A New Unsupervised Anomaly Detection Framework for Detecting Network Attacks in Real-Time

Wei Lu and Issa Traore

Department of Electrical and Computer Engineering, University of Victoria,
PO Box 3055 STN CSC, Victoria, B.C., Canada
{wlu, itraore}@ece.uvic.ca

Abstract. In this paper, we propose a new unsupervised anomaly detection framework for detecting network intrusions online. The framework consists of new anomalousness metrics named IP Weight and an outlier detection algorithm based on Gaussian mixture model (GMM). IP Weights convert the features of IP packets into a four-dimensional numerical feature space, in which the outlier detection takes place. Intrusion decisions are made based on the outcome of outlier detections. Two sets of experiments are conducted to evaluate our framework. In the first experiment, we conduct an offline evaluation based on the 1998 DARPA intrusion detection dataset, which detects 16 types of attacks out of a total of 19 network attack types. In the second experiment, an online evaluation is performed in a live networking environment. The evaluation result not only confirms the detection effectiveness with DARPA dataset, but also shows a strong runtime efficiency, with response times falling within seconds.

1 Introduction

Intrusion detection has been extensively studied since the seminal report written by Anderson [1]. Traditionally, intrusion detection techniques are classified into two categories: misuse detection and anomaly detection. Misuse detection is based on the assumption that most attacks leave a set of signatures in the stream of network packets or in audit trails, and thus attacks are detectable if these signatures can be identified by analyzing the audit trails or network traffic behaviors. However, misuse detection approaches are strictly limited to the latest known attacks. How to detect new attacks or variants of known attacks is one of the biggest challenges faced by misuse detection.

To address the weakness of misuse detection, the concept of anomaly detection was formalized in the seminal report of Denning [4]. Denning assumed that security violations could be detected by inspecting abnormal system usage patterns from the audit data. As a result, most anomaly detection techniques attempt to establish normal activity profiles by computing various metrics, and an intrusion is detected when the actual system behavior deviates from the normal profiles. According to Axelsson, "the early anomaly detection systems were

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 96–109, 2005.

self-learning, that is, they automatically formed an opinion of what the subject's normal behavior was" [2]. Self-learning techniques combine the early statistical model based anomaly detection approaches [10][12][17], and the AI based approaches [8] or the biological models based approaches [9], and thus they are still applied for current anomaly detection schemes. According to whether they are based on supervised or unsupervised learning techniques, anomaly detection schemes can be classified into two categories: unsupervised anomaly detection and supervised anomaly detection [14].

Supervised anomaly detection establishes the normal profiles of systems or networks through training based on labeled datasets. In contrast, unsupervised anomaly detection attempts to detect intrusions without using any prior knowledge of attacks or normal instances. The main drawback of supervised anomaly detection is the need of labeling the training data, which makes the process error-prone, costly and time consuming. Unsupervised anomaly detection addresses these issues by allowing training based on unlabelled datasets and thus facilitating online learning and improving detection accuracy.

Clustering algorithm is one of the most widely used unsupervised learning techniques. Some examples of using clustering algorithms for intrusion detection were suggested in literature [5], [6] and [14]. Although clustering techniques have showed their capability for intrusion detection, labeling clusters is still a difficult problem faced by this kind of approach. In order to label the clusters, the approach usually makes two assumptions: (1) data instances always belong to two categories: normal clusters and intrusive clusters; (2) the number of normal data instances largely outnumbers the number of intrusions. However, these assumptions are not always the case in practice. The number of clusters is not supposed to be determined in advance. When data instances include only normal behavioral data, the assumptions will lead a high false alert rate. In order to obtain an efficient and effective detection, we propose in this paper a new unsupervised anomaly detection framework based on outlier detection techniques. The proposed detection scheme consists of a feature extraction technique based on new anomalousness metrics, named IP Weight and an outlier detection algorithm based on Gaussian mixture model (GMM).

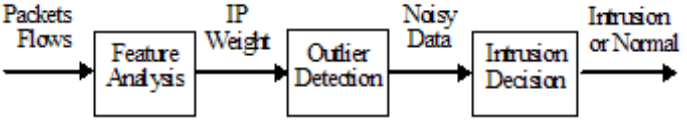

Fig. 1. General architecture

Fig. 1 illustrates the general architecture of our framework, which consists of three components, namely feature analysis, outlier detection and intrusion decision. During feature analysis, IP Weights are generated from standard IP packet flows. This allows extracting salient and useful domain knowledge and reducing significantly the dimensionality of the feature space. Then, noisy data