Intrusion Detection System Integrating Layered Framework with Neural Network

[1] **Sajil Eruvenkai** , [2] **Swati Tandale** , [3] **Chaitali Deochake,** [4] **Sayali Laigude**

[1,2,3,4] Sinhgad Institute of Technology and Science, Pune-41, India

Abstract - The increased reliance on network has made it necessary to increase the security and privacy of the data across the network .One of the major threats in such a situation is of intruders who try to attack the network system. The main focus is to prepare the network against such attacks. In this paper, we present layered framework integrated with neural network to build an effective intrusion detection system. This system has experimented with Knowledge Discovery & Data Mining (KDD) 1999 dataset. Neuroph studio has been used to train the neurons. The results show that the proposed system has high attack detection accuracy and less false alarm rate.

Keywords - *IDS; neural network, layered framework, KDD cup99 dataset.*

1. Introduction

Intrusion detection is identifying unauthorized access to a system the unauthorized access is not necessary to come from outside only. The intruder could be an authorized user who has certain privileges and is trying to access files beyond his privileges or is trying to hamper the files he is allowed to access. Thus, security of data and continuity of services can only be ensured by IDS. It is required that IDS can handle large amount of data without affecting performance and without dropping data and can detect attacks reliably without giving false alarms.

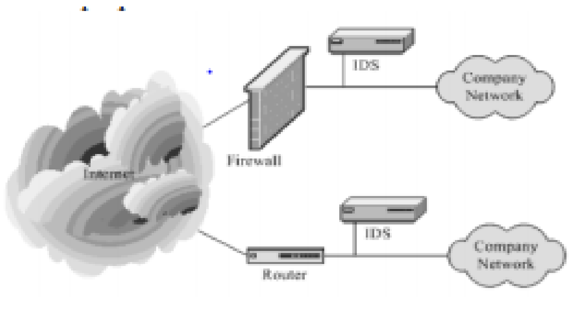


Figure 1: Basic IDS Working

1.1 An IDS is Broadly Classified as

A. Misuse based system

In misuse based IDS, detection is performed by looking for the exploitation of known weak points in the system, which can be described by a specific pattern or sequence of events or data. That means these systems can detect only known attacks for which they have a defined signature.

B. Anomaly based system

In anomaly based IDS, detection is performed by detecting changes in the patterns of utilization or behavior of the system. The main advantage of anomaly detection system is that they can detect previously unknown attacks.

To prepare the system we are using neural network. Set of neurons are trained by inputting the data sets-KDD CUP99.

1.2 Literature Survey

Because the last few years have seen a dramatic increase in the number of attacks, intrusion detection has become the mainstream of information assurance. The purpose of intrusion detection is to help computer systems prepare for and deal with attacks. Intrusion detection systems collect information from a variety of sources within computer systems and networks. For most systems, this information is then compared to predefined patterns of misuse to recognize attacks and vulnerabilities. This system was having some drawbacks. Later on the new concept of snort arises, that was having capability of handling IDS in network. However, there are new techniques of intrusion detection including the use of support vectors and neural network machines.

These techniques, along with behavioral data forensics, create a database of normal user behaviour and will alert the security officer if a deviation from that normal behaviour occurs. In the majority of intrusion detection systems, however, both network and host based intrusion detection systems combine to deal with attack detection and prevention from both inside and outside sources. Still, the intrusion detection system itself has an inherent risk attributed to it because of the absence of human intervention in some response scenarios.

2. Proposed Model

IDS under consideration combine the advantages of both layered framework and neural network The proposed IDS is used to detect four common types of attacks like Denial of Service(DoS),Probe, Remote to Local(R2L),User to Root (U2R) and normal records also. Thus, IDS is divided into four layers which are used to classify attacks as mentioned in figure below

Each layer of IDS consists of three components:

1) Data preprocessor

This component is used to collect the data from desired Source. Here, KDD cup 99 dataset is used which is publicly available

2) Encoder

Encoder is basically used to encode the data into desired Format.

3) Classifier

This component is used to analyze the audit pattern and classify it to detect attacks.Layered framework and back propagation alogirthm is used.

