ANFIS and Fuzzy Based Faulty Node Detection for Wireless Sensor Network

DISSERTATION/THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE
OF

MASTER OF TECHNOLOGY
IN
Control and Instrumentation

Submitted by:

AKSHAY SHARMA

2K17/C&I/01

Under the supervision of

Dr. Bhavnesh Jaint
Dr. Anup Mandpura

DEPARTMENT OF ELECTRICAL ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

2022

Abstract

One of the main challenges in WSN is detection and management of faulty nodes. Currently, the great majority of fault detection approaches rely on surrounding nodes' views of data, which ignores the happenings of the event or issues coverage. In this paper, we describe a novel distributed fuzzy logic-based defective node identification approach for heterogeneous WSNs. The algorithm, it is hypothesized, weights the observed data depending on criteria such as distance, coverage, and the difference between them. When the proposed distributed technique is employed, each sensor node can accurately estimate its own state even in the presence of events such as sudden and temporary failures. According to rigorous simulations, the proposed technique decreases false positives while also improving problem detection accuracy.

DEPARTMENT OF ELECTRICAL ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CERTIFICATE

I, AKSHAY SHARMA, Roll No. 2K17/C&I/01 student of M. Tech. (Control & Instrumentation), hereby declare that the dissertation/project titled "ANFIS and fuzzy based faulty node detection for wireless sensor networks" under the supervision of Dr. Bhavnesh Jaint and Dr. Anup Mandpura of Electrical Engineering Department Delhi Technological University in partial fulfillment of the requirement for the award of the degree of Master of Technology has not been submitted elsewhere for the award of any Degree.

Place: Delhi **AKSHAY SHARMA**
Date: 24.06.2022

Dr. BHAVNESH JAINT
Professor
Dr. ANUP MANDPURA
Professor

CONTENTS

Chapter 1

1.1 INTRODUCTION

When we talk about Wireless Sensor Networks, we're referring to a network of geographically scattered devices called as nodes that collaborate to wirelessly share data from a visible field. The information accumulated through diverse nodes is sent to a node which acts as sink that utilizes the information by itself or transmit to remote locations using varied networks through internet (Priyanka Rawat *et al. 2014*)

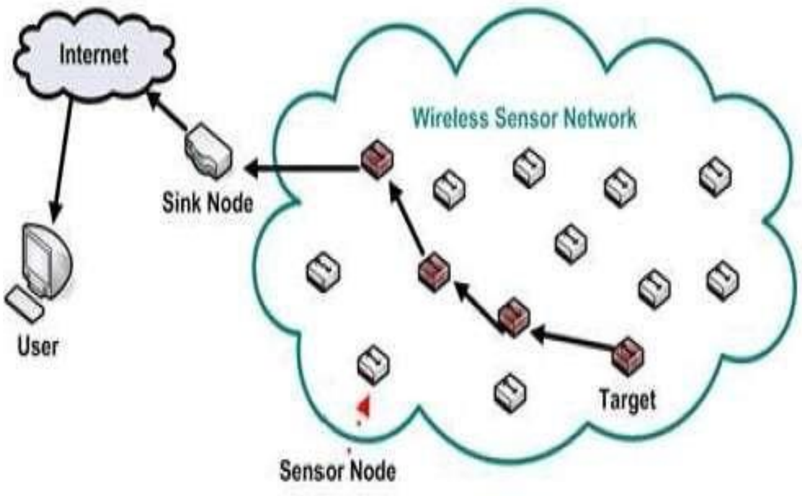

Figure 1.1 Simple WSN

Components of Sensor Node

Position or location identifying technology, sensor mote, mobilizer,sensor, ADC, CPU with storing capacity, power unit, transceiver along with power producer are all components of a sensor node. The location of the node is determined using a position or location finding mechanism.

