Chapter 8
Enhancing Intrusion Detection Systems Using Intelligent False Alarm Filter:
Selecting the Best Machine Learning Algorithm

Yuxin Meng
City University of Hong Kong, China

Lam-For Kwok
City University of Hong Kong, China

ABSTRACT

Intrusion Detection Systems (IDSs) have been widely implemented in various network environments as an essential component for current Information and Communications Technologies (ICT). However, false alarms are a big problem for these systems, in which a large number of IDS alarms, especially false positives, could be generated during their detection. This issue greatly decreases the effectiveness and the efficiency of an IDS and heavily increases the burden on analyzing real alarms. To mitigate this problem, in this chapter, the authors identify and analyze the reasons for causing this problem, present a survey through reviewing some related work in the aspect of false alarm reduction, and introduce a promising solution of constructing an intelligent false alarm filter to refine false alarms for an IDS.

DOI: 10.4018/978-1-4666-4514-1.ch008

1. INTRODUCTION

Intrusion detection is a process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems (Bace, 2000) and this concept is evolved from audit. To conduct the process of intrusion detection, *Intrusion Detection Systems* (IDSs) have been developed with the purpose of automatically detecting intrusions (e.g., Malware, Virus, Trojan) by monitoring local systems or network events.

Traditionally, there are two major types of intrusion detection systems: *Host-based IDS* (HIDS) and *Network-based IDS* (NIDS). A host-based IDS mainly monitors the events which occurred in a local computer system, and then reports its findings. On the other hand, a network-based IDS aims to monitor network traffic and detect network attacks through analyzing incoming network packets. HIDS and NIDS can be regarded as two aspects of an intrusion detection process. In real deployment, a security administrator usually implements both of them with the purpose of providing a more comprehensive protection in a network environment or in a computer system.

Nowadays, IDSs are being widely deployed in various business environments (e.g., bank, insurance company) to protect network security. In general, the specific detection approaches can be classified into three folders: *signature-based IDS*, *anomaly-based IDS* and *hybrid IDS*. A signature-based IDS (or called *misuse-based IDS*) (Roesch, 1999) detects an attack by comparing its signatures with current network events (e.g., network packets). A signature (or called *rule*) is a kind of descriptions to describe a known attack or exploit. An anomaly-based IDS (Paxson, 1999) identifies anomalies by means of pre-established *normal profile*. Note that anomalies are patterns in data that do not conform to a well defined notion of normal behavior and a normal profile is used to describe a normal event (e.g., a normal network connection). A hybrid IDS (Ali, Halim, & G¨okhan, 2009) is capable of conducting both signature-based detection and anomaly-based detection. Through combining these two detection approaches, a hybrid IDS is expected to provide much more information about network traffic and identify network attacks more powerfully.

However, a false alarm is a very challenging problem in information and communications technologies (ICT) (i.e., designing any secure and practical protocols, deploying and setting a network, evaluating any network architectures or systems), and especially a key limiting factor for an intrusion detection system (Axelsson, 2000). In real-world applications, a large number of false alarms could be generated by these IDSs during the detection (McHugh, 2000), which can greatly reduce the effectiveness of an IDS and heavily increase the burden of identifying true alarms and analyzing helpful information. In particular, we identify that this problem stems primarily from three reasons as below:

- **Protocol Issues:** In a network, some protocols and packets (e.g., UDP) can be easily spoofed and modified, which provide a chance for attackers to bypass the examination of an IDS, or mislead the analysis work.
- **Network Architecture Issues:** There is a lack of contextual information about their protected network environment for current IDSs.
- **Inherent Challenging Issues in an IDS:** Both a signature-based IDS and an anomaly-based IDS are suffering from inherent limitations (i.e., it is hard to accurately identify an attack).

To mitigate the problem of false alarms, in this chapter, we introduce a promising method of using intelligent false alarm filter, by adaptively selecting an appropriate machine learning algorithm, to filter out IDS false alarms and