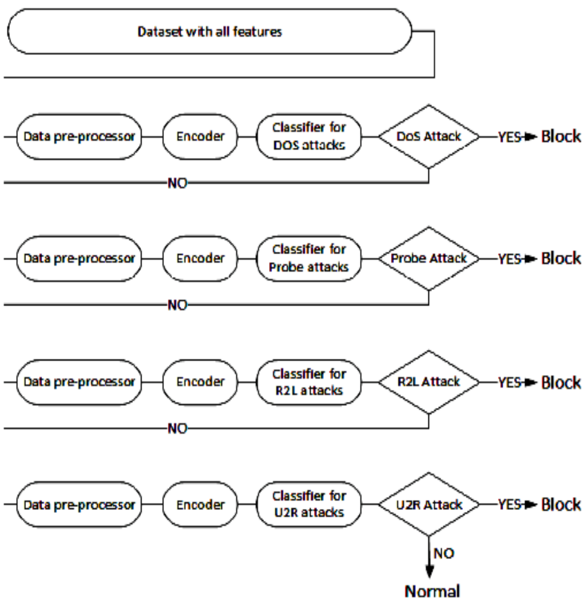


Figure 2: Work flow Diagram

3. Working

The neurons are trained using neuroph studio.The KDD CUP99 is inputed to train the neurons.The error rate is continuously monitored and traced until minimum error rate is obtained .the perceptron model is used for the working.it is a multi layered perceptron model.the neurons are placed on the nodes of the network.41 neurons are trained as per the 41 features in the data set.the data is filtered through this trained neurons and if a threat is detected then it is blocked.

1. Provide training to raw data in Neural Network.
2. Extract features from processed Data.
3. Set pattern and decision rules from Knowledge Database.
4. Provide rules sets to Intrusion Detection System.
5. Input read time data to Intrusion Detection System.
6. Set alarm to failure and pass of Intrusion Detection System test from pattern matching.
7. Display result.

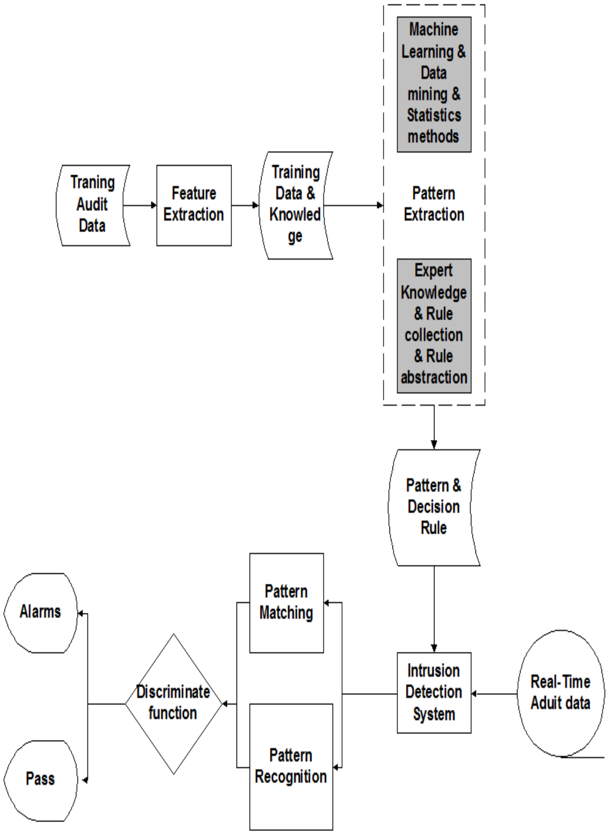


Figure 3:Structure

3.1 Equations

Hebb Learning Rule

1. If two neurons on either side of a synapse are activated simultaneously, the strength of the synapse will increase.
2. The connection (synapse) between input pj and output ai is the weight wij.

Unsupervised learning rule:

$$w_{ij}^{new} = w_{ij}^{old} + \alpha f_i(a_{iq}) g_j(p_{jq}) \Rightarrow w_{ij}^{new} = w_{ij}^{old} + \alpha \cdot a_{iq} p_{jq}$$

3. Not only do we increase the weight when pj and ai are positive, but we also increase the weight when they are both negative.

Supervised learning rule:

$$w_{ij}^{new} = w_{ij}^{old} + \alpha \cdot t_{iq} p_{jq} \Rightarrow W^{new} = W^{old} + t_q p_q^T (\alpha = 1)$$

In our system we are using supervised learning. The system will act to the threats it has been trained for.

3.2 Figures

The above diagram shows the structure of the neural network. This model is obtained after the data set inputed to the system.

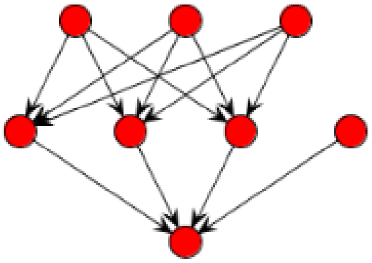
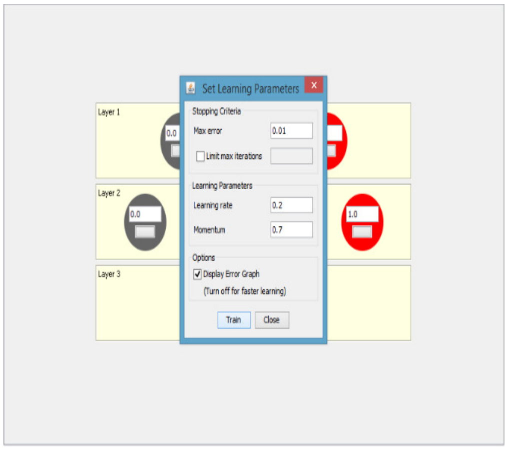


Figure 4: Structure of neural network

- The above diagram shows the structure of the neural network.