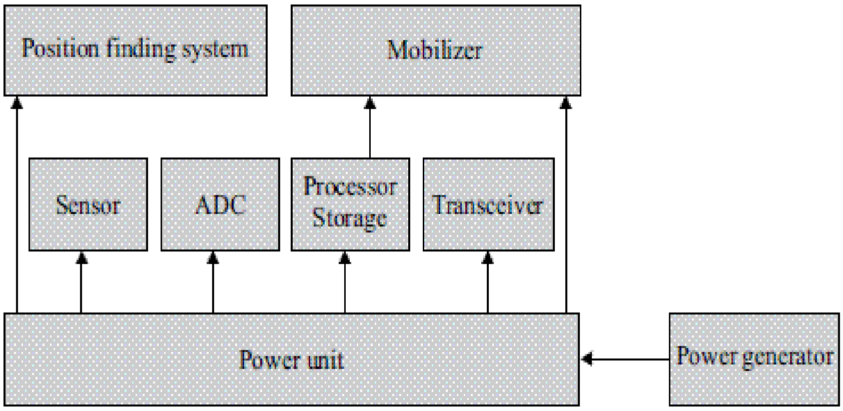

Figure 1.2 Components of sensor node

Detection of node movement is the responsibility of the mobilizer. Sensors are used to sense the surroundings based on the application. ADC converts the analog value of sensed data to digital value. The combination of sensor and ADC is called sensing unit. The small processor with storage capability processes the data. It is called processing unit. The sensor collected data is sent to the sink through transceiver. These nodes are generally battery power operated. Power unit is responsible for power generation for consumption by components.

Protocol Stack

There are five communication layers and three management planes present in the WSN protocol stack.

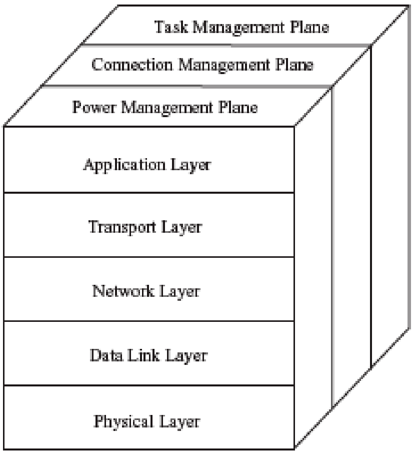

Figure 1.3 WSN Protocol stack

Application layer deals with various applications such as dissemination of queries and localization of nodes. Transport layer handles data flow throughout the network. It is especially concerned with data transportation from the sensor nodes to the sink. Network layer takes in charge of routing. Data link layer takes care of mobility of nodes and control error. MAC protocol in shares medium to all sensors to send environment data. The physical layer is responsible for the conversion of the data received by data link layer into suitable form for further transmission.

The power management drives optimum usage of the nodes as these nodes are equipped with limited power. This results in lots of algorithms for the systematic use of power. Connection management takes care of movement of sensor nodes and detects neighboring nodes referred to as mobility management. Task management performs scheduling of sensing tasks on the sensor field (Shantala Devi Patil et al. 2016).

1.2 Deployment of Sensor Nodes

Various methods are used for deploying sensor nodes. Based on the area, deployment is done either indoor mechanism or outdoor mechanism. Indoor deployment is implemented within a closed circle, for example with in a building. Outdoor deployment is implemented for wide range of area which is not closed. Based on the placement of nodes, there are two different strategies followed in the sensor network. They are unplanned and planned deployment. The unplanned deployment is implemented by placing sensor nodes on the large- scale region. For example, nodes are dropped through air by helicopter with the help of parachute and additional devices to change the dropping behavior. Another example is centrifugal sprinkler which is used for spraying required water uniformly in the region of a candidate. For emergency situation like forest fire these methods prove to be effective. This also called as random scheme. Planned deployment is implemented by placing the nodes carefully on the particular places with regular interval between nodes. It will be useful only for small area. The other name of the planned deployment is deterministic deployment sometimes, the sensor nodes have to move from place to place to reach the destination. For example, the sensor nodes placed in vehicles need to move their positions wherever the vehicle moves. In regards to the maneuver of the senor nodes, there are two classifications. One is called virtual force method. It uses law of movement related to physics. Another is called pre-computed method. The direction and place of movement of sensor nodes are done based on the previously computed place. Sometimes, combination of both the methods will be used.

