Name: Muna Mhammad Taher Jawhar
Title: Enhanced Design of an Intrusion Detection System
Supervisor: Monica Mehrotra
Department of Computer Science

Abstract

The rapid growth and deployment of network technologies and Internet services has made security and management of networks a challenging research problem. This growth is accompanied by an exponential growth in the number of network attacks, which have become more complex, more organized, more dynamic, and more severe than ever. These attacks can easily cause millions of dollar of damage to an organization. Detecting these attacks is an important issue of network security. Current network protection techniques are static, slow in responding to attacks, and inefficient due to the large number of false alarms. Therefore there is an increasing need for building effective security monitoring and detection system such as Intrusion Detection System to prevent such illicit accesses. Intrusion Detection System provide defense mechanism which monitors (oversees) user activity and network traffic to identify suspicious activity or patterns that may suggest potential intrusion or attack. Intrusion Detection attempts to detect computer and network traffics by examining various data records observed in processes on the network. Intrusion Detection System is split into two groups misuse detection system and anomaly detection system.

We present two network Intrusion Detection models which can efficiently detect both known and unknown types of network attacks with a high detection rate and low false alarms. The first model is signature based intrusion detection using neural networks. We have used two neural networks, the first one is traditional Hamming net and MAXNET. The second one is multi layer Perceptron with different architecture and training algorithms to find the best one, and we have compared between the two networks. After that we do an enhancement to the hamming network to give better performance.

The second model is anomaly based intrusion detection using neural network. We used two networks, the first one is hamming net and MAXNET, the second one is multi layer Perceptron. After that we do an enhancement to the model to make it work

better. We use hybrid fuzzy clustering with neural network to produce a new model with better performance. We used the data for training and testing the models from KDD Cup99 data set.

We have successfully implemented Intrusion Detection models. The experimental results of the intrusion detection model shows that the system can efficiently and effectively detect and protect against any type of network attacks.