Comparison between Conventional Network and ANN with Case Study

Souvik Paul[1], Digbijay Guha[2], Atrayee Chatterjee[3], Samarth Metha[4], Ayushi Shah[5]

[1,2] Assistant Professor, BCA Department of The Heritage Academy, West Bengal, India
[3] Lecturer, BCA Department of The Heritage Academy, West Bengal, India
[4, 5] Student, BCA Department of The Heritage Academy, West Bengal, India

---***---

Abstract – *Ad-Hoc Networks are inherently self-forming, self-arranging and their nodes are free to move arbitrarily and organize themselves at random. Router is a networking device that sends messages or data packets between computer networks. Network Bridge is a computer networking device which makes a single combined network from multiple communication networks or network segments. Repeater is an electronic device which receives a signal and retransmits it. Artificial Neural Networks are computing systems inspired by the Biological Neural Networks that constitute animal brains. This paper aims at achieving a comparative study among Artificial Neural Network, Ad-Hoc Networks, Router, Bridge, and Repeater. On the basis of that a case study is generated to test the validation of these.*

Key Words: Artificial Neural Network, Ad-Hoc Network, Router, Bridge, Repeater

1. INTRODUCTION

Ad-Hoc Wireless Networks are inherently self-forming, self-arranging and self-administering. The nodes are free to move arbitrarily and organize themselves at random. The biggest challenge in these kinds of networks is finding the path between the communication end points of nodes that are movable. Because of restricted transmission range of wireless interfaces, the communication traffic has to be extended over a number of intermediate nodes to facilitate the communication between two nodes. Thus, these kinds of networks are also called as multi-hop ad-hoc networks. Every node acts as both, a host and as a router.

The rapid development in ad hoc technology is widely used in portable computing such as laptop, mobile phone used to access the web services, telephone calls when the user are in travelling. Development of self-organizing network decreases the communication cost. The growth of 4G technologies enhances anytime, anywhere, anyhow communication in ad hoc network. Ad hoc network is simple to design and install. The ad hoc networks are self-forming, self-maintaining, self-healing architecture. The challenges are, no fixed access point, dynamic network topology, contrary environment and irregular connectivity. Ad hoc network immediately forms and accommodate the modification and limited power.
The limitation associated with wireless devices is the power constraint of the nodes i.e. each node has only limited battery power which should be used judiciously for the node to survive longer. The principle behind ad hoc network is multi-hop relaying. The use of ad hoc voice communication was used in many ancient/tribal societies with the help of a string of repeaters of drums, trumpets, or horns.

The security issue in ad hoc network is dynamic topology, bandwidth, small device size and limited battery life. Due to the dynamic nature, it is difficult to maintain secured transmission in the network (Papadimitratos and Haas, 2002). The ad hoc network does not depend on any pre-existing infrastructure so that the node can leave and join the network in such a situation where security may fall down. Two types of attack occur in ad hoc network, first is passive attack, this attack does not change the transmitted data in the network. But, it can allow unauthorized user to discover the message. Second, is active attack, it is a severe attack and prevents the message flow between the node in the network. It may allow the unauthorized user to modify the message. Dropped packet, battery drained, bandwidth consumption, unreliable packets, delay, connection break and false routing can identify the malicious node.

With the increased number of lightweight devices as well as evolution in wireless communication, the ad hoc networking technology is gaining effort with the increasing number of widespread applications. Ad hoc networking can be used anytime, anywhere with limited or no communication infrastructure. The preceding infrastructure is fancy or annoying to use. The ad hoc network architecture can be used in real time business applications, corporate companies to increase the productivity and profit.

The ad hoc networks can be classified according to their application as Mobile Ad hoc Network (MANET) that is a self-arranging infrastructure less network of mobile devices communicated through wireless link. Vehicular Ad hoc Network (VANET) uses travelling cars as nodes in a network to create a mobile network. Wireless Sensor Network (WSN) consists of autonomous sensors to control the environmental actions.

The importance of ad hoc network has been highlighted in many fields which are described below:

- **Military Arena:** An ad hoc networking will allow the military battleground to maintain an information network among the soldiers, vehicles and headquarters (Bangnan et al., 2003).

- **Provincial Level:** Ad hoc networks can build instant link between multimedia network using notebook computers or palmtop computers to spread and share information among participants (e.g. Conferences).
- **Personal Area Network:** A personal area network is a short range, localized network where nodes are usually associated with a given range.
- **Industry Sector:** Ad hoc network is widely used for commercial applications. Ad hoc network can also be used in emergency situation such as disaster relief. The rapid development of non-existing infrastructure makes the ad hoc network easily to be used in emergency situation.
- **Bluetooth:** Bluetooth can provide short-range communication between the nodes such as a laptop and mobile phone.