Based on the utilization, three methods will be used. First one is called bedspread method. It will be used only for a particular area where the person is available. For example, if a VIP attends any function, then dais will be covered with sensors of bedspread to identify any suspicious activities. Second one is stumbling block scheme which is used for deployment of nodes in complete area of a place where the function is organized. For example, if the Prime minister attends a function, then protection is extended to the entire area including the dais. It is like fencing the complete area. Third one is target object. This scheme is useful when we need to enter into the enemy campus.

Potential area-based scheme considers locating a person inside natural obstacles such as buildings, ponds etc. It is suitable for nodes which have a capability to move. These nodes are deployed in a small area and it will maximize its coverage by moving and placing the nodes uniformly.

Combination of random scheme and moving capability of sensor nodes uses many deployment schemes. They are virtual stress-based scheme, connectivity conserved virtual stress scheme, scheme based on FLOOR, Press-Release based scheme, distributed exploitation Method, SEEDS: Scalable power Efficient Exploitation Scheme, distributed self-scattering scheme, error revoking and identical, scheme based on Vector, Voroni, Minimax scheme, centroid movement schemes, scan movement schemes, glowworm swarm optimization method (Vikrant Sharma *et al. 2016*).

Based on the coverage, there are two classifications such as area exposure and location exposure. The entire area marked for sensing should be enclosed by some sensor motes in the area of exposure. In location exposure, some sensor motes should be attached to places wherever the application needs.

12.1Data Collection in Sensor Node

Data collection in wireless sensor network is done by three steps such as deployment of sensor nodes, information delivery and dissemination of control data. Various schemes are brought forth in the previous segment for the deployment of nodes in the sensor field. Various schemes are present besides the above discussion. Information delivery is done as usual by satisfying all the Reliability, latency, throughput, and energy usage are examples of Quality-of-Service parameters. (Feng Wang *et al. 2011*).

Dissemination of control data generally accompanies various methods. But every method falls under the category of gossiping and flooding. In the flooding method, the control data has been sent to all the neighboring nodes except the sensor node which transmits control data. Whenever a sensor node receives the control data, it simply passes the data to neighboring units. The process of flooding makes certain fast response. One of the drawbacks is possibility of receiving the same control data more than once from different sensor nodes. Apart from this drawback, energy consumption is also an issue as every node receives and passes control data. Another method which simply selects single neighbor and transmits the control packets is gossip method. Single copy of the control data is sent to any node. Maximum energy will be saved in gossip communication but the drawback is delay in communication (Mukta Chandna et al. 2015).

1.3 TOPOLOGIES USED IN WSN

1.3.1 Bus topology

In this topology the messages are transmitted from source node to the destination node while also delivering messages to all other nodes. Every node receives the message in bus topology, but only the intended node will process it and take action. All the other nodes simply ignore the received message. The sink node is positioned on the end of the bus. It is suitable only for limited number of sensor nodes. As the counts of nodes increases, it will lead to the performance issue related to the drawback of this topology.

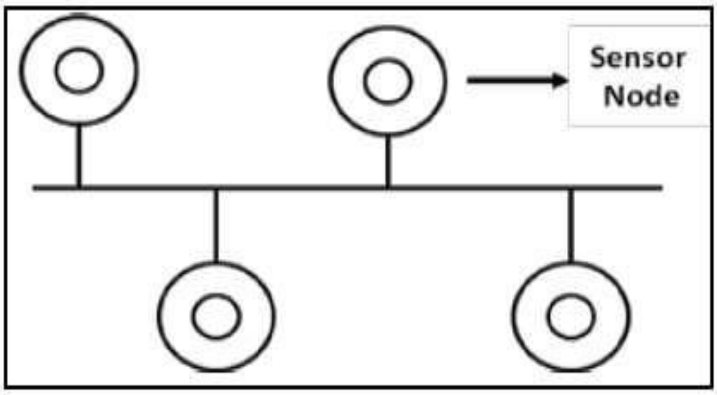

Figure 1.4 Bus topology

1.3.2Tree topology

Tree topology uses single node as a gateway or router which is root for the entire tree. It is used

