

# **PROJECT REPORT**



## **ADVANCES IN INTRUSION DETECTION / PREVENTION SYSTEM**

**UNDER THE GUIDANCE**

**OF**

**HEAD. PROF. Dr.B.M MEHTRE**

**IDRBT**

**Submitted By**

**N.VIGNESHWARAN**

**(Indian Academy of Sciences, Bangalore)**

## **CERTIFICATE**

This is to certify that Mr.N.VIGNESHWARAN, M.E from Indian Academy Of Sciences, Bangalore, have undertaken a project at IDRBT, Hyderabad from May 05, 2015 to Jun 30, 2015.

He was assigned the project “ADVANCES IN INTRUSION DETECTION / PREVENTION SYSTEM” under my guidance.

I wish him all the best for all his future endeavors.

Head. Professor

Dr.B.M.Mehtre

(Project Guide)

IDRBT, Hyderabad

## **ACKNOWLEDGMENT**

I express my deep sense of gratitude to my Guide Dr.B.M,Mehtre Head and Professor, IDRBT for giving me an great opportunity to do this project in the Institute for development and research in Banking Technology and providing all the support.

I am also thankful to Dr.B.L.Deekshatulu, and Dr.Rajarshi Pal, for providing feedback regarding the project.

I am thankful to Mr.Hiran.V Nath, other faculties and colleagues who constantly encouraged me for my project work and guided me by providing all the necessary information.

I am also thankful to Indian Academy of Sciences, Bangalore and SSN College of Engineering, Chennai for giving me this golden opportunity to work in a high-end research institute like IDRBT. Am very much thankful to my parents for their support given to me and to make it as possible.

**N.VIGNESHWARAN**

(IASc, Bangalore)

## **ABSTRACT**

Network Security is to protect computer network against hacking, misuse, unauthorized changes to the system and securing a computer network infrastructure. A firewall is a mechanism used to achieve network security. It can be either hardware or software based, that controls incoming and outgoing network traffic based on a set of rules. Network attack is the intrusion or threat can be defined as any deliberate action that attempts unauthorized access, information manipulation, or rendering the system unstable by exploiting the existing vulnerabilities in the system. An intrusion is any set of activities that attempt to compromise the integrity, confidentiality or availability of a resource. Intrusion Detection system (IDS) / Intrusion Prevention System (IPS) has become a prerequisite in computer networks. IDS/IPS is a device or software application that monitors network or system activities for malicious activities. These type of IDS/IPS used in the network is known as Network based IDS/IPS.

Network based Intrusion detection/prevention system (NIDPS) protects a network of hosts and systems. Based on the intrusion detection method, it is classified as Signature based and Anomaly based IDS/IPS. Signature based IDS/IPS is that they operate in much the same way as a virus scanner, by searching for a known identity or signature. It can only detect an intrusion attempt if it matches a pattern that is in the database, therefore the databases need to constantly be updated to detect the new attacks. An Anomaly based Intrusion Detection/Prevention System is a system for detecting computer intrusions by monitoring system activity and classifying it as either normal or anomalous. If malicious activity may be looks like normal traffic to the system, it will never send an alarm. Major drawback of anomaly based IDS/IPS is that it generates more false positive alarm.

Our proposed model is to implement the architecture of multimodel based Anomaly IDS with time delay neural network(TDNN) based NIDS system. Virtual machine was used to implement the architecture of multimodal based anomaly IDS with Network based IDS system. Captured the packets in real time network traffic using the tool JPCAP. Packet features like Source IP, Destination IP, frames, Port, Mac Address, format, Protocol type, Datalink, interface device name are extracted and analyzed. Done the implementation of both the proposed algorithms of multimodal based anomaly IDS with Neural Network based NIDS system using JAVA code. Then Packet analysis and testing have done with the data sets of US army. With that it can detect the new attacks.

<b>CHAPTER 1 – INTRODUCTION</b>	<b>7</b>
1.1 Introduction to Network Security	7
1.1.1 Information Security	7
1.1.2 Network Attacks and its types	8
1.1.3 Intrusion	9
1.1.4 Intrusion Detection/Prevention System	9
1.1.5 Classification of Intrusion Detection Systems	10
1.1.6 Network Intrusion Detection System	10
1.1.7 Signature based IDS/IPS	11
1.1.8 Anomaly based IDS/IPS	12
1.1.9 Markov Model	13
1.1.10 Hidden Markov Model	14
1.2 Neural Network	17
1.2.1 Feed Forward Network	20
1.2.2 Back Propagation	20
1.2.3 Supervised Learning	21
1.2.4 Unsupervised Learning	21
<b>CHAPTER 2 - LITERATURE SURVEY</b>	<b>22</b>
2.1 Literature Survey on Intrusion Detection System	22
<b>CHAPTER 3 – PROPOSED WORK</b>	<b>23</b>
3.1 Proposed model	24
3.2 Outputs	25
<b>CHAPTER 4 - CONCLUSION AND FUTURE WORK</b>	<b>26</b>
4.1 Conclusion	26
4.2 Future Work	26
References	27

## LIST OF FIGURES

FIGURE No.	TITLE	PAGE No.
1.1	Components of Intrusion Detection System	10
1.2	Network Intrusion Detection System	11
1.3	Signature Based IDS/IPS	12
1.4	Anomaly Based IDS/IPS	13
1.5	Markov Model	14
1.6	Hidden Markov Model	14
1.7	State Transition with Probability	17
1.8	Neural Network	18
1.9	Feed Forward Neural Network	21
1.10	Proposed Model	24
1.11	Packet Captured Output	25
1.12	Neural Network Algorithm Output	26

## **CHAPTER 1 - INTRODUCTION**

### **1.1 Introduction to Network Security**

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

#### **Need for Network Security**

In the past, hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and generally open networks have generated an increased need for network security and dynamic security policies.

The easiest way to protect a network from an outside attack is to close it off completely from the outside world. A closed network provides connectivity only to trusted known parties and sites; a closed network does not allow a connection to public networks.