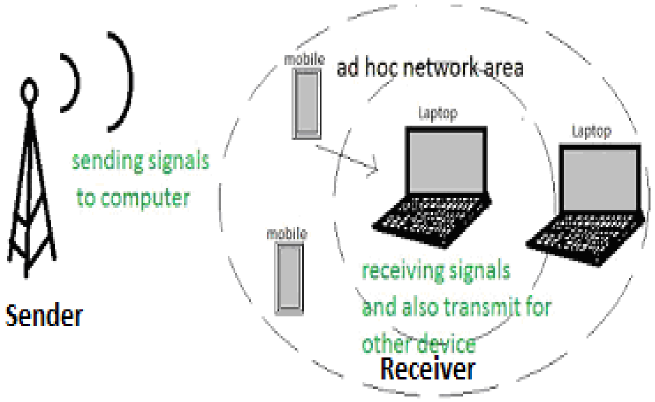

Fig -1: Wireless Ad Hoc Network

1.1 Network Planning

Network planning is concerned with the cost-effective deployment of a communication infrastructure to provide adequate coverage, capacity, and quality for end user services. This task is traditionally viewed as an operation for "high-end" networks, examples being 3G cellular networks. Once deployed, the infrastructure in such networks is relatively static. In this work, our objective is to investigate more dynamic service provisioning in more "low-end" networks, specifically wireless ad hoc networks. The defining characteristic of ad hoc networks is their loose and self-organized structure, as opposed to the centralized structure in cellular networks. Two example application scenarios, where techniques in this paper might be applicable, are community wireless networks, which are fixed wireless ad hoc networks formed by wireless LAN devices in a neighborhood, and ad hoc networks formed by the laptop computers of participants in a meeting. Abstractly, the problem of network planning considered in this paper is the problem of allocating physical and link layer resources, or supplies, to minimize a cost function while fulfilling certain transport and application layer communication demands.

1.2 Routing in Ad Hoc Wireless Networks

As the nodes in a wireless ad hoc network can be connected in a dynamic and arbitrary manner, the nodes themselves must behave as routers and take part in discovery and maintenance of routes to other nodes in the network.

The goal of a routing algorithm is to devise a scheme for transferring a packet from one node to another. One challenge is to define/choose which criteria to base the routing decisions on. Examples of such criteria include hop length, latency, and bandwidth and transmission power.

Some challenges in designing a routing protocol for ad hoc wireless networks, and a brief overview of these is given below:

- **Mobility:** The network needs to adapt to rapid changes in the topology due to the movement of the nodes, or the network as a whole.
- **Resource Constraints:** Nodes in a wireless network typically have limited battery and processing power, and these resources must be managed optimally by the routing protocol.
- **Error-Prone Channel State:** The characteristic of the links in a wireless network typically varies, and these calls for an interaction between the routing protocol and the MAC protocol to, if necessary, find alternate routes.
- **Hidden Terminal Problem:**

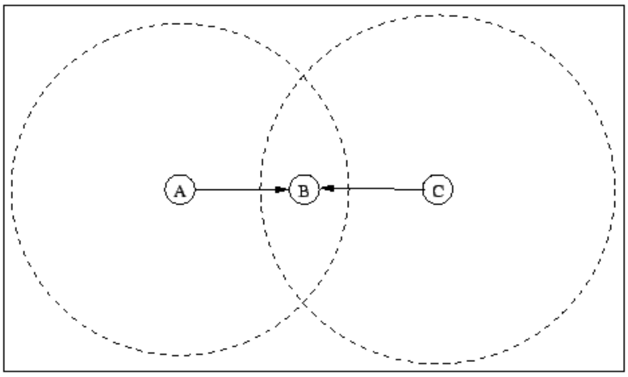

Fig -2: The Hidden Terminal Problem

Node A and C try and communicate with B simultaneously, but cannot detect the interference.

- **Exposed Terminal Problem:**

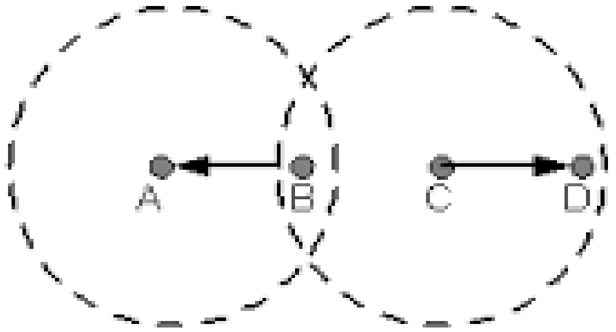

Fig -3: The Exposed Terminal Problem

Consider a topology similar to that of Fig-2, but added a node D only reachable from node C. Furthermore, suppose node B communicates with node A, and node C wants to transmit a packet to node D. During the transmission between node B and node A, node C senses the channel as busy. Node C falsely conclude that it may not send to node D, even though both the transmissions (i.e., between node B and node A, and between node C and node D) would succeed. Bad reception would only occur in the zone between node B and node C, where neither of the receivers is located. This problem is often referred to as ``the exposed terminal problem''. Both the hidden and the exposed terminal problem cause significant reduce of network throughput when the traffic load is high.

