Scientific Journal of Impact Factor (SJIF): 7.37
E-ISSN (O): 2348-4470
P-ISSN (P): 2348-6406
International Journal of Advance Engineering and Research Development
Volume 13, Issue 4, April 2026

Intelligent Intrusion Detection: A Deep Learning Approach for Cyber Attack Classification Using ANN

Manish Gupta[1], Prof. Shalini Roy[2], Prof. Deepak Srivastava[3]
[1]Research Scholar, Computer Science Dept., Indian Institute of Technology Roorkee, India
[2]Professor, School of Computing, Banaras Hindu University, India
[3]Associate Professor, Faculty of Engineering, Motilal Nehru National Institute of Technology Allahabad, India

Abstract: *Technological advancements have lead to increase in number of computer technologies. Due to increase in computer technologies the security of it has become a major concern .There is a need to secure the computer systems from intruders and hackers. Thus for securing the computer systems Intrusion Detection System (IDS) comes into scenario. IDS detect any intrusion arriving at the computer system and alert the administrator of the system about the arrival of intrusion. This paper presents a new approach for developing IDS using Artificial Neural Network. The proposed system uses backpropagation algorithm to train the neural network for classifying the attacks. The real time classification of attack is achieved by using feed forward algorithm.*

Keywords: *Intrusion Detection System (IDS), Artificial Neural Network (ANN) ,Back Propagation Algorithm, Intrusion.*

I. INTRODUCTION

Due to the expeditious growth and fast expansion of computer network, the world is facing the new challenges related to security, availability, integrity and confidentiality of computer system. Along with this, the number of intruders and hackers are also increasing.so there is a need of a system which protects the computer data from these threats. One such system which has gained popularity in the recent years is Intrusion Detection System.

I. INTRUSION DETECTION SYSTEM (IDS)

Before studying the IDS first understand the meaning of intrusion. Set of actions that attempt to break the security of computer system by duplication, alteration, destruction and unauthorized access to computer data is known as Intrusion. To protect our computer from such intrusions, intrusion detection system is useful. An IDS is a computer program which triggers the administrator when any intruder or machine is trying to access, delete or modify the information through illegal activities without following security policy.

Basically it is used for detecting, blocking and reporting unauthorized activities in the computer system. It monitors the system activities and events and analyzes them for sign of intrusion by comparing them with the predefined set of patterns. The purpose of IDS is to protect the computer data from an unauthorized access, duplication, alteration and destruction .It helps to protect the computer from the threats related to security, confidentiality and availability of the system.

II. TYPES OF IDS

IDS are classified based on the factors such as source of audit trail, knowledge of resources and types of responses.

I. Knowledge of resources:

I. Misused Based: It is also known as signature based or knowledge based IDS. In this type of system, the suspicious behavior of system or the attacks are defined in terms of patterns. If the behavior of current system found similar to these defined patterns then it declared it as an intrusion.

II. Anomaly Based: It is also known as heuristic or behavior based IDS. In this type of system, the normal behavior of system is defined in terms of patterns. If the behavior of current system is deviated from this predefined patterns, then it is declared as an intrusion

III. Hybrid: Basically it is combination of first two systems

IV. Source of audit patterns:

I. Network based: This type of IDS works for particular network and examines entire network traffic. It also monitors the data flow from that network.

II. Host Based: This type of IDS, used for individual computer. It monitors OS audit trails, system logs and kernel operations for individual host.

III. Application Based: It works for particular application and protects that application from intrusion.

IV. Type of response:

I. Active Response: An active IDS not only detects the attacks but also perform some prevention action against an intrusion.

II. Passive Response: This type of IDS only detects the attack and gives alert to the administrator. But it is incapable of performing any action against the attacks

III. LITERATURE SURVEY

There are several techniques available for the detection of intrusions in computer system. The concept of IDS was firstly proposed by Dorothy Denning to provide security. IDES (Intrusion Detection Expert System) used statistical approach for implementing Intrusion Detection System. This system uses profiles which contains the information about the normal behavior of user and then compares this with current user behavior and indicates the intrusion when there is slight difference between them. The disadvantage of this system is that it is not able to detect the attacks which are sequentially dependent on each other. Determining the threshold for particular attack is also difficult.