#### **1.1.1 Information Security**

Information security is the protection of information and minimises the risk of exposing information to unauthorised parties. It is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organisational, human-oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

The value of information comes from the characteristics it possesses

- Availability
- Accuracy
- Authorization
- Confidentiality
- Integrity
- Utility

### **1.1.2 Network Attack and its Types**

Networks attacks are subject to attacks from malicious sources. Network attack is the intrusion or threat can be defined as any deliberate action that attempts unauthorized access of Information manipulation and by exploiting the existing vulnerabilities in the system. A Network attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Network attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

#### **Types of Attacks**

- Passive Attacks
- Active Attacks

Passive Attacks- An network intruder intercepts data travelling through the network

(e.g) Wiretapping, port and idle Scanner

Active Attacks - An intruder initiates commands to disrupt the network's normal operation.

(e.g) DOS, Spoofing, SQL Injection, Cross-site Scripting



### **1.1.3 Intrusion**

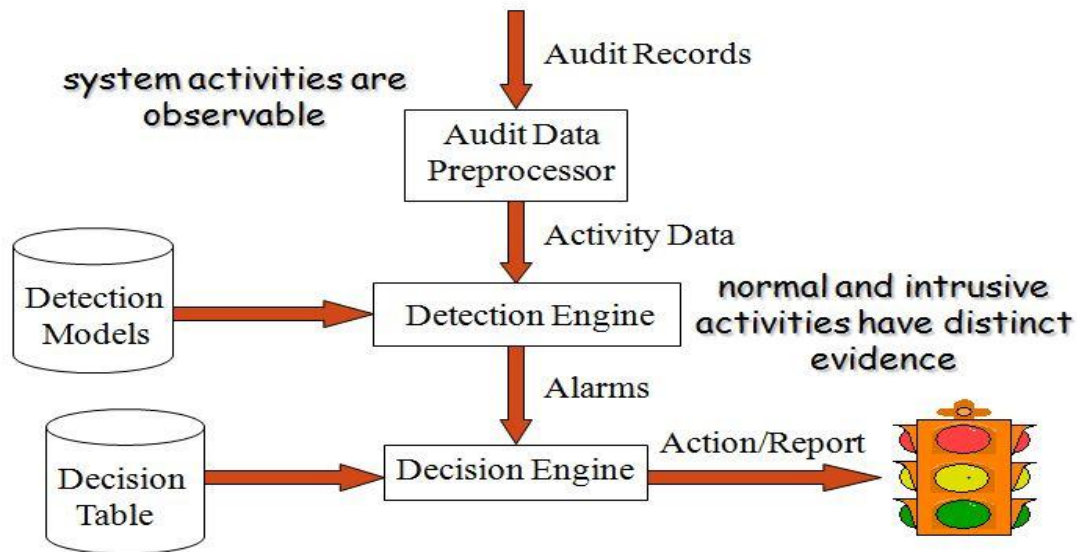
A deliberate attempt to enter a network and break the security of the network and thus breaking the confidentiality of the information present in the systems of the network . The person who tries to attempt such an action is called as an Intruder and the action can be termed as Network Intrusion. It is any set of activities that attempt to compromise the integrity, confidentiality or availability of a resource.

### **1.1.4 Intrusion Detection/Prevention System (IDS/IPS)**

An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. Many IDS tools will also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control. An IPS is a type of IDS that can prevent or stop unwanted traffic. The IPS usually logs such events and related information. An Intrusion Prevention System (IPS) goes one step further and not only detects attacks but attempts to prevent them as well.

#### **Intrusion Detection functions:**

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations



**Figure 1.1 Components of Intrusion Detection System**

### **Advantages of Intrusion Detection Systems**

- The network or computer is constantly monitored for any invasion or attack.
- The system can be modified and changed according to needs of specific client and can help outside as well as inner threats to the system and network.
- It effectively prevents any damage to the network.
- It provides user friendly interface which allows easy security management systems.
- Any alterations to files and directories on the system can be easily detected and reported

### **1.1.5 Classification of Intrusion Detection System**

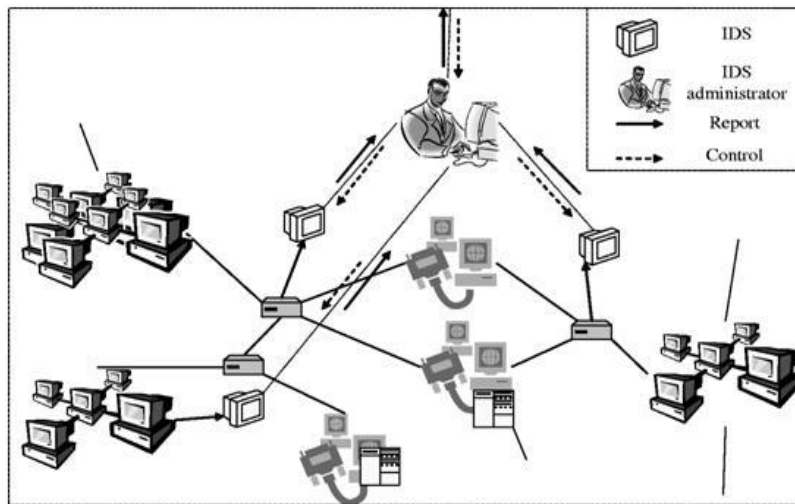
Based on the type of systems the IDS protects

- Network Intrusion Detection System
- Signature based IDS/IPS
- Anomaly based Intrusion Detection System

### **1.1.6 Network Intrusion Detection System**

This system monitors the traffic on individual networks or subnets by continuously analyzing the traffic and comparing it with the known attacks in the library. If an attack is

detected, an alert is sent to the system administration. It is placed mostly at important points in the network so that it can keep an eye on the traffic travelling to and from the different devices on the network. The IDS is placed along the network boundary or between the network and the server. An advantage of this system is that it can be deployed easily and at low cost, without having to be loaded for each system.

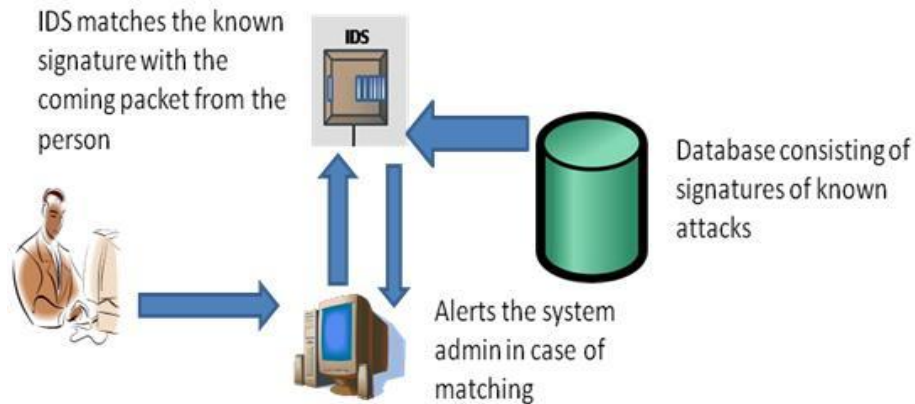


**Figure 1.2 Network Intrusion Detection System**

### 1.1.7 Signature based IDS/IPS

Signature based IDS/IPS is that they operate in much the same way as a virus scanner, by Searching for a known identity or signature.