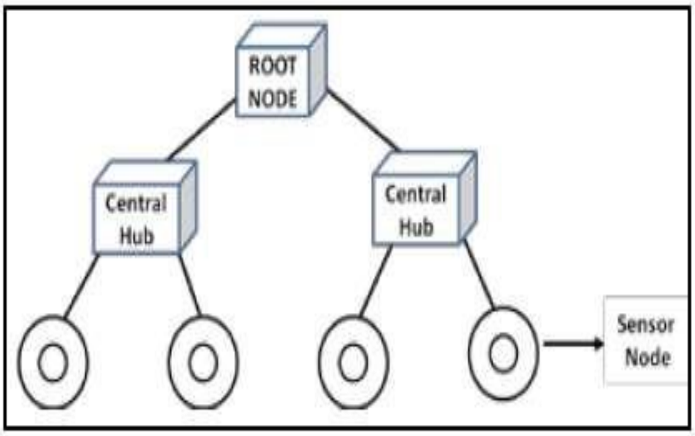

Figure 1.5 Tree topology

As a chief communication node in the tree hierarchy the children of a root node are the sink node which acts as a central node for its own children. As per the tree topology the sensor nodes are connected with them sink. After performing the sensing operation, the responsible node transmits the sensed data to the parent node which is a sink node. The path for sensor network in tree topology is either one-hop or multi-hop. The path selected would be an optimal path with minimum delay. The sensor nodes count attached to the sink node must be balanced. Many load balancing algorithms are used for maintaining the equal number of nodes on both sink nodes, but still research is going on to find efficient load balancing.

1.3.3 Star topology

The sink node will be placed in the center place of all the sensor nodes. In this topology, the node is unable to have direct communication with rest of the nodes. For the communication with another node, sink node is used as an intermediate node or router. It follows the client-server paradigm. The role of server is performed by the sink node and rest of the nodes takes role of clients. If any node senses the information, then it will be sent to the central sink.

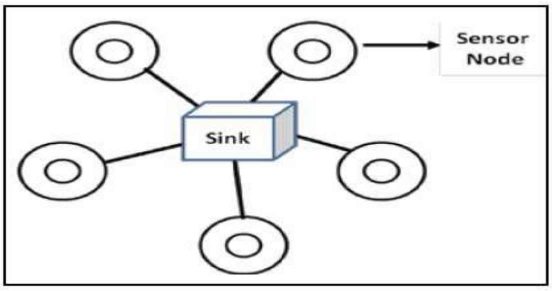

Figure 1.6 Star topology

1.3.4 Ring topology

It is the connection of the sensor nodes in a bangle like formation. The communication is carried out only in a single direction. Either it uses clockwise direction or anticlockwise direction. The failure of single node leads to complete breakdown of the ring.

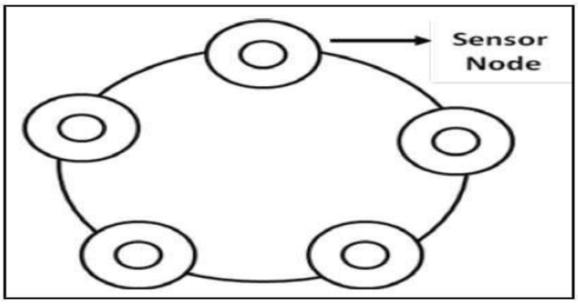

Figure 1.7 Ring topology

1.3.5 Mesh topology

In this topology, there is complete interconnection among the nodes present in the network. It is termed as full mesh. If a few nodes are not directly connected, referred as partial mesh. This topology holds the advantage of making sure of delivering the data to the destination. It has an option to select one path from multiple existing paths.