1.3 Table-driven (Proactive) Routing

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network.

The main disadvantages of such algorithms are:

- Respective amount of data for maintenance.
- Slow reaction on restructuring and failures.

Examples of proactive algorithms are:

- Optimized Link State Routing Protocol (OLSR) RFC 3626, RFC 7181.
- Babel RFC 6126
- Destination Sequence Distance Vector (DSDV)
- DREAM
- B.A.T.M.A.N.

1.4 On-demand (Reactive) Routing

This type of protocol finds a route on demand by flooding the network with Route Request packets.

The main disadvantages of such algorithms are:

- High latency time in route finding.
- Excessive flooding can lead to network clogging.

Examples of on-demand algorithms are:

- ABR - Associativity-Based Routing
- Ad hoc On-demand Distance Vector(AODV) (RFC 3561)
- Dynamic Source Routing (RFC 4728)
- Flow State in the Dynamic Source Routing
- Power-Aware DSR-based

1.5 Hybrid (both Proactive and Reactive) Routing

This type of protocol combines the advantages of proactive and reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice of one or the other method requires predetermination for typical cases.

The main disadvantages of such algorithms are:

- Advantage depends on number of other nodes activated.
- Reaction to traffic demand depends on gradient of traffic volume.

Examples of hybrid algorithms are:

- ZRP (Zone Routing Protocol)
- ZRP uses IARP as pro-active and IERP as reactive component.
- ZHLS (Zone-based Hierarchical Link State Routing Protocol)

1.6 Hierarchical Routing Protocols

With this type of protocol the choice of proactive and of reactive routing depends on the hierarchic level in which a node resides. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding on the lower levels. The choice for one or the other method requires proper attributation for respective levels.

The main disadvantages of such algorithms are:

- Advantage depends on depth of nesting and addressing scheme.
- Reaction to traffic demand depends on meshing parameters.

Examples of hierarchical routing algorithms are:

- CBRP (Cluster Based Routing Protocol)
- FSR (Fisheye State Routing protocol)
- Order One Network Protocol; Fast logarithm-of-2 maximum times to contact nodes. Supports large groups.
- ZHLS (Zone-based Hierarchical Link State Routing Protocol)

2. ROUTER

A router is a networking device that sends messages or data packets between computer networks. Routers perform the traffic directing functions on the Internet. Message or data packet is sent from one router to another router through the networks that constitute the internetwork until it reaches its destination node from the origination node.

A router is connected to two or more data lines from different networks. When a message or data packet comes in on one of the data lines, the router reads the network address information in the message or data packet to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network. This creates an overlay internetwork.

Common types of routers are home and small office routers that simply pass IP packets between the computers and the Internet. An example of a router is the owner's cable or DSL router, which connects to the Internet through an Internet Service Provider (ISP). More complicated routers, such as enterprise routers, connect large business or ISP networks up to the powerful core routers that forward data at high speed along the optical fiber lines of the Internet backbone. Commonly routers are hardware devices, but software-based routers also available.

A router has two stages of operation called planes:

- **Control Plane:** A router maintains a routing table that contains which route is to be used to forward a data packet, and through which physical interface connection. It does these operations using internal pre-configured directives, called static routes, or by learning routes using a dynamic routing protocol. Static and dynamic routes are stored in the Routing Information Base (RIB). The control-plane logic then strips non-essential directives from the RIB and makes a Forwarding Information Base (FIB) for the forwarding-plane.
- **Forwarding Plane:** The router forwards data packets between incoming and outgoing interface connections. It routes them to the correct network type using information that the data packet header contains. It uses data recorded in the routing table control plane.