An IDS can use signature-based detection, relying on known traffic data to analyze potentially unwanted traffic. This type of detection is very fast and easy to configure. However, an attacker can slightly modify an attack to render it undetectable by a signature based IDS. Still, signature-based detection, although limited in its detection capability, can be very accurate. An advantage of this system is it has more accuracy and standard alarms understood by user.



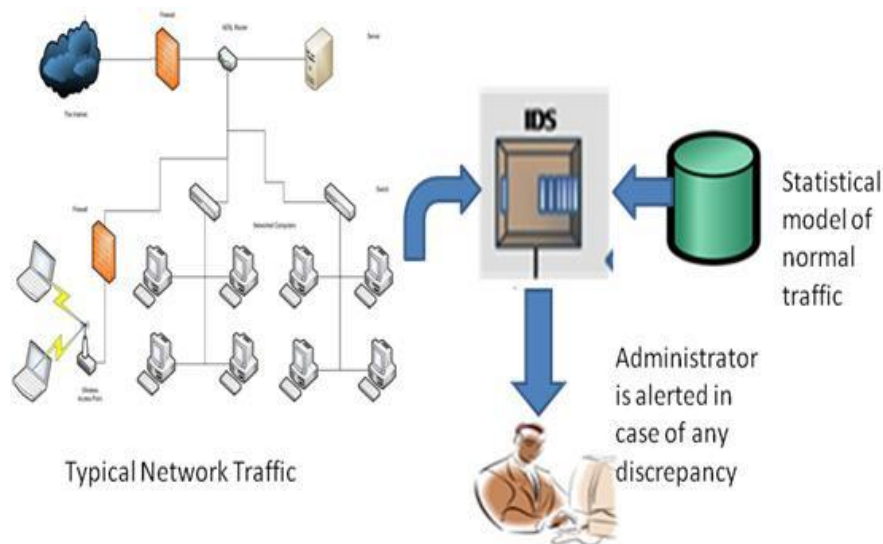
**Figure 1.3 Signature Based IDS/IPS**

### **Limitations**

- It detects the attacks, only if it matches a pattern preloaded in the database
- To detect new attacks it has to be Updated
- If the Network is in traffic, the Signature based IDS/IPS can have a difficult time of inspecting every single packets and forces it to be dropped.

### **1.1.8 Anomaly based Intrusion Detection System**

An Anomaly based Intrusion Detection/Prevention System is a system for detecting computer intrusions by monitoring system activity and classifying it as either normal or anomalous. It consists of a statistical model of a normal network traffic which consists of the bandwidth used, the protocols defined for the traffic, the ports and devices which are part of the network. It regularly monitors the network traffic and compares it with the statistical model. In case of any anomaly or discrepancy, the administrator is alerted. An advantage of this system is they can detect new and unique attacks.



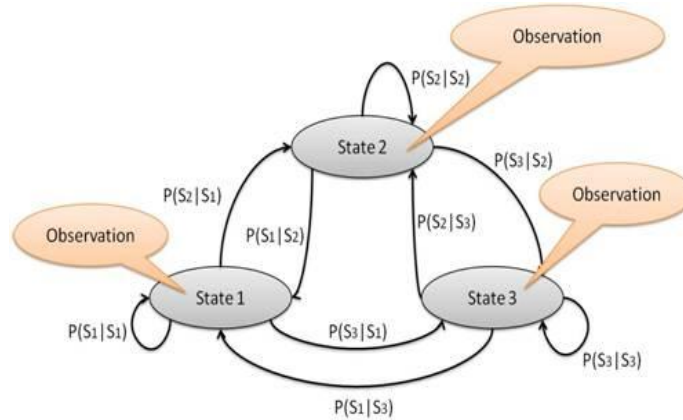
**Figure 1.4 Anomaly Based IDS/IPS**

#### **Limitations:**

- If malicious activity may be looks like normal traffic to the system, it will never send an alarm.
- Major drawback of anomaly based IDS/IPS is that it generates more false positive alarm.

#### **1.1.9 Markov Model**

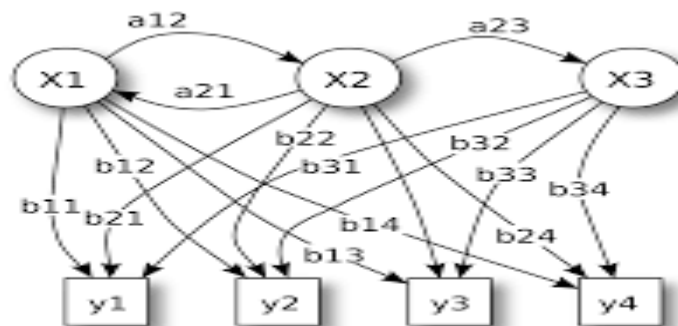
A Markov chain is a set of states that are interconnected through certain transition probabilities, which determine the topology and the capabilities of the model. During a first training phase, the probabilities associated to the transitions are estimated from the normal behaviour of the target system. The detection of anomalies is then carried out by comparing the anomaly score (associated probability) obtained for the observed sequences with a fixed threshold. In the case of a hidden Markov model, the system of interest is assumed to be a Markov process in which states and transitions are hidden. Only the so-called productions are observable.



**Figure 1.5 Markov Model**

### 1.1.10 Hidden Markov Model

An HMM is a doubly stochastic process with an underlying stochastic process that is not observable (it is hidden), but can only be observed through another set of stochastic processes that produce the sequence of observed symbols. The Hidden Markov Model is a finite set of states, each of which is associated with a (generally multidimensional) probability distribution. Transitions among the states are governed by a set of probabilities called transition probabilities. In a particular state an outcome or observation can be generated, according to the associated probability distribution. It is only the outcome, not the state visible to an external observer and therefore states are "hidden" to the outside; hence the name Hidden Markov Model.



