Volume 2, Issue 10, October 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Comprehensive Analysis on Intrusion Detection Using Neural Network

**Saranya.V**[1]
[1]M.Phil Research Scholar,
PSGR Krishnammal College for Women,
Coimbatore-641004.

**Amsaveni.R**[2]
[2]Assistant Professor, Dept of Computer Science
PSGR Krishnammal College for Women,
Coimbatore-641004.

**Abstract:** ***Intrusion detection is the process of detecting intrusion in network which it compromises the confidentiality integrity and availability of a resource. In this paper we mainly focused on neural network algorithm applied for detecting intrusion. Aim of our research paper is to determine which neural network classifies the attacks with high detection rate and low false alarm rate. Five different types of algorithm are used in this paper multi layer perceptron, generalized feed forward, principle component analysis, self organizing feature map and radial basis function.***

***Keywords: Intrusion detection, neural network, attack types***.

## 1. INTRODUCTION

Intrusion detection is an important step to protect intrusion from computer system. It is used to detect, identify and stop intrusion. Basically intrusion detection system consist of host based and network based each approach have different functionality to monitoring and securing data and it consist of advantage and disadvantage. Host based intrusion detection examine data held on individual computer that serve as hosts, while network based intrusion detection examine data exchanged between computer.

### 1.1 ROLE OF IDS

The role of IDS is to detect abnormal traffic pattern from normal traffic where IDS monitors incoming and outgoing traffic. Common approach for implementing IDS is anomaly detection and misuse/signature detection.

**Anomaly detection**:-It is based on the normal behavioral pattern of the user when the user deviates from normal behavior then it is termed as intrusive.

**Misuse/signature detection**:- It is based on already known attack, if the attack matches already known attack then it is termed as intrusive.

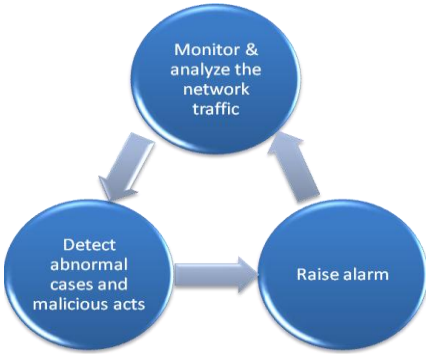


Fig.1- Role of IDS

### 1.2 COMPONENTS OF INTRUSION DETECTION SYSTEM

IDS consists of several component following are some of the most important components

**Agent or Sensor: -** The term Agent is typically used in the host and the term sensor is used in network. It generates security events, monitors and analyzes activity in network.

**Console: -** It is a program that provides an interface between the IDS user and administrator.

**Engine: -** Records the event logged by the sensor in a database and uses a system of rules to generate alerts from security events received.

### 1.3 TYPES OF ATTACKS

**Denial of Service (DOS): - I**n this type of attack it slow down the system or shut down the system so it disrupt the service and deny the legitimate authorized user.

**User to Root Attack (U2R):** - In this type of attack at first attacker starts to access normal user account on the system e.g: by taking down the password, dictionary attack. At last attacker achieves root to access the system

 

**Remote to User Attack (R2U): -** In this type of attack an attacker who has the capability to send packet to a machine over a network but does not have an account on that machine, make use of some vulnerability to achieve local access as a user of that machine.

**Probes: -** In this type of attack examines a network to collect information or discover well-known vulnerabilities. These network investigations are reasonably valuable for an attacker who is staying an attack in future. An attacker who has a record, of which machines and services are accessible on a given network, can make use of this information to look for fragile points.

**1.4 DATASET**

KDD cup 99 dataset is based on 1998 DARPA, where dataset is based on four attack categories (Dos, probing, u2r and r2l) it consists of 41 features. 41 features are classified in to three groups.

**1. Basic Features**:

In this feature attributes are extracted from TCP/IP connection.

**2. Traffic Features**:

In this feature attributes are classified as same host features and same service features it is monitored based on past 2 seconds.

**3. Content Features:**

It consists of attribute, which it looks for suspicious behavior of the data portion

Following shows list of 41 features used in dataset

| S.No | Feature Name | Description |
|---|---|---|
| 1. | Duration | Duration of the connection |
| 2. | Protocol type | Connection protocol e.g tcp,udp etc., |
| 3. | Service | Destination service e.g telnet, ftp etc., |
| 4. | Flag | Status flag of the connection |
| 5. | Src bytes | Bytes sent form source to destination |
| 6. | Dst_bytes | Bytes sent from source to destination |
| 7. | Land | 1 if connection is from/to the same host/port ; otherwise set to 0 |
| 8. | Wrong_fragment | Number of wrong fragment |
| 9. | Urgent | Number of urgent packets |
| 10. | Hot | Number of "hot " indicators |
| 11. | Num_failed_logins | Number of failed logins |
| 12. | Logged_in | 1 if successfully logged in; 0 otherwise |
| 13. | Num_compromised | Number of compromised conditions |
| 14. | Root_shell | 1 if root shell is obtained otherwise set to 0 |
| 15. | Su_attempted | 1 if "su root" command attempted ;0 otherwise |
| 16. | Num_root | Number of "root" accesses |