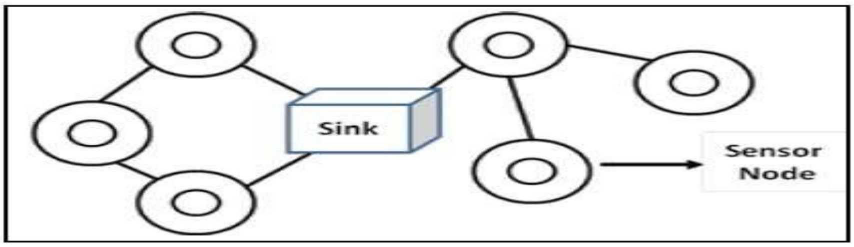

Figure 1.8 Mesh topology

1.3.6 Circular topology

It is implemented in the places where n tier security is needed. It has n number of circles. The inner circle is named as tier1 and the outer circle is tier2. Each circle has numerous sensor nodes deployment. This arrangement of each circle is similar to ring topology. But it distinguishes from ring as on the circumcenter the sink node is placed. The placement of several nodes is haphazard. Sink node receives information from every single node in the network. The path is automatically formed diagonally by the diagonal nodes, and all nodes in that path use only that path.

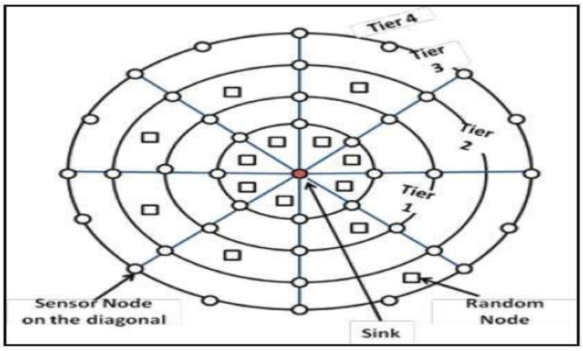

Figure 1.9 Circular topology

1.3.7 Grid Topology

The sensing area is partitioned into many portions called grid. All the grids have equal number of sensor nodes. Though many nodes are available, only one node in a grid is active all the time. For increasing the network lifetime, the role of active node switches among the senor nodes. The head node in each grid have the responsibility of delivering the observed data from rest of the nodes in that grid. This topology saves energy as well as increase the life time of the network. (Divya Sharma et al. 2013)

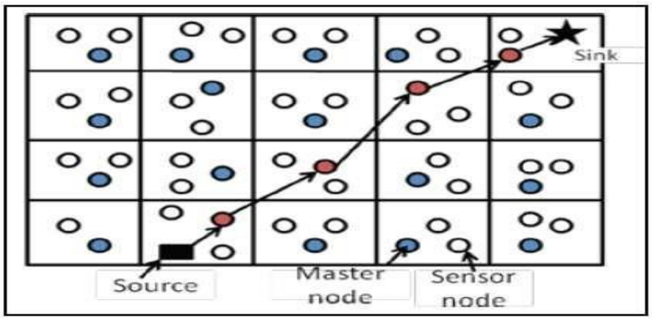

Figure 1.10 Grid topology

1.3.8 Chain based topology

The sensor nodes connect themselves like a chain to transmit the data. A leader node is selected among all the nodes and that will act as sink node. Any node will receive the information from its predecessor node and then the same is transferred to its successor node. Finally, the information will find its way to the sink. It will save a lot of energy and the life time of the network will be increased. (Quazi Mamun 2012)