**Figure 1.6 Hidden Markov Model**

For HMM completely, following elements are needed.

- The number of states of the model,  $N$ .
- The number of observation symbols in the alphabet,  $M$ . If the observations are continuous then  $M$  is infinite.
- A set of state transition probabilities  $A = \{a_{ij}\}$ .

$$a_{ij} = p\{q_{t+1} = j | q_t = i\}, \quad 1 \leq i, j \leq N,$$

where  $q_t$  denotes the current state.

Transition probabilities should satisfy the normal stochastic constraints,

$$a_{ij} \geq 0, \quad 1 \leq i, j \leq N$$

and

$$\sum_{j=1}^N a_{ij} = 1, \quad 1 \leq i \leq N$$

- A probability distribution in each of the states,  $B = \{b_j(k)\}$ .

$$b_j(k) = p\{o_t = \nu_k | q_t = j\}, \quad 1 \leq j \leq N, \quad 1 \leq k \leq M$$

where  $\nu_k$  denotes the  $k^{th}$  observation symbol in the alphabet, and  $o_t$  the current parameter vector.

Following stochastic constraints must be satisfied.

$$b_j(k) \geq 0, \quad 1 \leq j \leq N, \quad 1 \leq k \leq M \quad \text{and}$$

$$\sum_{k=1}^M b_j(k) = 1, \quad 1 \leq j \leq N$$

If the observations are continuous then we will have to use a continuous probability density function, instead of a set of discrete probabilities. In this case we specify the parameters of the probability density function. Usually the probability density is approximated by a weighted sum of  $M$  Gaussian distributions  $N$ ,

$$b_j(o_t) = \sum_{m=1}^M c_{jm} \mathcal{N}(\mu_{jm}, \Sigma_{jm}, o_t)$$

where,

$$\begin{aligned} c_{jm} &= \text{weighting coefficients} \\ \mu_{jm} &= \text{mean vectors} \\ \Sigma_{jm} &= \text{Covariance matrices} \end{aligned}$$

$c_{jm}$  should satisfy the stochastic constraints,

$$c_{jm} \geq 0, \quad 1 \leq j \leq N, \quad 1 \leq m \leq M$$

and

$$\sum_{m=1}^M c_{jm} = 1, \quad 1 \leq j \leq N$$

- The initial state distribution,  $\pi = \{\pi_i\}$ .  
where,

$$\pi_i = p\{q_1 = i\}, \quad 1 \leq i \leq N$$

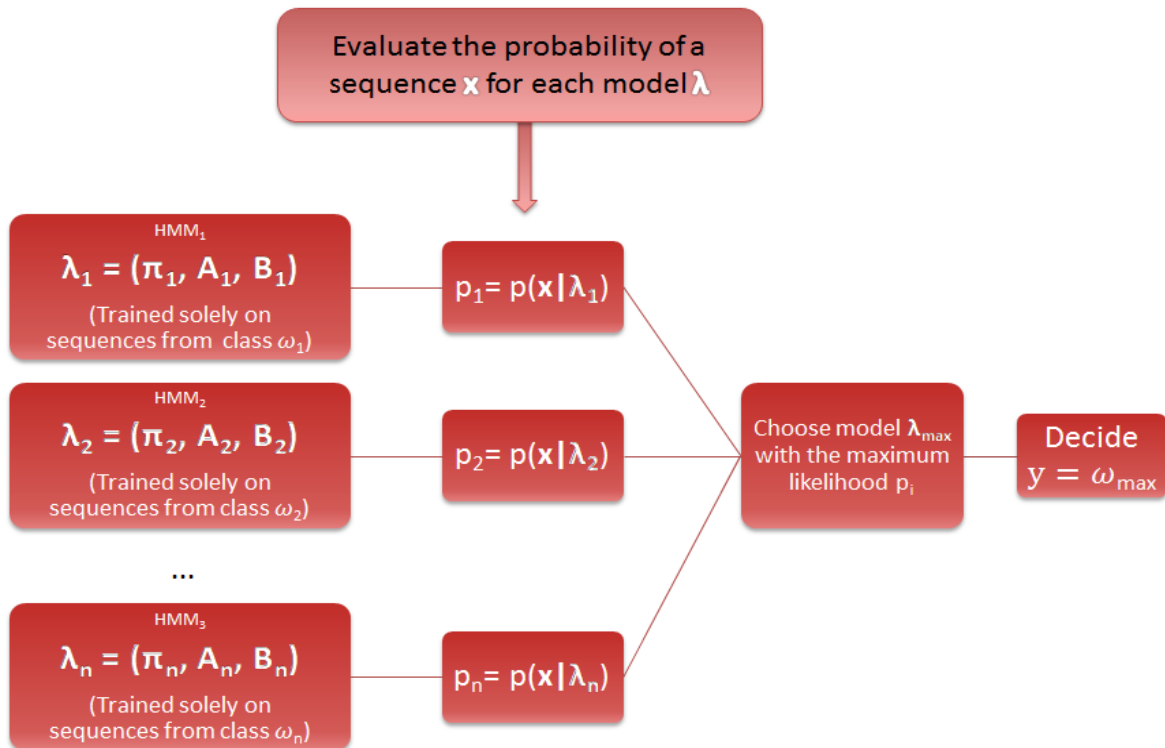
Therefore we can use the compact notation

$$\lambda = (A, B, \pi)$$

to denote an HMM with discrete probability distributions, while

$$\lambda = (A, c_{jm}, \mu_{jm}, \Sigma_{jm}, \pi)$$



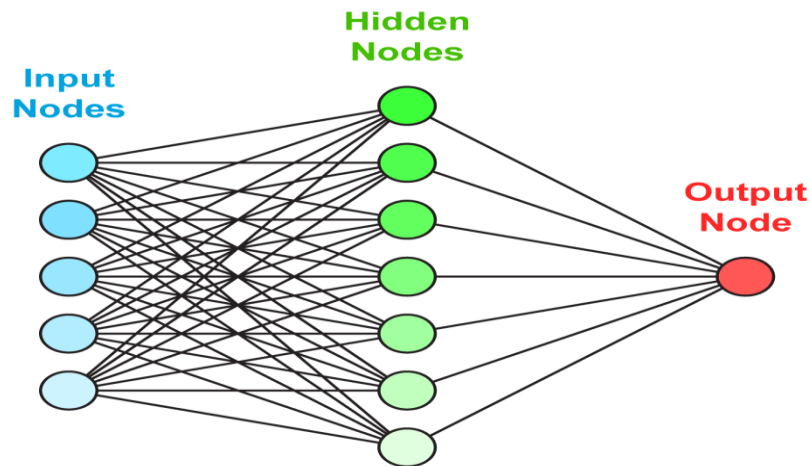


**Figure 1.7 State Transition with Probability**

## 1.2 Neural Network

An Neural Network (NN) is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information. The key element of this paradigm is the novel structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurones) working in unison to solve specific problems. NNs, like people, learn by example. An NN is configured for a specific application, such as pattern recognition or data classification, through a learning process. Learning in biological systems involves adjustments to the synaptic connections that exist between the neurones. This is true of NNs as well.