Another technique that is used for implementing IDS is Decision Tree Algorithm. Here tree like structure is used to model the underlying patterns or data. Different data mining algorithms are used along with decision tree to do the classification of attacks. This algorithm creates decision tree by taking set of predefined data as input and learns the patterns in that data. Based on this learning it creates rules to classify the various types of attacks.

State Transition Analysis is another approach for developing IDS. It constructs graphical representation of attacks based on the information about the state change of a computer system. It uses audit trails to construct these transition diagrams and the analysis tool is used for comparing the transition diagram of current user and transition diagram of known intrusions. But it fails to detect the attacks which cannot be modeled into transition diagrams and also fails in more complex situation

IV. PROPOSED SYSTEM

The proposed system is built by using pattern matching application of Artificial Neural Network (ANN). This system detects the attacks occurring at the host machine and classifies those attacks based on the training given to ANN using backpropagation algorithm.

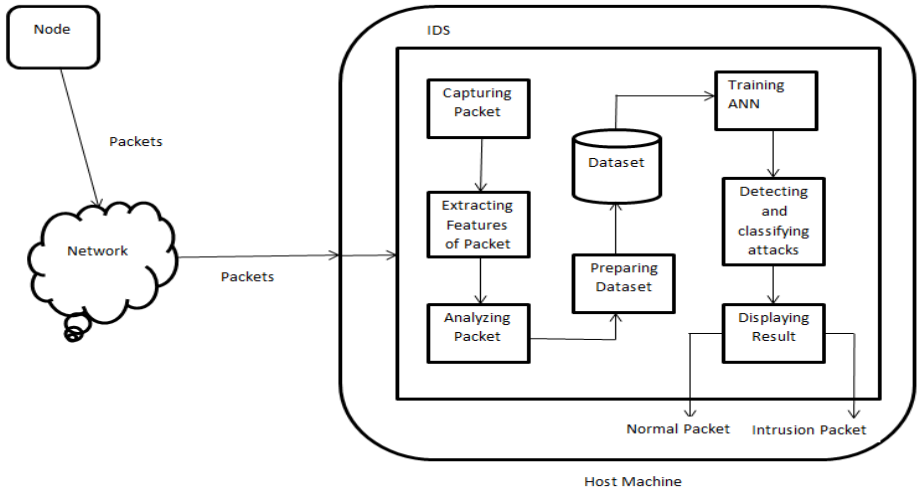

Fig.1.Block Diagram of Proposed System

The blocks of above Figure.1.are explained as follows:

I. Capturing Packet: It will capture the incoming packets in the host machine.

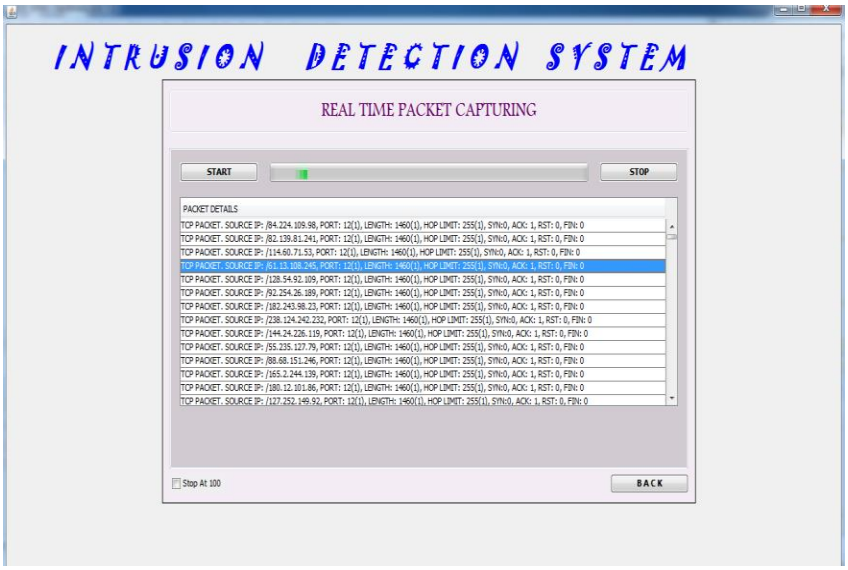

Fig.2.Packet Capturing.

