ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

https://doi.org/10.17559/TV-20210604113859
Original scientific paper

Dynamic Defense Mechanism for DoS Attacks in Wireless Environments Using Hybrid Intrusion Detection System and Statistical Approaches

Magudeeswaran PREMKUMAR*, Tharai Vinay Param SUNDARARAJAN, Gopalakrishnan MOHANBABU

Abstract: Security in wireless frameworks is a significant and difficult task because of the open environment. The Denial of Service (DoS) is as yet significant endeavour to make an online assistance inaccessible. The objective of this attack is to keep the authentic nodes from getting to the administrations. Intrusion detection systems assume an essential job in identifying DoS attacks that improve the performance of the system. However massive information from the system presents huge difficulties to the discovery of DoS attack, as the identification framework needs adaptable techniques for gathering, storing and processing a lot of information. In order to defeat these difficulties, this paper proposes Hybrid Intrusion Detection System (HIDS) framework dependent on different MLP strategies. In this article HIDS utilizes Naive Bayes (NB), irregular random forest (RF), decision tree (DT), multilayer perceptron (MLP), K-nearest neighbours (K-NN) and support vector machine (SVM) for better outcomes. The NSL-KDD dataset and UNSW-NB15 dataset are taken to examine the detection accuracy. The experiment results show that the proposed defence system is accomplished with high accuracy, high detection rate and low false alarm rate in both the datasets.

Keywords: denial-of-services; DoS defense; hybrid mechanism; intrusion detection; machine learning; wireless sensor networks

1 INTRODUCTION

The wireless sensor networks (WSNs) are comprised of several tiny sensors networked with low- yield wireless environments. Wireless sensor networks are used in many devices for healthcare tracking, habitat monitoring, military applications, battlefield monitoring, smart grid and so on. These networks are endowed with sensing, data pre processing and communication modules. In this thousands of sensors were composed with a network Id which is rapidly deployed to collect the critical information from hostile and unattended circumstances. A node is comprised of four components: one sensing unit, one transceiver, one processer and one battery. The first component is comprised of optical converters and sensors. The phenomenon detected by sensing system is transformed by A to D converters into full digital signals. The processing circuit is followed by a small storage unit and the sensor node communicates with the other nodes. The transceiver system acts as a connection between the node and the network. Li, Ni MH batteries or power-saving devices such as solar powered systems use an electrical unit. The main constraint of the network is the node having limited energy resources, minimal processing memory, safety risks, and the least communication and processing capacity. In a device, DOS attacks are propelled by remotely controlled, powerful, and narrowly disseminated botnet PCs of zombies. Many of the traffics or administration demands are at the same time or persistently sent to the objective framework. The objective framework gets unusable, reacts gradually, or crashes totally because of the attack [7].

The distinguishing proof of the first aggressors is hard for the protection strategies on the grounds that the aggressors have caricature IP addresses and secured inside zombies with the intention of heavily influenced by them [5].

The DoS attack detection based on the KNN classifier is shown in Fig. 1. The KNN algorithm is based on the iterative relocation of a dataset separated into k clusters. The average square distance between cluster centres and data points is reduced.

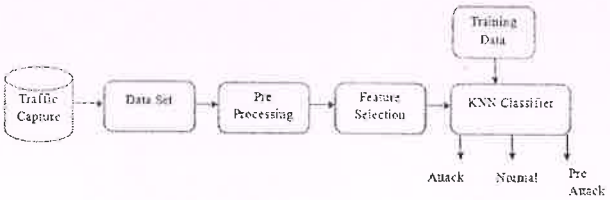

Figure 1 DoS attack detection based on KNN classifier

Before the last attacks are dispatched, the DoS attacks are manual and must perform a few steps, including identification of traded off devices to create zombies on the internet, port filtering, and sending malware. Parameters unique to the target can also be organised by the perpetrators, while the others can be tracked using mechanised instruments [12]. The FC resembles the attacks as far as numerous clients access a framework simultaneously. In FC there is an unusual and abrupt ascent in real rush hour gridlock as a result of extraordinary occasions. It is hard for guarded frameworks to recognize FC unusual traffic from DoS attacks. Some entrenched audit and reviews on DoS attacks and safeguard strategies are accessible in the writing, including [12]. The survey researches the guard techniques that are sent for distinguishing, alleviating, as well as forestalling DoS attacks. It orders DoS safeguard strategies as indicated by the class of defencelessness, the level of mechanization, effect, and elements. In addition, this survey incorporates typical testing sets and assessment strategies. The aim of this survey is to expand the scope and shape the course of DoS study. It leads to some open research issues and gives a few thoughts for future research.

2 RELATED WORKS

In the last few years, several detection and mitigation mechanisms have been recorded for DoS attacks aimed at service providers [16]. For DoS attack detection, many methods have been suggested so far. Some of the latest work in DoS attack detection is summarized in this section.

Song and Liu [10] are proposing an authentic detection method that employs dynamic K-Nearest Neighbours (K-