A technical neural network consists of simple processing units, the neurons, and directed, weighted connections between those neurons. Here, the strength of a connection (or the connecting weight) between two neurons  $i$  and  $j$  is referred to as  $w_{i,j}$



**Figure 1.8 Neural Network**

### **Why Neural Network**

Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. A trained neural network can be thought of as an "expert" in the category of information it has been given to analyse.

Other advantages include:

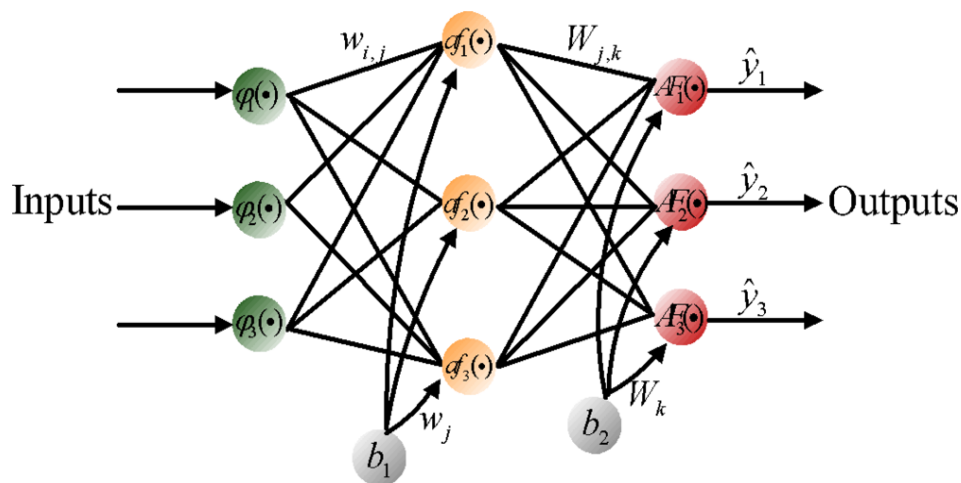
1. Adaptive learning: An ability to learn how to do tasks based on the data given for training or initial experience.
2. Self-Organisation: An NN can create its own organisation or representation of the information it receives during learning time.

3. Real Time Operation: NN computations may be carried out in parallel, and special hardware devices are being designed and manufactured which take advantage of this capability.
4. Fault Tolerance via Redundant Information Coding: Partial destruction of a network leads to the corresponding degradation of performance. However, some network capabilities may be retained even with major network damage.

### 1.2.1 Feed-forward networks

Feed-forward ANNs allow signals to travel one way only; from input to output. There is no feedback (loops) i.e. the output of any layer does not affect that same layer. Feed-forward ANNs tend to be straight forward networks that associate inputs with outputs. They are extensively used in pattern recognition. This type of organisation is also referred to as bottom-up or top-down.

Feedback networks can have signals travelling in both directions by introducing loops in the network. Feedback networks are very powerful and can get extremely complicated. Feedback networks are dynamic; their 'state' is changing continuously until they reach an equilibrium point. They remain at the equilibrium point until the input changes and a new equilibrium needs to be found. Feedback architectures are also referred to as interactive or recurrent, although the latter term is often used to denote feedback connections in single-layer organisations.



**Figure 1.9 Feed Forward Neural Network**

### 1.2.2 Back Propagation Algorithm

In order to train a neural network to perform some task, we must adjust the weights of each unit in such a way that the error between the desired output and the actual output is reduced. This process requires that the neural network compute the error derivative of the weights (**EW**). In other words, it must calculate how the error changes as each weight is increased or decreased slightly. The back propagation algorithm is the most widely used method for determining the **EW**.

The back-propagation algorithm is easiest to understand if all the units in the network are linear. The algorithm computes each **EW** by first computing the **EA**, the rate at which the error changes as the activity level of a unit is changed. For output units, the **EA** is simply the difference between the actual and the desired output. To compute the **EA** for a hidden unit in the layer just before the output layer, we first identify all the weights between that hidden unit and the output units to which it is connected.

We then multiply those weights by the **EAs** of those output units and add the products. This sum equals the **EA** for the chosen hidden unit. After calculating all the **EAs** in the hidden layer just before the output layer, we can compute in like fashion the **EAs** for other layers, moving from layer to layer in a direction opposite to the way activities propagate through the network. This is what gives back propagation its name. Once the **EA** has been computed for a unit, it is straight forward to compute the **EW** for each incoming connection of the unit. The **EW** is the product of the **EA** and the activity through the incoming connection.

The back propagation algorithm trains a given feed-forward multilayer neural network for a given set of input patterns with known classifications. When each entry of the sample set is presented to the network, the network examines its output response to the sample input pattern. The output response is then compared to the known and desired output and the error value is calculated. Based on the error, the connection weights are adjusted.

### 1.2.3 Learning Methods : Supervised learning

Supervised learning which incorporates an external teacher, so that each output unit is told what its desired response to input signals ought to be. During the learning process global information may be required. Paradigms of supervised learning include error-correction learning, reinforcement learning and stochastic learning. An important issue concerning supervised learning is the problem of error convergence, ie the minimisation of error between the desired and computed unit values. The aim is to determine a set of weights which minimises the error. One well-known method, which is common to many learning paradigms is the least mean square (LMS) convergence.

