Chapter 8
Hybridization of Machine Learning Algorithm in Intrusion Detection System

Amudha P.
Avinashilingam Institute for Home Science and Higher Education for Women, India

Sivakumari S.
Avinashilingam Institute for Home Science and Higher Education for Women, India

ABSTRACT

In recent years, the field of machine learning grows very fast both on the development of techniques and its application in intrusion detection. The computational complexity of the machine learning algorithms increases rapidly as the number of features in the datasets increases. By choosing the significant features, the number of features in the dataset can be reduced, which is critical to progress the classification accuracy and speed of algorithms. Also, achieving high accuracy and detection rate and lowering false alarm rates are the major challenges in designing an intrusion detection system. The major motivation of this work is to address these issues by hybridizing machine learning and swarm intelligence algorithms for enhancing the performance of intrusion detection system. It also emphasizes applying principal component analysis as feature selection technique on intrusion detection dataset for identifying the most suitable feature subsets which may provide high-quality results in a fast and efficient manner.

INTRODUCTION

Network security has become a vital aspect of computer technology as there is great improvement in usage of internet. There is a tremendous growth in the field of information technology due to which, network security is also facing significant challenges. As traditional intrusion prevention techniques have failed to protect the computer systems from various attacks and intruders, the concept of Intrusion Detection System (IDS) proposed by Denning (1987) has become an essential component of security infrastructure for the networks connected to the internet and is useful to detect, identify and track the intruders.

DOI: 10.4018/978-1-5225-9611-0.ch008

Intrusion Detection System

An Intrusion Detection System (IDS) is a software application that continuously perceives computer network looking for malicious actions or strategy defilements and generates reports. According to recent studies, an average of twenty to forty new vulnerabilities in commonly used networking and computer products are discovered every month. These wide-ranging vulnerabilities in software enlarge or increase today's insecure computing/networking environment. Hence, such insecure environment has paved way to the ever evolving field of intrusion detection and prevention. The cyberspace's equivalent to the burglar alarm, intrusion detection systems complement the beleaguered firewall.

Intrusion Detection System is a security mechanism which has been acknowledged by the researchers from all over the world because of their capability to keep track of the network behaviour, so that abnormal behaviour can be detected quickly. The traditional IDS is unable to handle the recent attacks and malwares. Hence, IDS which is a vital element of the network needs to be safeguarded.

Steps of IDS are

- Monitoring and analysing traffic.
- Identifying abnormal activities.
- Assessing severity and raising alarm.

Figure 1 shows the basic architecture of intrusion detection system.

The Major Components of IDS Include

- Knowledge Base which encompasses pre-processed information provided by network experts and collected by the sensors.
- Configuration Device which provides data related to the present state of the IDS.
- Detector – ID Engine which identifies intrusive actions based on the data collected from sensors and sends an alarm to response component if intrusion occurs.
- Response Component which initiates response if an intrusion is detected.
- Data Gathering Device which is responsible for collecting data from monitored system.

The packets that are received are transmitted over the computer network and captured. Data are collected and pre-processed to remove the noise and irrelevant attributes. Then the pre-processed data are analysed and classified based on their severity actions. If the record is found normal, then it does not need any change in the action, otherwise, it is sent for report generation. Depending on the state of the data, alarms are raised to alert the administrator to handle the state in advance. The attack is modelled in order to facilitate the classification of network data.

Intrusion Detection Methods

In IDS, detection method is categorized into misuse detection and anomaly detection (Endler 1998) which are also known as knowledge based and behaviour based intrusion detection (Debar 2000) respectively. Patterns of well-known attacks are used to identify intrusions in misuse detection, whereas, anomaly