs of the IDS alarms to changes in network behavior. Finally each of these routers report any anomaly to the intrusion monitoring center in the secret enclaves. We allow for routers to make decisions on intrusion detection by cooperating with other routers in the WLAN.

C. Challenges with Aggregate Statistics

The intrusion detection metrics such as *packet conductance* while being non-invasive also pose challenges in IDS design for anonymous networks. Particularly for wireless networks, aggregated statistics are even more challenging to model. Bandwidth consumption is not constant in wireless networks even when there are no attacks. The stochastic nature of the wireless channel imposes stochasticity in the metric's performance with time. The stochastic nature of wireless channels could result from factors such as changes in propagation environment, mobility and different propagation models. Hence, the variance of metrics about its mean will not be small as could be seen in wired networks which can capture certain instances of flooding attacks with relatively good accuracy [4]. This leads to the fact that false alarms could be raised by IDS in anonymous networks which rely on raw aggregated statistics for intrusion detection. We have implemented our IDS which considers these challenges using a simulation setup, the screenshot of the same is shown in Figure 2.

References

[1] D. Denning, "An intrusion-detection model," *IEEE Transactions on Software Engineering,*, vol. 13, no. 2, pp. 222–232, 1987.

[2] S. Northcutt, "Network intrusion detection: An analyst's hand-book," *EDPACS*, vol. 27, pp. 1–2, 2000.

[3] R. Dingledine, N. Mathewson, and P. Syverson, "TOR: The second-generation onion router," DTIC Document, Tech. Rep., 2004.

[4] A. Studer and A. Perrig, "The coremelt attack," in *Proceedings of the 14th European conference on Research in computer security*, 2009, pp. 37–52.