 

| | | |
|---|---|---|
| 17. | Num_file_creation | Number of file creations |
| 18. | Num_shells | Number of shell prompts |
| 19. | Num_access_files | Number of operation on access control files |
| 20. | Num_outbound_cmds | Number of outbound commands in ftp session |
| 21. | Is_host_login | 1 if the login belongs to the host otherwise set to 0 |
| 22. | Is_guest_login | 1 if the login belongs to the guest login otherwise set to 0 |
| 23. | Count | Number of connections to the same host as the current connection in the past two seconds |
| 24. | Srv_count | Number of connections to the same services aa the current connection in the past two seconds |
| 25. | Serror_rate | % of connection that have “SYN” errors |
| 26. | Srv_serror_rate | % of connection that have “SYN” errors |
| 27. | Rerror_rate | % of connection that have “REJ” errors |
| 28. | Srv_rerror_rate | % of connection that have “REJ” errors |
| 29. | Same_srv_rate | % of connection to the same service |
| 30. | Diff_srv_rate | % of connection to the different service |
| 31. | Srv_diff_host_rate | % of connection to the different host |
| 32. | Dst_host_count | Count of connections having the same destination host |
| 33. | Dst_host_srv_cont | Count of connections having the same destination host and using the same service |
| 34. | Dst_hostdst_same_srv_rate | % of connections having the same destination host |
| 35. | Dst_host_diff_srv_rate | % of diff services on the current host |
| 36. | Dst_host_same_src_portrate | % of connections to the current host having the same source port |
| 37. | Dst_host_srv_diff_host_rate | % of the connections to the same service coming from different hosts |
| 38. | Dst_hot_serror_rate | % of connections to the current host that have s0 error |
| 39. | Dst_host_srv_serror_rate | % of connections to the current host and specified service that have an s0 error |
| 40. | Dst_host_rerror_rate | % of connections to the current host that have RST serror |
| 41. | Class label | Type of attack |

 

## 2. NEURAL NETWORK

A Neural network is an information processing system that is inspired by the way biological nervous system to process the information. It consists of large number of highly interconnected processing elements working with each other to solve specific problem. Processing elements are termed as neurons it is basically a summing element followed by an activation function. The output of each processing elements after applying the weight parameter associated with the connection is fed as the input to all of the processing elements in the next layer. The learning process is essentially an optimization process in which the parameters of the best set of connection coefficient i.e., weights for solving a problem. It follows three steps

1. Present the neural network with a number of inputs i.e., vectors each representing a pattern.
2. Check how closely the actual output generated for a specific input matches the desired output
3. Change the neural network parameters i.e., weights to better approximate the outputs.

### 2.1 Multilayer perceptron:

A Multilayer perceptron(MLP) are layered feed forward network typically trained with static back propagation. These networks have found their way into countless applications requiring static pattern classification. Their main advantage is that they are easy to use, and that they can approximate any input/output map. The main disadvantage is that they train slowly and require lot of training data.

### 2.2 Generalized feed forward:

Generalized feed forward(GFF) networks are a generalization of the MLP such that connections can jump over one or more layers. Multi layer perceptron can solve any problem that a generalized feed forward network can solve. In general generalized feed forward networks often solve the much more efficiently. Good example for this two-spiral problem. Without describing the problem, it suffices to say that a standard multi layer perceptron requires hundreds of times more training epochs than the generalized feed forward network containing the same number of processing elements.

### 2.3 Radial basis function(RBF)

Radial basis function networks are nonlinear hybrid networks are typically containing a single hidden layer of processing elements. This layer uses Gausian transfer functions rather than the standard sigmoid functions employed by multi layer perceptron. The centers and widths of the gaussians are set by unsupervised learning rules and supervised learning is applied to the output layer. These networks tend to learn much faster than multi layer perceptrons. If a generalized regression or probabilistic net is chosen all the weights of the network can be calculated analytically. In this case the number of cluster centers is by definition equal to the number of exemplars and they are all set to the same variance.

### 2.4 Self-organizing feature map

Self-organizing feature maps(SOFM) transform the input of arbitrary dimension into one or two dimensional discrete map subject to a topological(neighborhood preserving) constraint. The feature maps are computed using kohonen-unsupervised learning. The output of the self organizing feature map can be used as input to a supervised classification neural network such as the multi layer perceptron. This networks key advantage is the clustering produced by the self organizing feature map which reduces the input space into representative features using a self-organizing process. Hence the underlying structure of the input space is kept, while the dimensionally of the space is reduced.

### 2.5 Principal component analysis

Principal component analysis(PCA) combined unsupervised and supervised learning in the same topology. Principal component analysis is an unsupervised linear procedure that finds a set of uncorrelated features, principal component from the input. An multi layer perceptron is supervised to perform the nonlinear classification from these components.