II. Extracting Features of Packet: This block will extract the features of the incoming packets.

III. Analyzing packet: This block analyzes the extracted features of the packets to check whether it is normal or suspicious packet.

IV. Preparing Dataset: Based on the analysis of the packets, the dataset is prepared. This dataset contain the information about the features of the packets including the type of packet whether it is normal or attacking packet.

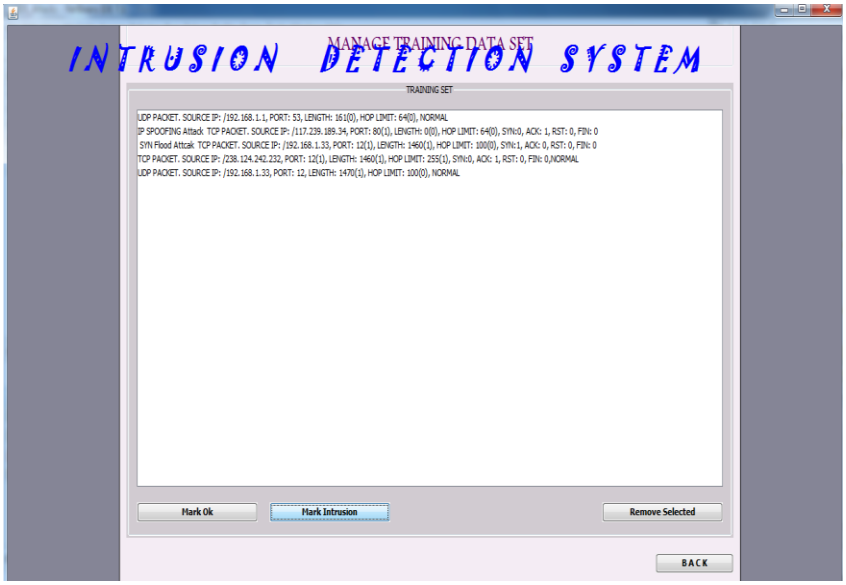

Fig.3.Preparing and Managing dataset.

5. Training ANN: Here the backpropagation algorithm is used for training the neural network which uses the dataset information as input

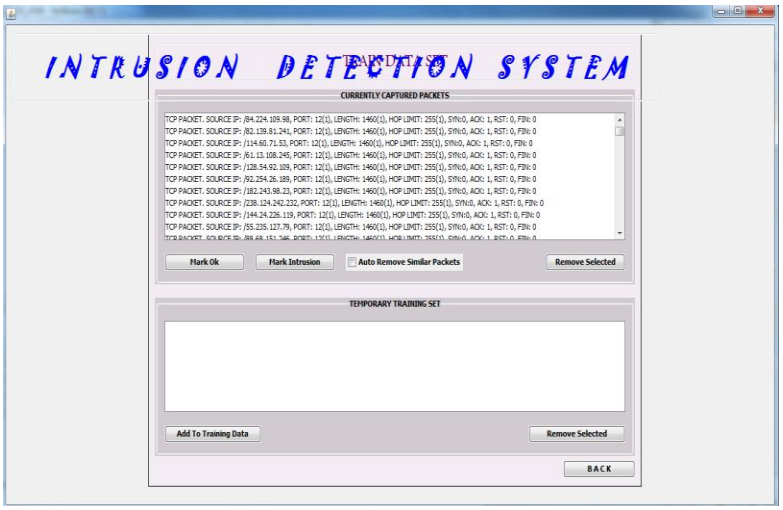

Fig.4.Training ANN Dataset

I. Detecting and classifying Attacks: Based on the training given to the ANN, it detects and classifies the packets in the real time scenario.

II. Displaying Result: The work of this block is to display the attacking packets along with its features and type of attack.