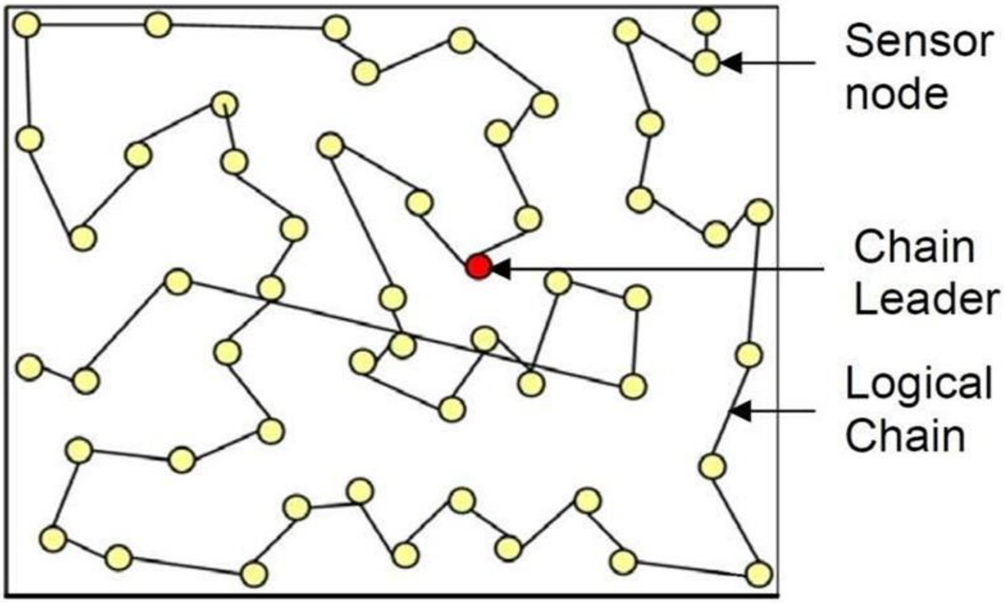

Figure 1.11 Chain based topology

1.4 Types of WSN

Based on the place of sensor nodes deployment, it is classified into terrestrial, underground and underwater WSN. Based on the data used for communication, it is named as multimedia WSN. Owing to mobility, it is named as mobile WSN.

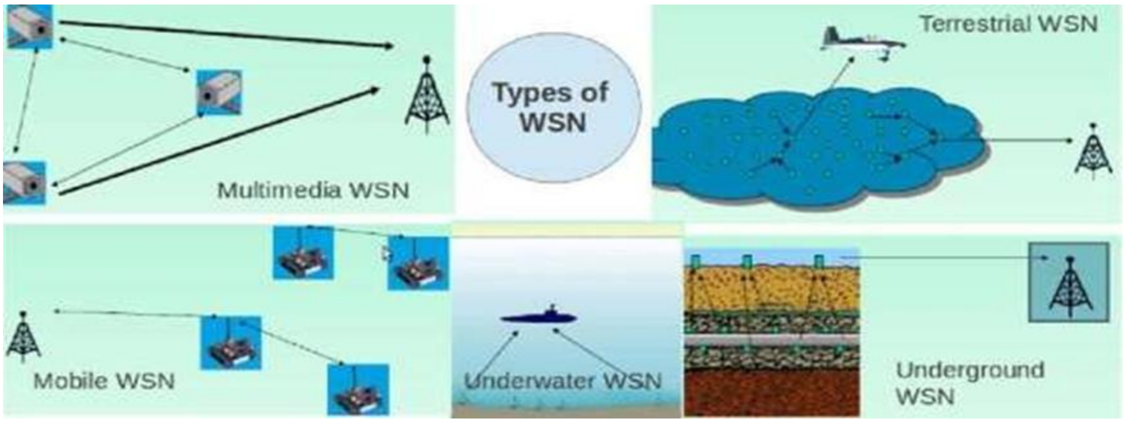

Figure 1.12 Types of WSN

1.4.1 Terrestrial WSN

Depending on the application area's situation, huge amount of sensor nodes deployment is done. It uses unplanned deployment scheme and nodes are scattered geographically. Cost of the sensors must be very minimum. Sensor nodes in terrestrial WSN use solar energy for recharging their battery power.

1.4.2 Underground WSN

Sensor nodes are deployed under land such as inside the mines or caves. They are very useful for monitoring the status underground level. In normal scenario, the sensed information of any sensor node is sent to base station. Underground WSN needs additional sink which will be placed above the land. Communication is very difficult due to reduction of the amplitude of a signal. Replacement of the nodes or recharge of battery of sensor nodes is also very difficult**.**

1.4.3 Underwater WSN

Sensor nodes are deployed under water such as deep-sea. These types of sensor nodes are very costly. So only a few nodes are deployed under water. These nodes have an ability to configure themselves and adapt to unexpected situation. For data collection, they use autonomous vehicles. Vehicle moves near all the sensor nodes and gather the sensed information from those nodes. Similar to underground sensor nodes underwater sensor nodes are also very difficult to replace or recharge. So, it uses lots of energy efficient mechanisms.

