Chapter 6
Combating Cyber Security Breaches in Digital World Using Misuse Detection Methods: Misuse Detection

Subbulakshmi T.
VIT University, India

ABSTRACT

Intrusion Detection Systems (IDS) play a major role in the area of combating security breaches for information security. Current IDS are developed with Machine learning techniques like Artificial Neural Networks, C 4.5, KNN, Naïve Bayes classifiers, Genetic algorithms Fuzzy logic and SVMs. The objective of this paper is to apply Artificial Neural Networks and Support Vector Machines for intrusion detection. Artificial Neural Networks are applied along with faster training methods like variable learning rate and scaled conjugate gradient. Support Vector Machines use various kernel functions to improve the performance. From the kddcup'99 dataset 45,657 instances are taken and used in our experiment. The speed is compared for various training functions. The performance of various kernel functions is assessed. The detection rate of Support Vector Machines is found to be greater than Artificial Neural Networks with less number of false positives and with less time of detection.

1. INTRODUCTION

This paper focuses on Network Intrusion detection systems and related issues in identifying and monitoring attacks and the causes of attacks. A significant challenge in the area of Information security is to provide security both physically and technically to the information which may be stored either in the network (Network Intrusion Detection Systems) or host (Host Intrusion Detection Systems). Intrusion (Endorf et al., 2006) is defined as an active sequence of related events that deliberately cause harm or attack attempts both successful and unsuccessful such as rendering the system unusable, accessing unauthorized information or manipulating such information. Intrusion detection systems are defined as

DOI: 10.4018/978-1-5225-0193-0.ch006

(Endorf et al., 2006) tools, methods and resources to help identify assess and report unauthorized or unapproved network or host both due to insider and outsider threats. The placement of IDS in the network can be after the firewall and before the router. Another place of IDS may be before the firewall to completely stop external intrusions. On every system of the network the Host IDS can be placed along with the Network IDS to have more effective protection.

Based on the mode of detection Intrusion detection systems are categorized into two types. Misuse detection systems detect intrusions by comparing with previously detected intrusions database through pattern matching technique. Anomaly Intrusion Detection Systems are capable of detecting both known and unknown intrusions using the behaviour profiles by applying more sophisticated statistical techniques (Zhang et al., 2001)or Machine learning techniques (Mukkamala et al., 2005).

2. BACKGROUND

Soft computing was first proposed by Lotfi Zadeh to construct new generation computationally intelligent hybrid intelligent systems including Neural networks, Fuzzy logic, approximate reasoning and derivative free optimization techniques like Genetic algorithms for most of the real world applications like function approximation, Image processing and Intrusion detection.

Neural Networks are applied to effectively find out the intrusions by Martin Botha, Rossouw von solms. Next Generation Proactive Identification Model is used to protect the system using neural networks. This model is based on the assumption that each user's behaviour is unique and when he leaves the system it could be recorded for further comparison. Fuzzy Default Logic(FDL) (Jian et al., 2003)is applied to Intrusion Detection using reasoning and FDL-IDS was developed which increases detection speed and accuracy which reduces the cumulative cost of developing an traditional Intrusion Detection Expert System (Denning, 1987). A Novel attack detection method is proposed to detect intrusions using fuzzy logic and data mining. The proposed system is designed as both misuse and anomaly detection system by combining well-formed fuzzy if-then rules and simple data mining.

ANN and SVM are employed for intrusion detection using (Mukkamala & Sung, 2005) DARPA dataset and it is observed that SVMs are superior to ANN in three critical respects. SVM train and run an order of magnitude faster; SVM scale much faster; and SVMs give high classification accuracy. Feature selection and ranking is presented using two methods: first is Performance Based Ranking Method using performance metrics and 34 out of 41 features are selected for classification by a Multilayer FF ANN. Second using SVMs with support vector decision function. 23 out of 41 features are selected in this method for classification. SVMs prove higher classification accuracy.

NN and SVM are applied for misuse detection using DARPA data with (Mukkamala et al., 2005) all 41 features. The key idea is to discover useful patterns or features that can describe user behavior on a system and use them to build classifiers that can recognize known intrusions and anomalies in real time. The SVM IDS was developed for binary classification. The two classes are Normal (1) and Attack or intrusive patterns (-1). Attacks belong to 22 different attacks out of 25 which belong to four classes DoS, R2U, U2S and Probing. Data consists of 14292 points where 7312 for training and 6980 for testing. RBF kernel is used. The accuracy got in this is 99.50% with only 6 misclassifications. Three Multilayer FF