Attacks classification in Network Intrusion Detection System Using ANN

Dr.A.P. Adsul¹,Pooja Danke²,Meghana Jagdale³,Kuldeep Chaudhari⁴,Samarth Jadhav⁵
¹,²,³,⁴,⁵Sinhgad Institute Of Technology And Science

Abstract
Nowadays with the dramatic growth in communication and computer networks, security has become a critical subject for computer systems. A good way to detect the algorithms, methods and applications are created and implemented to solve the problem of detecting the attacks in intrusion detection systems. Most methods detect attacks and categorize in two groups, normal or threat. This work presents a new approach of intrusion detection system based on artificial neural network. This work utilizes a Multi-Layer Perceptron (MLP) for intrusion detection system. The designed system will detect the attacks and classify them in six groups with the two hidden layers of neurons in the neural network.

Keywords: Artificial Neural Networks (ANN), Intrusion Detection System (IDS), MLP, Network Security.

1. INTRODUCTION
Today because of existence of Internet and highly increase in usages of computers and Internet by people, companies and governments doing their works and the dependency of systems to computer networks, as a result the security plays an essential role to prevent the attacks. The highly connected computing world has also equipped the intruders and hackers with new facilities for their destructive purposes. To detect malicious, illegal activities and brief attack description we needed efficient intrusion detection system. The system designed in this work usage the artificial neural network to minimize false positive and false negative alarms and improves the detection rate of attacks. For real time detection we are considering ICMP packets only.

Artificial Neural Network (ANN) is the network of individual neurons. Each neuron in a neural network acts as an independent processing element. Each processing element (neuron) is fundamentally a summing element followed by an activation function. The most successful application of neural network is classification or categorization and pattern recognition. There are two types of learning Supervise and Unsupervised. Multilayer Perceptron is well known architecture of supervised learning. The MLP is employed for Pattern Recognition problems.

2. System Architecture
The figure 2.1 illustrates the architecture of the attack classification system. In this the Packet Monitor module monitors network stream real time and capture packets to serve for the data source of the NIDS. In the pre-processing phase, network traffic collected and processed for use as input to system. The Feature Extractor module extracts feature vector from the network packets (connection records) and submits the feature vector to classifier module. The function of Classifier module is to analyse the network stream and to draw a conclusion whether intrusion happens or not. When detecting intrusion happens, Decision module will send a warning message to user.

Figure 2.1: System Architecture
The Knowledgebase module serves for the training samples of the classifier phase. The artificial neural network can work effectively only when it has been trained correctly and sufficiently. The intrusion samples can be perfected under user participation, so the capability of the detection can improve continually.

**Attacks Classification:** There are at least four different known categories of computer attacks including denial of service (DOS) attack, user to root (U2R) attack, remote to user (R2L) attack and probing attacks. Six types of attacks are considered: Smurf, Teardrop, Satan, Guest, Warezclient. These six attack types are selected from four different attack categories (denial of service, probing, user to root and remote to user) to check for the ability of the intrusion detection system to identify attacks from different categories.

3. System Implementation and Result

The section describes the detailing of the attack detection system as well as the result obtained from it.

3.1 Home page and File Select

![Figure 3.1: File Select](image1)

Input to system is given in text and arff format. After that data labelling is done. Data is labelled according to normal and attack packet as +1 and -1 as last bit position.

3.2 MLP Output

![Figure 3.3: MLP Output](image2)
Table is shown with output count and categories of attacks.

### 3.4 Detection

![Figure 3.4: Detection](image)

Table is shown with Detection rate, false positive alarm rate and false negative alarm rate.

### 3.5 Detection Chart

![Figure 3.5: Detection Chart](image)

Chart shows percentage of detection rate of attacks and false alarm.

**X axis:** Poles of Detection and False alarm.

**Y axis:** Percentage rate

### 3.6 Real time detection

![Figure 3.6: Real time Detection](image)
System detects the attack from another system which pings to home system.

4. Conclusion
Using Artificial Neural Network we have designed Network Intrusion Detection System. There is use of Multi-Layer Perceptron for learning purpose and Aprori Algorithm for rule creation. By end we able to detect and classify attack into Denial of Service (DoS), Probe, User to Root(U2R), Remote to User(R2L) categories with greater efficiency.

Acknowledgement
This research paper cannot be considered complete without mentioning Prof. Dr. A. P. Adsul. We wish to express true sense of gratitude towards her valuable contribution. We are grateful to her for constant encouragement and guidance in the fulfilment of this activity.

References