### 1.2.4 Unsupervised learning

Unsupervised learning uses no external teacher and is based upon only local information. It is also referred to as self-organisation, in the sense that it self-organises data presented to the network and detects their emergent collective properties. Paradigms of unsupervised learning are Hebbian learning and competitive learning. From Human Neurones to Artificial Neurones the aspect of learning concerns the distinction or not of a separate phase, during which the network is trained, and a subsequent operation phase. We say that a neural network learns off-line if the learning phase and the operation phase are distinct. A neural network learns on-line if it learns and operates at the same time. Usually, supervised learning is performed off-line, whereas unsupervised learning is performed on-line.

## CHAPTER 2 - LITERATURE SURVEY

### 2.1 Literature Survey on Intrusion Detection System

Chunjie Zhou, Shuang Huang, et al.[1] in this paper they have used an anomaly detection based on multimodel has proposed and intelligent detection algorithms are designed. Classifier based on an intelligent hidden Markov model. A novel multimodel-based anomaly intrusion detection system with embedded intelligence and resilient coordination for the field control system in industrial process automation is designed. In this system, an anomaly detection based on multimodel has proposed, and the corresponding intelligent detection algorithms are designed. Furthermore, to overcome the disadvantages of anomaly detection, a classifier based on an intelligent hidden Markov model, have designed to differentiate the actual attacks from faults. The unique feature of the proposed intelligent intrusion detection system has that it uses complete multiple models of PCS built through the integration of multi domain knowledge to detect system anomaly, and employs HMM models to identify attacks from the sequential anomaly alerts. So in conclusion, the proposed intelligent intrusion detection system can detect the attack from both spatial and temporal aspects. In addition, since our intrusion detection system developed for PCSs takes into account the system knowledge instead of attack signatures, unknown type and new type of attack can also be detected by the proposed IDS. This paper is based on anomaly intrusion detection without consideration of attack knowledge. For the future, a comprehensive intrusion detection system for PCSs, which integrates system knowledge and attack knowledge, will be researched to optimize resources and time.

Al-Jarrah, O. ; Dept. of Comput. Eng., et al.[2] in this paper they have used an intelligent system to maximize the recognition rate of network attacks by embedding the temporal behavior of the attacks into a TDNN neural network structure. The proposed system consists of five modules: packet capture engine, preprocessor, pattern recognition, classification, and monitoring and alert module. This system captures packets in real time using a packet capture engine that presents the packets to a preprocessing stage using two pipes. The preprocessing stage extracts the relevant features for port scan and host sweep attacks, stores the features in a tapped line of a TDNN, and produces outputs that represent possible attack behaviors in a pre-specified number of packets. These outputs are used by the pattern recognition neural networks to recognize the

attacks, which are classified, by the classifier network to generate attack alerts. DARPA data sets are used to evaluate the systems in terms of recognition capability and throughput. Test results show that this system detects all types of attacks much faster than rule based systems such as SNORT.

## **CHAPTER 3 – PROPOSED WORK**

### **Limitations of Signature based IDS**

- It detects the attacks, only if it matches a pattern preloaded in the database
- To detect new attacks it has to be Updated
- If the Network is in traffic, the Signature based IDS/IPS can have a difficult time of inspecting every single packets and forces it to be dropped.

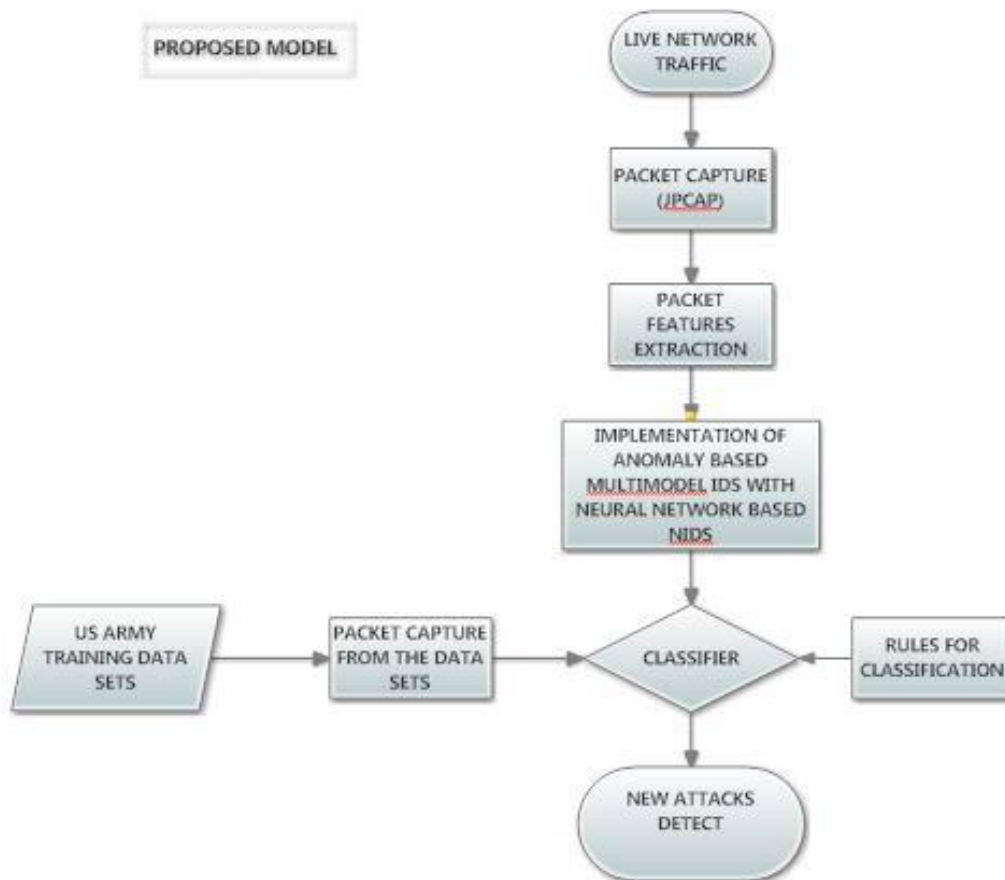
### **Limitations of Anomaly based IDS**

- If malicious activity may be looks like normal traffic to the system, it will never send an alarm.
- Major drawback of anomaly based IDS/IPS is that it generates more false positive alarm.

From the literature survey the Signature based IDS have the limitations of detecting Zero Day Attacks and detect only if it matches a pattern in Data Base. Another one is it can able to detect attacks only if has updated. If the Network is in traffic, the Signature based IDS/IPS can have a difficult time of inspecting every single packet and forces some packets to be dropped.