Fig -4: Router

2.1 Types of Router

- **Access Router:** Access Routers are placed at customer sites such as branch offices that do not need hierarchical routing of their own. Typically, they are optimized for low cost. Examples of such routers are 'small office/home office' (SOHO) models .Some SOHO routers are capable of running alternative free Linux-based firmware like Tomato, OpenWrt or DD-WRT.
- **Distribution Router:** Distribution Routers combine traffic from multiple access routers, either at the same site, or from multiple sites to a major enterprise location. Distribution routers are often responsible for enforcing quality of service across a wide area network (WAN), so they may have sizeable memory installed, multiple WAN interface connections, and substantial onboard data processing routines. They may also give connectivity to groups of file servers or other external networks.
- **Core Router:** In enterprises, a Core Router may provide a "collapsed backbone" which interconnects distribution tier routers from many buildings of a campus, or huge enterprise locations. They tend to be optimized for high bandwidth, but lack some of the features of edge routers.
- **Edge Router:** It is also called a Provider Edge Router which is positioned at the edge of an ISP network. The router uses External BGP to EBGP routers in other ISPs, or a large enterprise Autonomous System.
- **Subscriber Edge Router:** It is also called a Customer Edge Router which is located at the edge of the subscriber's network. It also uses EBGP to its provider's Autonomous System. It is typically used in an organization.
- **Inter-Provider Border Router:** It interconnects ISPs. It is a BGP router that maintains BGP sessions with other BGP routers in ISP Autonomous Systems.
- **Voice/Data/Fax/Video Processing Routers:** These types of routers are commonly referred to as Access Servers or Gateways. These devices are used to direct and process voice, data, video and fax traffic on the Internet. Since 2005, most long-distance phone calls have been processed as IP traffic (VOIP) through a voice

gateway. With the advent of the Internet, usages of access server type routers are expanded. Firstly it is used with dial-up access and another resurrection with voice phone service.

- **Multilayer Switches:** Larger networks commonly use Multilayer Switches. Layer 3 devices are used to interconnect multiple subnets within the same security zone. Higher layer switches are used to do filtering, translation, load balancing or other higher level functions especially between zones.

3. BRIDGE

A Network Bridge is a computer networking device which makes a single combined network from multiple communication networks or network segments. This task is called Network Bridging. Bridging is different from routing. Routing allows multiple different networks to communicate independently while remaining separate. In the OSI model, bridging is performed in the first two layers (Physical Layer, Data Link Layer), below the Network Layer (layer 3). If one or more segments of the bridged network are wireless the device is known as a Wireless Bridge and the task is known as as Wireless Bridging.

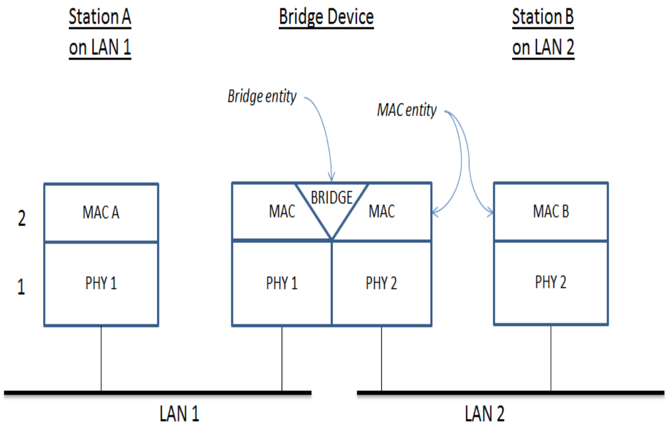

Fig -5: A Bridge connecting two LAN segments

3.1 Types of Bridging

- **Simple Bridging:** A simple bridge connects two network segments, typically by operating transparently and deciding on a frame-by-frame basis whether or not to forward from one network to the other. A store and forward technique is typically used so, during forwarding, the frame integrity is verified on the source network and CSMA/CD delays are accommodated on the destination network. Contrary to repeaters that simply extend the maximum span of a segment, bridges only forward frames that are required to cross the bridge. Additionally, bridges reduce collisions by partitioning the collision domain.
- **Multiport Bridging:** A multiport bridge connects multiple networks and operates transparently to decide on a frame-by-frame basis whether and where to forward traffic. Like the simple bridge, a multiport bridge typically uses store and forward operation. The multiport bridge function serves as the basis for network switches.
- **Transparent Bridging:** A transparent bridge uses a forwarding database to send frames across network segments. The forwarding database starts empty. Entries in the database are built as the bridge receives frames. If an address entry is not found in the forwarding database, the frame is flooded to all other ports of the bridge, flooding the frame to all segments except the one from which it was received. By means of these flooded frames, the destination network will respond and a forwarding database entry will be created.
- **Source Route Bridging:** Source route bridging is used on token ring networks. The operation of the bridge is simpler and much of the bridging functions are performed by the end systems, particularly the sources, giving rise to its name. The source-route bridging algorithm was developed by IBM and was proposed to the IEEE 802.5 committee as the means to bridge between all the LANS.
- **Source Route Transparent Bridging:** It is a hybrid of source routing and transparent bridging. It allows source routing and transparent bridging to coexist on the same bridged network by using source routing with hosts that support it and transparent bridging otherwise.