Set Learning Parameters

Stopping Criteria

Max error 0.01

□ Limit max iterations

Learning Parameters

Learning rate 0.2

Momentum 0.7

Options

☑ Display Error Graph

(Turn off for faster learning)

Figure 5: Initialization of parameters

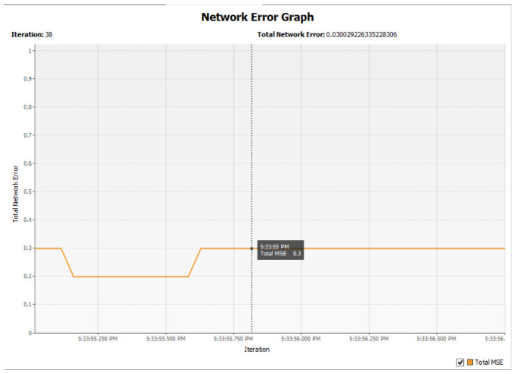


Figure 6

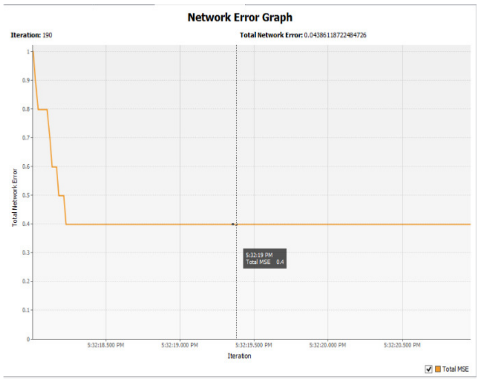


Figure 7

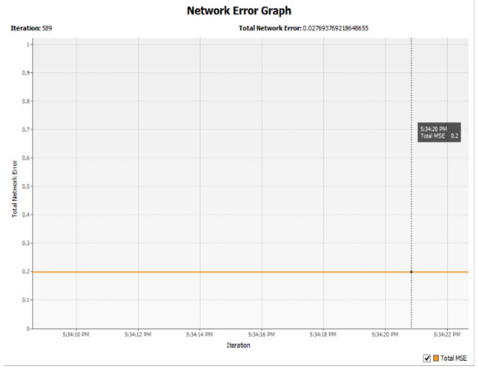


Figure 8

In the above diagrams the error rate is continuously tracked.as shown in the diagram the value decreases continuously as per the training given to the system. Initially the value is 0.04 then decreases to 0.03.As the value reaches 0.02 it recurs,. This is the minimum error rate that can be obtained.

4. Conclusions

In this paper, intrusion detection system is designed by integrating layered framework with neural network. From practical point of view, the experimental results imply that there is still scope of improvement as the proposed systems are not able to detect all types of attacks, thus it is interesting to investigate in this direction.

Appendix

KDD CUP DATA SET

Training data set

- back dos
- buffer overflow u2r
- ftp_write r2l
- guess_passwd r2l
- imap r2l
- ipsweep probe
- land dos
- load module u2r
- multihop r2l
- neptune dos
- nmap probe
- Perl u2r
- phf r2l
- pod dos
- portsweep probe
- rootkit u2r
- satan probe
- smurf dos
- spy r2l
- teardrop dos
- warezclient r2l
- warezmaster r2l

LIST OF DATA SET
Count
Srv_count
Serror_rate
Srv_serror_rate
Rerror_rate
Srv_rerror rate
Same_srv_rate
Diff_srv_rate
Srv_diff_host_rate
Dst_host_count
Dst_host_srv_count
Dst_host_same_srv_rate
Same_srv_rate
Dst_host_same_src_port_rate
Dst_host_srv_diff_host_rate
Dst_host_serror_rate
Dst_host_srv_serror rate
Dst_host_rerror_rate
Dst_host_srv_rerror rate

References

[1] Novel Intrusion Detection System integrating Layered Framework with Neural Network 2013 3rd IEEE.

[2] Getting started with neuroph by Zoran Sevarac and Marko Koprivica.

[3] A. Ghosh, A. Schwartzbard, "A study in using Neural Networks for Anomaly and Misuse Detection," Proceedings of the 8th USENIX Security Symposium, 1999.