Chapter 9
Visualization Technique for Intrusion Detection

Mohamed Cheikh
Constantine 2 University, Algeria

Salima Hacini
Constantine 2 University, Algeria

Zizette Boufaida
Constantine 2 University, Algeria

ABSTRACT

Intrusion detection system (IDS) plays a vital and crucial role in a computer security. However, they suffer from a number of problems such as low detection of DoS (denial-of-service)/DDoS (distributed denial-of-service) attacks with a high rate of false alarms. In this chapter, a new technique for detecting DoS attacks is proposed; it detects DOS attacks using a set of classifiers and visualizes them in real time. This technique is based on the collection of network parameter values (data packets), which are automatically represented by simple geometric graphs in order to highlight relevant elements. Two implementations for this technique are performed. The first is based on the Euclidian distance while the second is based on KNN algorithm. The effectiveness of the proposed technique has been proven through a simulation of network traffic drawn from the 10% KDD and a comparison with other classification techniques for intrusion detection.

INTRODUCTION

Intrusion Detection Systems (IDSs) were introduced by Anderson (Anderson.J,1980). Denning (Denning.D,1987) designed then an intrusion detection model which marked a real impetus of the field. IDSs are essential complements to the preventive security mechanisms provided for computing systems and networks. They are used in the monitoring control process for the detection of potential intrusions and infections (Zanero, 2004).

DOI: 10.4018/978-1-7998-5348-0.ch009

IDS is based on two basic approaches, the behavioral approach and the scenario approach. The scenario approach, often called misuse detection approach defines the user actions that constitute abuse. It uses rules defined to encode and detect known intrusions. The behavioral approach, on its side, can detect unknown intrusions, and does not require any prior knowledge of intrusions (Boudaoud.K,2000). This approach is based on the fact that an intruder does not behave the same way as a regular user. Contrary to the user, who has a normal behavior, the intruder has an abnormal behavior. Thus, all intrusive activities are necessarily abnormal (Sundaram.A,2000).

Classification techniques in IDS intended to classify network traffic into two classes: "normal" and "intrusion". Classification requires learning. The accuracy of this learning provides lower false positive rate and false negative rate (Maxime DUMAS,2011).

Among the techniques commonly used for classification in IDS, we find the ANN, SVM and often the K-means and others (see section 2).

This chapter presents a new technique for classifying DoS attacks based on a visual representation of the network traffic. This representation is based on simple geometric forms and has two objectives:

1. Find models of DoS attacks and in particular be able to distinguish between them and the normal traffic. These models are later used in the classifiers. Seven models were identified to recognize six types of DoS attacks (Neptune, Smurf, Teardrop, Land, Pack, Pod) to which is added the normal case.
2. Improve the detection rate, which presents a great challenge for IDS.

The effectiveness of this technique has been proved through simulation of network traffic drawn from the 10% KDD. The proposed technique treats DoS attacks. However, it can also be applied to other types of attacks with the integration of their geometric forms in the detection system.

The remaining of this chapter is organized as follows: Section 2 presents some works dealing with the classification in IDS, Section 3 describes the proposed detection technique. Finally, Section 4 concludes the chapter and suggests some perspectives.

RELATED WORK

There are several techniques used for classification in IDS, the most frequently are ANN, SVM and K-means as well as others.

The k-means classifier, originally an algorithm for pattern recognition that has proven its effectiveness against the text processing (Yang Y,1997) represents a simple and popular classification that uses statistics properties (Kaplantzis.S & N. Mani,2006). It allows the partition of a collection of objects into K classes (K is a number set by the user). In the context of intrusion detection, there are generally two groups (classes), one for attack and another for normal cases. The classification is then performed by taking each individual point in a test set and associating it with the nearest class. At the end, each point is assigned to a class "attack" or "normal." Most distance measures used in this category of classification algorithms are Euclidean and Manhattan distances.

Neural networks are also used for ANN classification in IDS (Kevin L et al,1990), (Herve Debar et al,1992), (Jake Ryan et al,1998), (James Cannady,1998), (B. Subba, 2016). In the work of Fox et al. (Kevin L et al,1990), the authors propose the use of artificial neural networks to detect intrusions. The