4. REPEATER

In telecommunications, a Repeater is an electronic device which receives a signal and retransmits it. Repeaters are used to enlarge transmissions so that the signal can cover longer distances or be received on the other side of an obstruction. Some types of repeaters broadcast an identical signal, but modify its transmission method.

A wireless repeater or wireless range extender takes an existing signal from a wireless router or wireless access point and rebroadcasts it for creating another network. When two or more hosts have to be connected with one another and the distance is too lengthy for a direct connection to be established, a wireless repeater is used to link the gap.

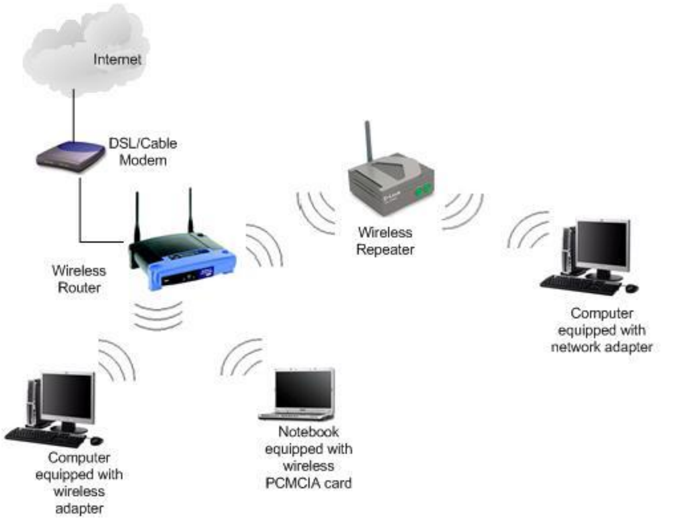
Internet
DSL/Cable Modem
Wireless Router
Wireless Repeater
Computer equipped with network adapter
Computer equipped with wireless adapter
Notebook equipped with wireless PCMCIA card

Fig -6: Repeater

4.1 Types of Repeater

- **Telephone Repeater:** This is used to enhance the range of telephone signals in a telephone line. These are most commonly used in trunk lines that carry long distance calls. Telephone repeaters were the first type of repeater and were some of the first applications of amplification. The development of telephone repeaters between 1900 and 1915 made long distance phone service possible. However the majority telecommunications cables are now fiber optic cables which use optical repeaters.

  - **Submarine Cable Repeater:** It is a type of telephone repeater which is used in underwater submarine telecommunications cables.

- **Optical Communication Repeater:** It is used to enhance the range of signals in a fiber optic cable. Digital information travels through a fiber optic cable in the form of short pulses of light. An optical communications repeater usually consists of a phototransistor which converts the light pulses to an electrical signal, an amplifier to amplify the power of the signal, an electronic filter which reshapes the pulses and a laser which converts the electrical signal to light again and sends it out the other fiber.
- **Radio Repeater:** It is used to enlarge the range of coverage of a radio signal. A radio repeater usually consists of a radio receiver connected to a radio transmitter. The received signal is enlarged and retransmitted, often on another frequency, to provide coverage beyond the obstacle. Usage of a duplexer can allow the repeater to use one antenna for both receive and transmit simultaneously.

  - **Broadcast Relay Station or Rebroadcastor or Translator:** It is a repeater used to expand the coverage of a radio or television broadcasting station. It consists of a secondary radio or television transmitter. The signal from the main transmitter often comes over leased telephone lines or by microwave relay.
  - **Microwave Relay:** It is a point-to-point telecommunications link which consists of a microwave receiver that receives information over a beam of microwaves from another relay station in line-of-sight distance, and a microwave transmitter which passes the information on to the next station over another beam of microwaves. Networks of microwave relay stations transmit telephone calls, television programs, and computer data from one city to another over continent-wide areas.
  - **Passive Repeater:** It is a microwave relay which consists of a flat metal surface to reflect the microwave beam in another direction. It is used to get microwave relay signals over hills and mountains when it is not required to enlarge the signal.
  - **Cellular Repeater:** It is a radio repeater to increase cell phone reception in a limited area. The device works like a small cellular base station, with a directional antenna to receive the signal from the nearest cell tower, an amplifier, and a local antenna to rebroadcast the signal to nearby cell phones. It is often used in downtown office buildings.
  - **Digipeater:** It is a repeater node in a packet radio network. It performs a store and forward function, passing on packets of information from one node to another.

5. ANN

Artificial neural networks or connectionist systems are computing systems inspired by the biological neural networks that constitute animal brains. Such systems learn (progressively improve performance) to do tasks by considering examples, generally without task-specific programming. For example, in image recognition, they might learn to identify images that contain cats by analyzing example images that have been tagged "cat" or "no cat" and using the analytic results to identify cats in untagged images. They have found most use in applications difficult to express in a traditional computer algorithm using rule-based programming.