Anomaly based IDS also have the limitations of generating more false positive alarms. If malicious activity may be looks like normal traffic to the system, it will never send an alarm. So we have planned to maximize the recognition rate of network attacks with intelligent system by embedding the temporal behavior of the attacks into a TDNN neural network structure. To overcome the limitations of anomaly detection, a classifier based on an intelligent hidden Markov model, is used and designed to differentiate the actual attacks from faults. We are proposing a model with combining the Multimodel model based Anomaly IDS with Time Delay Neural Network based NIDS.

### 3.1 PROPOSED MODEL

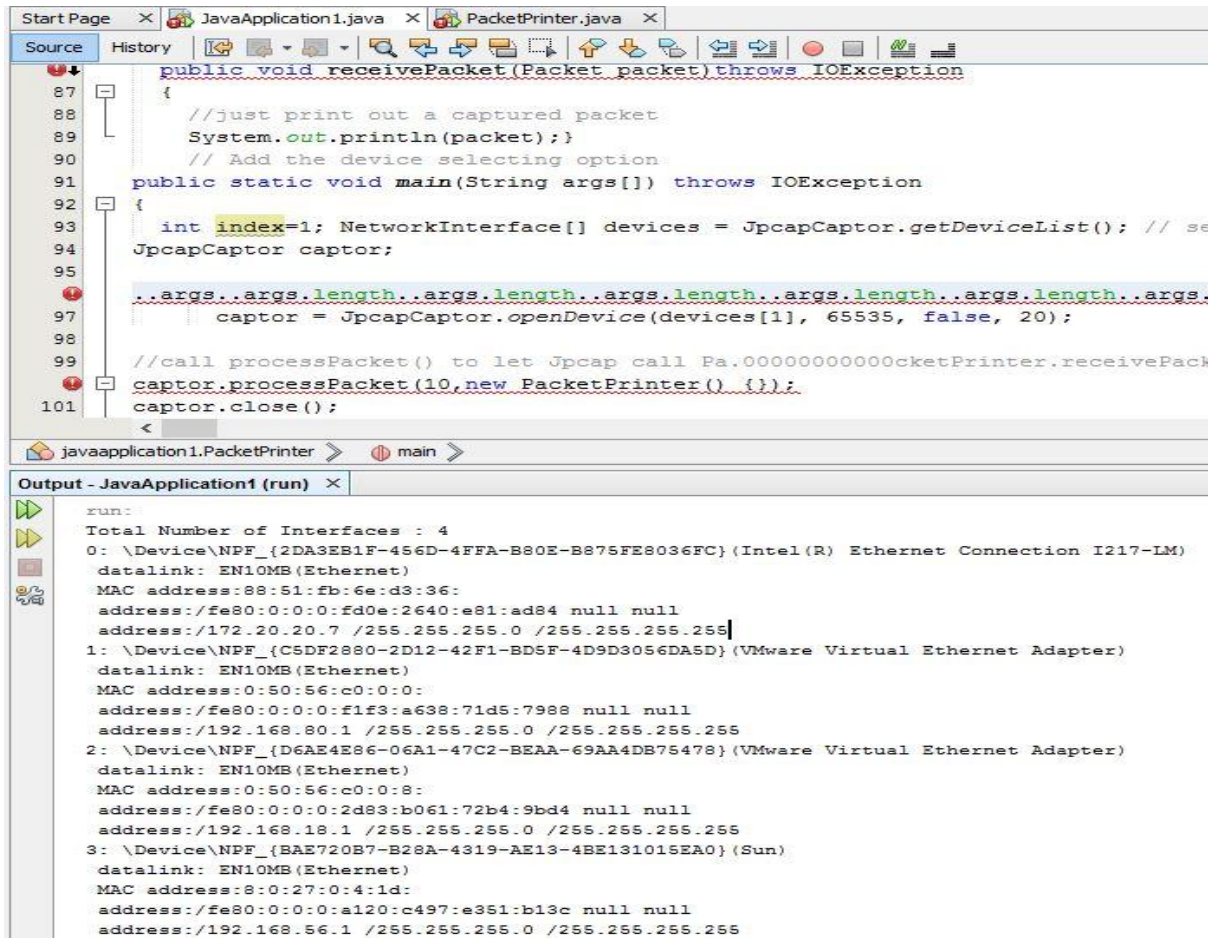


**Figure 1.10 Proposed Model**

- To write a Packet Capture Program using (JPCAP), to capture the real time network traffic
- Captured packets features can be analysed
- Planned to implement the multimodel based Anomaly IDS with Network IDS algorithm using JAVA code and make it to work with actual packets.
- Virtual machine can be used to implement the architecture of multimodal based anomaly IDS with Network based IDS system.
- Then Packet analysis and testing can be done by using the trianing data sets of US army.
- Classification of the packets can be done using the rules which differntiate the malisious and normal packets. With that it will detect the new attacks.



### 3.2 OUTPUT



The screenshot shows an IDE with two tabs: 'JavaApplication1.java' and 'PacketPrinter.java'. The 'PacketPrinter.java' tab is active, displaying the following code:

```

public void receivePacket(Packet packet) throws IOException
{
    //just print out a captured packet
    System.out.println(packet);
    // Add the device selecting option
}

public static void main(String args[]) throws IOException
{
    int index=1; NetworkInterface[] devices = JpcapCaptor.getDeviceList(); // se
    JpcapCaptor captor;

    ..args..args.length..args.length..args.length..args.length..args.length..args.
    captor = JpcapCaptor.openDevice(devices[1], 65535, false, 20);

    //call processPacket() to let Jpcap call Pa.000000000000cketPrinter.receivePack
    captor.processPacket(10, new PacketPrinter(). {});
    captor.close();
}

