Chapter 54
Feature Extraction Methods for Intrusion Detection Systems

Hai Thanh Nguyen
Gjøvik University College, Norway

Katrin Franke
Gjøvik University College, Norway

Slobodan Petrović
Gjøvik University College, Norway

ABSTRACT

Intrusion Detection Systems (IDSs) have become an important security tool for managing risk and an indispensable part of overall security architecture. An IDS is considered as a pattern recognition system, in which feature extraction is an important pre-processing step. The feature extraction process consists of feature construction and feature selection. The quality of the feature construction and feature selection algorithms is one of the most important factors that affects the effectiveness of an IDS. Achieving reduction of the number of relevant traffic features without negative effect on classification accuracy is a goal that largely improves the overall effectiveness of the IDS. Most of the feature construction as well as feature selection works in intrusion detection practice is still carried through manually by utilizing domain knowledge. For automatic feature construction and feature selection, the filter, wrapper, and embedded methods from machine learning are frequently applied. This chapter provides an overview of various existing feature construction and feature selection methods for intrusion detection systems. A comparison between those feature selection methods is performed in the experimental part.

INTRODUCTION

Intrusion Detection Systems (IDSs) have become an important security tool for managing risk and an indispensable part of overall security architecture (Northcutt, 1999). An Intrusion detection system gathers and analyzes information from various sources within computers and networks to identify suspicious activities that attempt to illegally access, manipulate, and disable computer systems. The two main intrusion detection approaches are misuse detection and anomaly detection (Denning, 1986). Misuse detection systems, for instance, Snort (Roesch, 1999), detect intrusions by look-

DOI: 10.4018/978-1-4666-3994-2.ch054

ing at specific signatures of known attacks. This approach is similar to the way of detecting viruses in many antivirus applications. A set of patterns of known attacks is necessary be built in advance for further detections. It is easy to implement misuse detection systems. However, these systems are not effective against novel attacks that have no matched patterns yet. Anomaly detection systems, such as IDES (Lunt et al., 1992), can overcome the shortcoming of the misuse detection systems. An anomaly detector assumes that normal behaviors are different from abnormal behaviors. Therefore, abnormal activities can be detected by looking at normal activities only. In fact, in these system, a profile of normal behavior is set up and is utilized to flag any observed activities that deviate significantly from the established profile as anomalies or possible intrusions. Although anomaly detection systems have potentials of detecting novel attacks, it is not easy to define normal behaviors and these systems tend to generate more false positive alerts than the misuse detection systems.

An approach for building anomaly intrusion detection systems is to utilize machine learning and statistical techniques. By means of this approach, an intrusion detection system is considered as a statistical pattern recognition system. Figure 1 shows the model of a statistical pattern recognition system that consists of two phases: training and classification. The test and training patterns as raw data are normalized, noise as well as unwanted data is removed by the preprocessing modules. In the training phase, the feature extraction/selection module looks for a representative feature set from the input patterns. Those features are then utilized for training a classifier. In the classification phase, the trained classifier is applied to assign the test patters to one of the pattern classes under consideration of the selected features from the training phase. In the following, we will focus on this approach for intrusion detection.

From Figure 1, it can be observed that feature extraction is an important part of a pattern recognition system. The feature extraction process consists of feature construction and feature selection. The quality of the feature construction and feature selection algorithms is one of the most important factors that influence the effectiveness of an IDS. Achieving reduction of the number of relevant traffic features without negative impact on classification accuracy is a goal that largely improves the overall effectiveness of the IDS. Most of the feature construction as well as feature selection works in intrusion detection practice is still carried out through manually utilizing domain knowledge. For automatic feature construction and feature selection, the filter, wrapper and embedded methods from machine learning are frequently applied. This chapter provides an overview of various existing feature construction and feature selection methods for intrusion detection systems.

Figure 1. Model of a statistical pattern recognition (Jain et al., 2000)