An ANN is based on a collection of connected units called artificial neurons, (analogous to axons in a biological brain). Each connection (synapse) between neurons can transmit a unidirectional signal with an activating strength that varies with the strength of the connection. If the combined incoming signals (from potentially many transmitting neurons) are strong enough, the receiving (postsynaptic) neuron activates and propagates a signal of to downstream neurons connected to it.

Typically, neurons are organized in layers. Signals travel from the first (input), to the last (output), possibly after traversing the layers multiple times. In addition to receiving and sending signals, units may have state, generally represented by real numbers, typically between 0 and 1. A threshold or limiting function may govern each connection and neuron, such that the signal must exceed the limit before propagating.

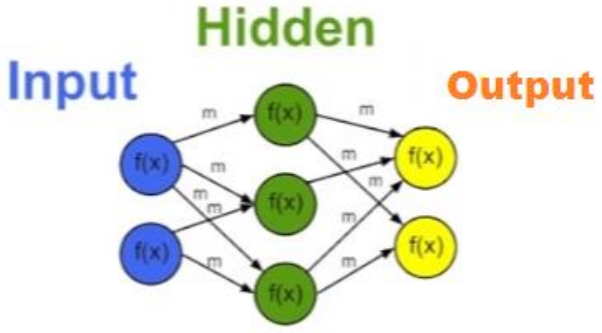

Fig -7: Basic ANN Layers

The original goal of the neural network approach was to solve problems in the same way that a human brain would. Over time, the goal shifted to matching specific mental abilities, leading to deviations from biology such as back propagation.

Neural networks have been used on a variety of tasks, including computer vision, speech recognition, machine translation, social network filtering, playing board and video games, medical diagnosis and in many other domains.
As of 2017, neural networks typically have a few thousand to a few million units and millions of connections. Their computing power is similar to a worm brain several orders of magnitude simpler than a human brain. Despite this, they can perform functions (e.g., playing chess) that are far beyond a worm's capacity.

5.1 ANN Algorithm

The Ann Algorithm has precisely three different elements: the input node, the output node and the hidden node.

1) Back Propagation:

The entire algorithm in ANN is based on Back Propagation meaning that the result of one step has to be back tracked to its original roots to justify and check if there are any errors. These nodes functions on the strength of connection. Stronger the strength, higher is the chances that an error might pop up.

Precisely speaking, this is the diagrammatic representation of a neural network. The input and the output nodes are given, and the hidden nodes are those functions that generate the actual predicted output.

2) Error Handling:

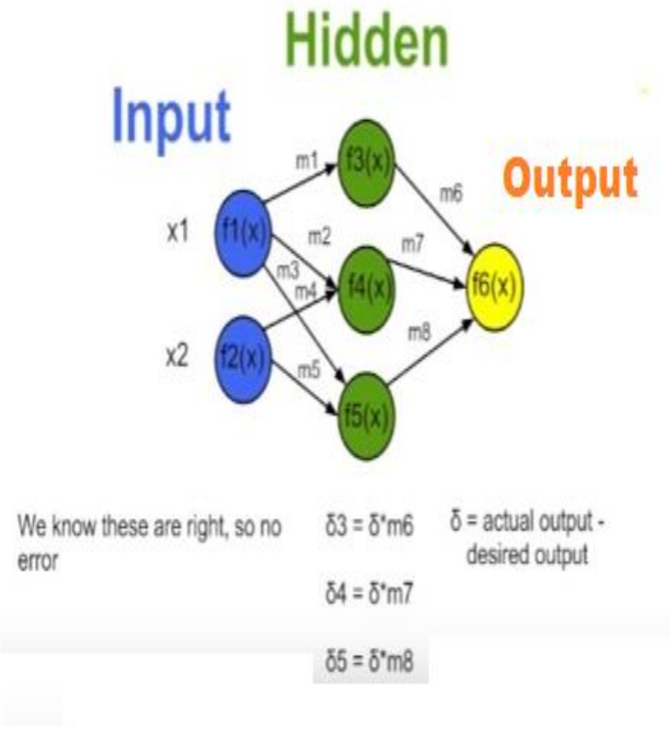

Fig -8: ANN Layers with Parameters

This image signifies the occurrence of the error which is represented by delta. This delta as we see from the diagram is back tracked to its initial roots to check for the occurrence of the error. More the strength and connectivity higher the chances are for an error to creep in.

5.2 A Case Study

A case study based on breast cancer data set that was available on Kaggle to predict the form of Cancer that an individual was having, i.e. Malignant or Benign.

A description about the Data set is given below.