## 3. LITERATURE SURVEY

Project dealing with the approach results in the system is called Hyperview. [4] it is a system that is built on two components . An ordinary expert system component has a task to monitor logs and according to the defined policy search the instructions. It is a signature based IDS second component neural network that can observe the behavior of the user and send the alarm if the observed behavior is violated. This work shows how neural network can be used in combination with expert systems and improves intrusion detection qualities. [5] Author describes and concludes that the combination of Radial basis function and Self-organizing map is very convenient to use as an intrusion detection model. He concludes that the evaluation of human integration is necessary to reduce the classification error. Experiment results are promising and show that Radial basis function- self-organizing map achieves, compared to radial basis function, similar or even better results. [6] Author describes an approach to dynamic intrusion detection using Self-organizing map. The authors estimate that orderly built unsupervised neural network approach is able to produce encouraging results. [7] Ryan et al. describes an offline anomaly detection system, which utilizes a back-propagation MLP neural network. The MLP was trained to identify users profile and at the end of each log session, the MLP evaluated the users commands for possible intrusion in offline. Authors described their research in a small computer network with ten users. Each feature vector described the connections of a single user during a whole day. They use three layers MLP two hidden layer. The MLP identified the user correctly 22 cases out of 24.[8] Author Mukamala used three and four layer neural networks and reported results of about 99.25% correct classification for their two class either normal or attack.

 

## 4. EXPERIMENT AND RESULTS

In our experiment consists of four layers of neural network. Input layers consist of 41 neuron, three hidden layers composed of 43,21and 41 neurons and an output layer of one neuron for "intrusion" or "normal" connection. In learning phase the output value is set to "0" if the connection record is normal otherwise output value is set to"1" the connection record is attack. Table 4.1 shows distribution of normal and attack records in our dataset.

Table 4.1 Connection records in dataset

| Connection type | KDD Data set | Our dataset |
|---|---|---|
| Normal | 20270 | 2000 |
| DOS | 391458 | 8000 |
| PRB | 4107 | 4000 |
| R2L | 1126 | 1100 |
| U2R | 52 | 52 |

In order to measure the performance of an intrusion detection two types of rates are measured. True Positive rate or Detection Rate according to the threshold value of the neural network and false positive rate or false alarm. The system achieves best performance for high value of detection rate and low value of false alarm rate. A Confusion matrix (CM) is defined as associating classes as labels for the rows and columns of a square matrix in the KDD dataset there are five classes normal, probe, denial of service, user to root attack, remote to local attack. Confusion matrix has dimensions of 5x5. An entry at rows I and column j CM (I, j) represents the number of misclassified patterns, which originally belong to class I yet mistakenly identified as a member of class j. The percent of correct classification (PCC) is used to evaluate the efficiency of classification of the instances belonging to our dataset.

The result of the experiment is detailed in below table 4.2

| Algorithm | Attack classification rate (%`) | Normal classification rate (%) | Detection rate (%) | False alarm rate(%) | Percent of correct classification(%) |
|---|---|---|---|---|---|
| MLP | 99.90 | 97.2 | 84.23 | 15.72 | 99.41 |
| GFF | 99.88 | 97.14 | 83.98 | 16 | 99.30 |
| RBF | 95.56 | 65.95 | 90.11 | 9.88 | 89.72 |
| SOFM | 98.47 | 61.57 | 91.27 | 8.71 | 91.20 |
| PCA | 97.07 | 54.1 | 93.83 | 6.16 | 88.6 |

According to the table 5.1 the Principle component analysis performs high detection rate and low false alarm rate

## 5. CONCLUSION

In this paper we classify the connection as normal or attack. The Principle Component Analysis neural network performs high detection rate as compare to other performance lower false alarm rate and minimum learning time. In future work I would like to implement this intrusion detection concept in hybrid neural network to achieve high performance and low false alarm rate.

## REFERENCES

[1] Anderson J.P "Computer Security Threat Monitoring & Surveillance", technical Report, James Anderson.co Fort Washington, Pennyslavia 1980.

[2] Dorthy E.Denning, "An intrusion detection model", IEEE transaction on Software Engineering", SE-13(2), 1987 pp222-232.

[3] Jake Ryan Meng-Jang Lin, Risto Miikkulainen "Intrusion detection with Neural Network"

[4] Debar H, Becker M, Siboni D "A neural network component for an intrusion detection system" IEEE symposium on research in computer security and privacy, Oakland , CA May 1992

 

[5] Horeis T.”Intrusion detection with neural networks combination of self-organizing maps and radial basis function networks for human expert integration” computational intelligence society research report August 2006

[6] Heywood M, Lichodzijewski P,Zincir –Heywood N “Dynamic intrusion detection using self organizing maps” In the annual Cannadian information technology security symposium August 2006

[7] Ryan J, Lin M, Miikkulainen R. “Intrusion detection with neural networks” In AI approaches to fraud detection and risk management

[8] Mukkamala S. “Intrusion detection using neural networks and support vector machine “ in the proceedings of the 2002 IEEE international joint conference on Neural networks”

 