ABSTRACT

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. In this paper, 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 form in order to highlight relevant elements. The effectiveness of the proposed technique has been proven through a MATLAB simulation of network traffic drawn from the 10% KDD, and a comparison with other classification techniques for intrusion detection.

Keywords: Classification Technique, Denial of Service (DoS) Attack, Intrusion Detection System (IDS), KDD, Network Security

DOI: 10.4018/IJISP.2014040102
**INTRODUCTION**

IDSs are tools for monitoring and controlling performance used for auditing information systems and detecting possible intrusions (Anderson, J, 1980; Denning, D, 1987).

Intrusion detection 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 intends 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 (Artificial Neural Network), SVM (Support Vector Machines) and often the K-means and others (see section 2).

This paper presents a new technique for classifying DoS attacks relying 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. 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 MATLAB 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 paper is organized as follows: Section 2 presents some works dealing with the classification in IDS, Section 3 describes the proposed detection technique. Section 4 adds an experimentation and discussion to this work. Finally, Section 5 concludes the paper 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
Related Content

Risks and Impacts of Children's Engagement in Solid Waste Management Activities in Hawassa City, Ethiopia

Optimizing Privacy-Accuracy Tradeoff for Privacy Preserving Distance-Based Classification
[www.igi-global.com/article/optimizing-privacy-accuracy-tradeoff-privacy/68819?camid=4v1a](www.igi-global.com/article/optimizing-privacy-accuracy-tradeoff-privacy/68819?camid=4v1a)
A Survey of Key Management in Mobile Ad Hoc Networks
[www.igi-global.com/chapter/survey-key-management-mobile-hoc/22065?camid=4v1a](www.igi-global.com/chapter/survey-key-management-mobile-hoc/22065?camid=4v1a)

Mobile Communities and the "Generation that Beeps and Hums"
[www.igi-global.com/chapter/mobile-communities-generation-beeps-hums/23349?camid=4v1a](www.igi-global.com/chapter/mobile-communities-generation-beeps-hums/23349?camid=4v1a)