"Features are computed from a digitized image of a fine needle aspirate (FNA) of a breast mass. They describe characteristics of the cell nuclei present in the image. n the 3-dimensional space is that described in: [K. P. Bennett and O. L. Mangasarian: "Robust Linear Programming Discrimination of Two Linearly Inseparable Sets", Optimization Methods and Software 1, 1992, 23-34].

Attribute Information:

1) ID number 2) Diagnosis (M = malignant, B = benign)
3-32)

Ten real-valued features are computed for each cell nucleus:

a) radius (mean of distances from center to points on the perimeter) b) texture (standard deviation of gray-scale values) c) perimeter d) area e) smoothness (local variation in radius lengths) f) compactness (perimeter^2 / area - 1.0) g) concavity (severity of concave portions of the contour) h) concave points (number of concave portions of the contour) i) symmetry j) fractal dimension ("coastline approximation" - 1)

The mean, standard error and "worst" or largest (mean of the three largest values) of these features were computed for each image, resulting in 30 features. For instance, field 3 is Mean Radius, field 13 is Radius SE, and field 23 is Worst Radius.
All feature values are recoded with four significant digits.
Missing attribute values: none
Class distribution: 357 benign, 212 malignant"

So from the result set neural net on R, with a configuration of 30-8-2-1 to get the desired result and I got an MSE of 0 signifying the perfect execution of the Network.