```

The output window, titled 'Output - JavaApplication1 (run)', shows the following text:

```

run:
Total Number of Interfaces : 4
0: \Device\NPF_{2DA3EB1F-456D-4FFA-B80E-B875FE8036FC} (Intel(R) Ethernet Connection I217-LM)
   datalink: EN10MB(Ethernet)
   MAC address:88:51:fb:6e:d3:36:
   address://fe80:0:0:0:fd0e:2640:e81:ad84 null null
   address://172.20.20.7 /255.255.255.0 /255.255.255.255
1: \Device\NPF_{C5DF2880-2D12-42F1-BD5F-4D9D3056DA5D} (VMware Virtual Ethernet Adapter)
   datalink: EN10MB(Ethernet)
   MAC address:0:50:56:c0:0:0:
   address://fe80:0:0:0:f1f3:a638:71d5:7988 null null
   address://192.168.80.1 /255.255.255.0 /255.255.255.255
2: \Device\NPF_{D6AE4E86-06A1-47C2-BEAA-69AA4DB75478} (VMware Virtual Ethernet Adapter)
   datalink: EN10MB(Ethernet)
   MAC address:0:50:56:c0:0:0:8:
   address://fe80:0:0:0:2d83:b061:72b4:9bd4 null null
   address://192.168.18.1 /255.255.255.0 /255.255.255.255
3: \Device\NPF_{BAE720B7-B28A-4319-AE13-4BE131015EA0} (Sun)
   datalink: EN10MB(Ethernet)
   MAC address:8:0:27:0:4:1d:
   address://fe80:0:0:0:a120:c497:e351:b13c null null
   address://192.168.56.1 /255.255.255.0 /255.255.255.255

```

**Figure 1.11 Packet Captured Output**

- Initially the connections has been made between the network traffic and Capturing tool using the interface datalink (Ethernet).
- Then the real time network packets were captured and save the packets in a file.
- After that read the captured packets from the file.
- Then sent the saved packets through the network interface.
- Packet features like Source IP, Destination IP, frames, Port, Mac Address, format, Protocol type, Datalink, Interface device name has been extracted

The screenshot shows an IDE with two tabs: 'NeuralNetwork.java' and 'JavaApplication1.java'. The 'Source' view displays the code for 'NeuralNetwork.java', which includes a loop for testing the network. The code sets inputs, calls 'feedForward()', and checks for success. The 'Output' view shows the results of running 'JavaApplication1' multiple times, displaying input sequences, success/failure status, and the total number of tests completed (465).

```

179         }else{
180             inputs[i] = 0.0;
181         }
182     } // i
183
184     feedForward();
185
186     } // Enter another number into this sample sequence.
187
188     if((index > OUTPUT_NEURONS - 2) && (successful == true)){
189         // If the random sequence happens to be in the correct order, the network reports success.
190         System.out.println("Success.");
191         System.out.println("Completed " + test + " tests.");
192         break;
193     }else{
194         System.out.println("Failed.");
195         if(test > MAX_TESTS){
196             System.out.println("Completed " + test + " tests with no success.");
197             break;

```

Output:

```

JavaApplication1 (run) #6 x JavaApplication1 (run) #9 x JavaApplication1 (run) #10 x
(0) 0.042 0.020 0.101 0.762 0.032 0.241
(1) Failed.

(0) 0.042 0.020 0.101 0.762 0.032 0.241
(2) Failed.

(0) 0.034 0.019 0.119 0.764 0.030 0.231
(4) Failed.

(0) 0.042 0.020 0.102 0.764 0.032 0.241
(3) 0.239 0.038 0.188 0.214 0.041 0.278
(3) 0.206 0.038 0.205 0.238 0.042 0.277
(3) 0.210 0.038 0.201 0.237 0.042 0.278
(3) 0.210 0.038 0.201 0.237 0.042 0.278
(4) Success.
Completed 465 tests.
BUILD SUCCESSFUL (total time: 0 seconds)

```

**Figure 1.12 Neural Network Algorithm Output**

### Input Data to the training TDNN algorithm:

- private static final int MAX\_SAMPLES = 4
- private static final int INPUT\_NEURONS = 6
- private static final int HIDDEN\_NEURONS = 3
- private static final int OUTPUT\_NEURONS = 6
- private static final int CONTEXT\_NEURONS = 3
- private static final double LEARN\_RATE = 0.2
- private static final int TRAINING\_REPS = 2000

- For the given input to training the time delay neural network, neuron 6, max samples 4, hidden neuron 6, output neuron 6 . learn rate 0.2 and iteration 2000.
- Output shows that it has completed 465 tests for 2000 iterations.

## CHAPTER 4 - CONCLUSION

### 4.1 Conclusion

Virtual machine was used to implement the architecture of multimodal based anomaly IDS with Network based IDS system. Captured the packets in real time network traffic using the (JPCAP). Packet features like Source IP, Destination IP, frames, Port, Mac Address, format, Protocol type, Datalink, interface device name are extracted and analyzed.. Done the coding for hidden markov model and time delay neural network algorithm. The coded TDNN algorithm has been iterated for training the model. Have done the implementation of both the proposed algorithms of multimodal based anomaly IDS with Network based IDS system using JAVA code and to work with actual captured packets. Then the Packet analysis and testing have done with the training data sets of US army. With that it can detect the new attacks.

### References

- [1] Chunjie Zhou, Shuang Huang, Naixue Xiong, Senior Member, IEEE, Shuang-Hua Yang, Senior Member, IEEE, Huiyun Li, Yuanqing Qin, and Xuan Li., Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation, IEEE Transactions On Systems, Man, And Cybernetics: Systems. Year: 2015, Volume: PP, Issue: 99 , DOI: 10.1109/TSMC.2015.2415763
- [2] Al-Jarrah, O. ; Dept. of Comput. Eng., Jordan Univ. of Sci. & Technol., Irbid, Jordan ; Arafat, A. , Network Intrusion Detection System Using Attack Behavior Classification, 5th International Conference on Information and Communication Systems (ICICS), 2014.

## Reference Sites

- [www.cisco.com](http://www.cisco.com)
- [www.snort.com](http://www.snort.com)
- [www.cyberdefencemagazine.com](http://www.cyberdefencemagazine.com)
- [www.symantec.com](http://www.symantec.com)
- [www.jpCaptutorial.com](http://www.jpCaptutorial.com)
- [www.neuralnetwork.com](http://www.neuralnetwork.com)

## Events Participated

- Attended the five days Programme with demo workshop on the topic of " Programme on Digital Forensics for Indian banks" Organized by Institute for Development and research in banking Technology from May 25-29, 2015.
- Participated and done Presentation on the topic of “ Recent Trends in Intrusion Detection/Prevention Systems “ in the Second Annual Summer Research Symposium held at TIFR Centre for Interdisciplinary Sciences, Hyderabad on 24<sup>th</sup> June, 2015