III. ARTIFICIAL NEURAL NETWORK

The proposed system classifies the different types of attack by using Artificial Neural Network. Artificial neural Network is one of the important information processing systems. The idea of ANN is emerged from biological nervous system.ANN is consists of number of tightly connected artificial neurons which are arranged in layered format. ANN consists of three layers i.e. input layer, hidden layer and output layer. ANN is mostly useful in the process of categorization and pattern matching. Similar to human brain, ANN learns from examples. For that purpose training is given to the network by using Backpropagation algorithm.

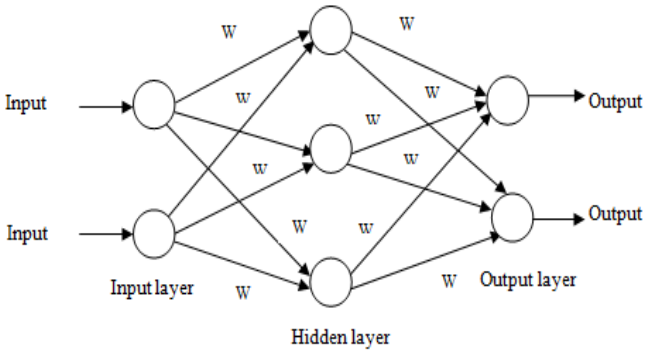

Fig.5. Structure of Artificial Neural Network

IV. BACKPROPOGATION ALGORITHM

A backpropagation algorithm is used for training the neural network for classification of attacks. This algorithm is based on supervised learning concept.

Steps of backpropagation algorithm for implementing the IDS:

1. Initialize the random value to the weights.
2. Apply the features of packet as input to the network

3. Calculate the output by considering the input and weight values.
4. Calculate the error by comparing obtained output and actual output.
5. Minimize this error by backtracking in the network and assigning the new values for weights.
6. Repeat all the steps again till ANN learns the data.

V. ATTACKS

The attacks which are classified by proposed system are as follows:

I. TCP SYN Flood

In TCP SYN Flood attack, TCP Connection requests are sent rapidly than a machine can process. Here attacks are sent through number of fake IP addresses such that the server replies to each received SYN packet. When the server replies to each SYN packet, then attacker is supposed to reply with SYN/ACK Packet. Instead of sending back the SYN/ACK, it resends the SYN packet. Thus keeping the server busy.

II. UDP Flood attack

UDP is basically connectionless protocol which does not provide reliability of connection and ordered delivery of messages. UDP Flood attack also sends large number of packets containing UDP datagram to the target machine. On receiving these packets the machine checks whether there are any applications related with these datagrams. If no applications are found then it sends back "Destination Unreachable" packet. Thus making the target machine passive by sending and receiving large number of packets.

III. ICMP Attack

ICMP is Internet Control Message Protocol which is a connectionless protocol which is a part of IP implementation and used for IP diagnosis, errors. In ICMP flood attack, large number of packets is sent to the target machine so that it will process the request and send back the reply. But due the arrival of large number of packets the CPU resources get busy and are not able to respond to valid requests.

6. CONCLUSION

This paper gives information about the IDS which classifies different types of attacks based on Artificial Neural Network. Due to supervised training given to ANN the real time classification of attacks is possible. This system only classifies the attacks but does not take any preventing action. Hence there is scope for future work to implement the Intrusion Prevention System.

REFERENCES

[1] NidhiSrivastav, Rama Krishna Challa, "Novel Intrusion Detection System integrating Layered Framework with Neural Network",2013 3rd IEEE International Advance Computing Conference(IACC), 2013
[2] Carlos Gershenson, "Artificial Neural Network for Beginners"
[3] Amrita Anand, Brajesh Patel, "An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012.
[4] Sandhya Peddabachigari, Ajith Abraham*, Johnson Thomas, "Intrusion Detection Systems Using Decision Trees and Support Vector Machines".
[5] Manish Kumar, Dr. M. Hanumanthappa," Intrusion Detection System Using Decision TreeAlgorithm"
[6]Minal Z, Pooja D,SnehalP,PoonamP,Priyanka P," Intrusion Detection System Using Artificial Neural Network", International Journal of Emerging Engineering Research and Technology ,Volume 2,Issue 6.