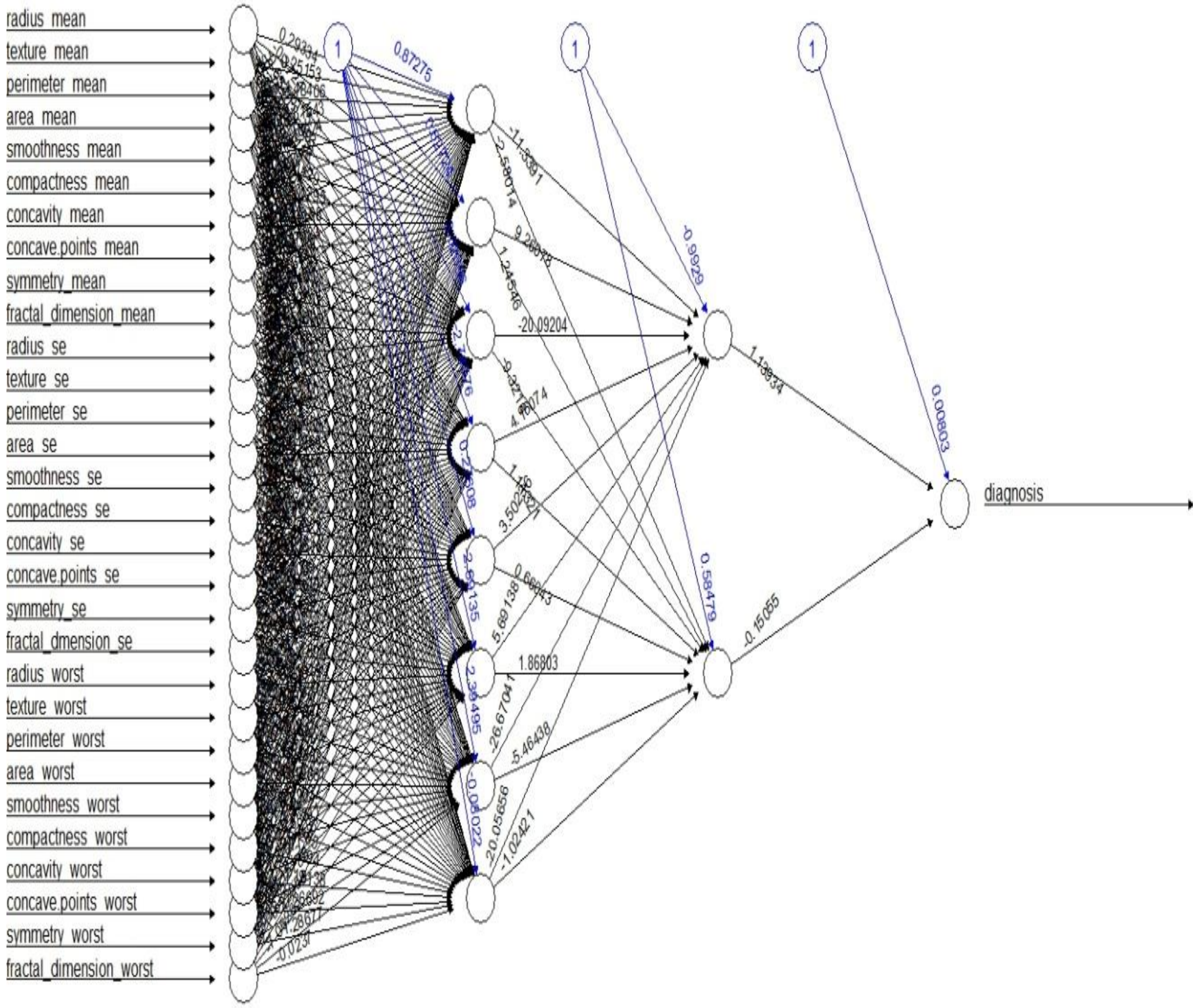

Fig -9: Four Layered ANN Network

All plotted lines which are best fit to see whether or not getting a perfect 45 degree line or not for getting best result.

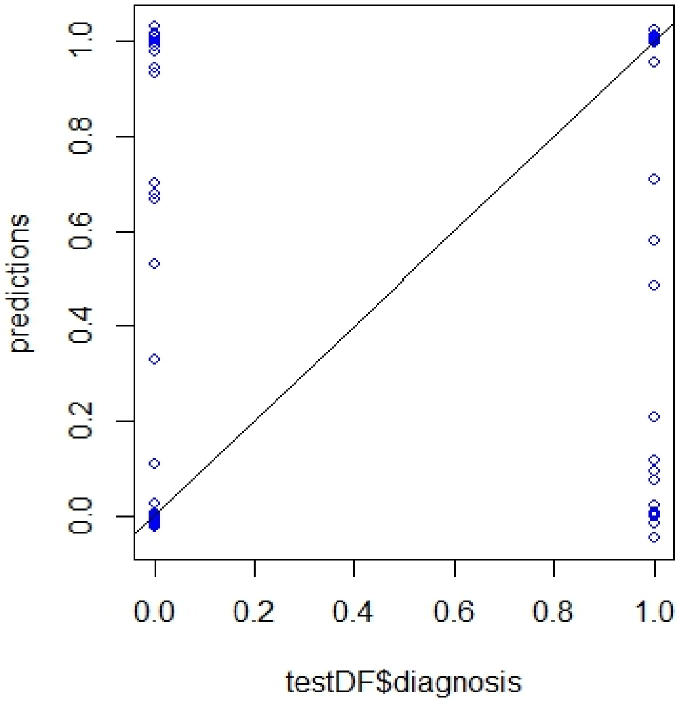

Fig -10: Plotting of Prediction and Test Diagnosis

3. CONCLUSIONS

Repeaters, bridges, and routers are devices which are used for linking individual LANs together to form larger internetworks. Repeaters operate at the Physical Layer. Bridges operate at the Data Link Layer. Routers operate at the Network Layer. Repeaters listen to all network traffic on one port and send it back out through one or more ports, extending smaller networks into a larger, single network. A repeater simply receives frames, regenerates them, and passes them along. Bridges join two or more network segments together, forming a larger individual network. Bridges function similarly to a repeater, except a bridge looks to see whether data it receives is destined for the same segment or another connected segment. If the data is destined for a computer on the same segment, the bridge does not pass it along. If that data is going to a computer on another segment, the bridge sends it along. Bridges use a routing table to determine whether data is destined for the local network or not. Bridges cannot join dissimilar networks. For joining dissimilar networks router must be used. Routers use the addressing information provided at the network level to join many networks together to form an internetwork. Routers divide larger networks into logically designed networks. Routers may seem a lot like bridges, but these are much smarter. Bridges cannot evaluate possible paths to the destination to determine the best route. This can result in inefficient use of network resources. Bridges also cannot use redundant paths. While two bridges can connect two networks, risk of sending packets in an endless loop between the two networks. This behavior eventually saturates the network, renders it unusable. The drawback to a router's inherent intelligence is their speed. Because these process so much information, routers tend to be slower than bridges. Artificial Neural Network is the real life simulation of the human brain. This paper dwells into decrypting ANN and analyzes the same algorithm on a data set of Cancer. The advantages of ANN are the detailed analysis it provides on a varied sets of inputs giving us the perfect set of results.

REFERENCES

[1] Data Communications and Networking2007Mc Graw Hill.
[2] Neural Networks2005 http://www.dkriesel.com/en/science/neural_networks.
[3] Cong Shuang,Toolbox for MATLAB neural network theory and application,1998 .
[4] About Feed Back Network from website http://www.idsia.ch/ ~juergen/rnn.html .
[5] Girish Kumar Jha, "Artificial Neural Network and its Applications", IARI New Delhi.
[6] Carlos Gershenson, "Artificial Neural Networks for Beginners", United kingdom.
[7] Haykin S., "Neural Networks A Comprehensive Foundation", 2nd edition, Pearson Education, 1999.