1.4.4 Multimedia WSN

Multimedia WSN is constructed by deploying the cheapest sensor nodes in a well-planned manner. It deals with multimedia data such as the combination of text, image, audio and video. These sensor nodes built with the capability to store the sensed multimedia data, process and forward them to sink node. Because of handling the variety of data, they need larger bandwidth.

1.4.5 Mobile WSN

Static WSNs use sensor nodes that do not move. But for dynamic WSNs, mobility is the main criteria. Mobility leads to other challenges from construction to data forwarding. So the mobile sensor is designed to have an ability to move around the application area, change the position and organize nodes. Mobile WSN covers larger area than static WSN (Priyanka Rawat et al. 2014).

1.5 APPLICATIONS OF WSN

1.5.1 Body Area Networks

Body Area Network (BAN) is used in medicinal and health care fields. Since the nodes are attached to human body the nodes must be very small size with reduced weight. It measures the physiological values such as breathing, heart beat while walking and running in order to monitor the patients. BAN is built with wireless connections and so it is also called as Wireless Body Area Network (WBAN). Electromagnetic signal strength will be varied at different parts of human body because water content of tissue differs place to place. It is used for patient monitoring and elder's care. The architecture of WBAN consists of four parts such as sensor nodes and sink node attached to the human body,gateway, internet and application. The sensors measure the changes in the body and send the data to the sink which is also attached to the human body. The sensed information is passed from sink node to gateway, from gateway to internet and internet to application where required. In the application domain, the doctors or healthcare professionals look at the medical reports. According to the measurements further medicines or treatment will be prescribed to the patient (Luis Filipe *et al. 2015*).

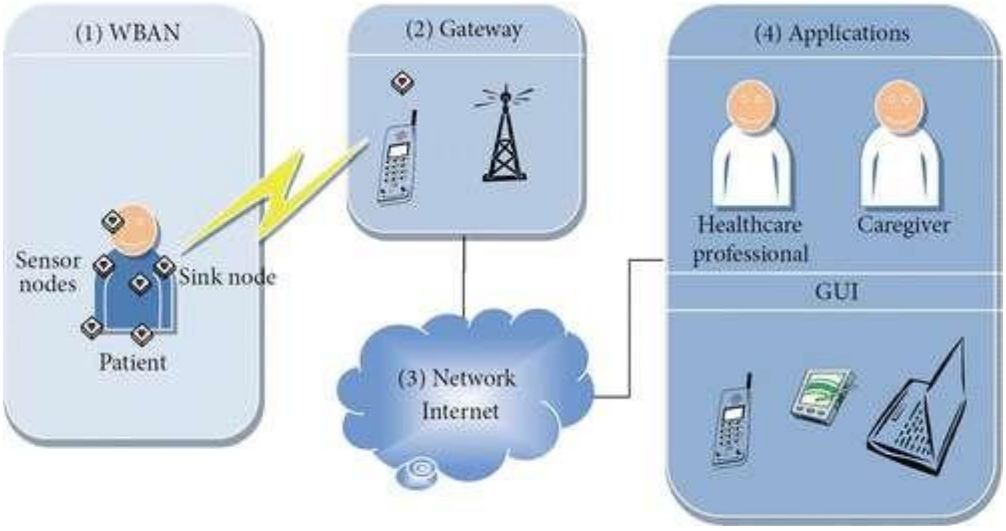

Figure 1.13 WBAN architecture

The WBAN architecture is 3-tier architecture. Three different communications are used in this architecture namely intra BAN, inter BAN and beyond BAN. The communication between sink node and sensor nodes of the same BAN is referred to as intra-BAN communication. Communication between BANs is called inter-BAN communication. Communication of the end user i.e., application side with internet is called as beyond-BAN communication (Rim Negraa *et al. 2016*).

1.5.2 Environmental Monitoring

Day by day, usage of vehicles increases in the cities. Large amount of carbon-dioxide is produced in the cities which is very dangerous for the environment. It affects human being as well as animals. Using sensor nodes, one can monitor the changes in carbon-dioxide, amount of water content in the atmosphere, speed as well as the direction of breeze, temperature etc.

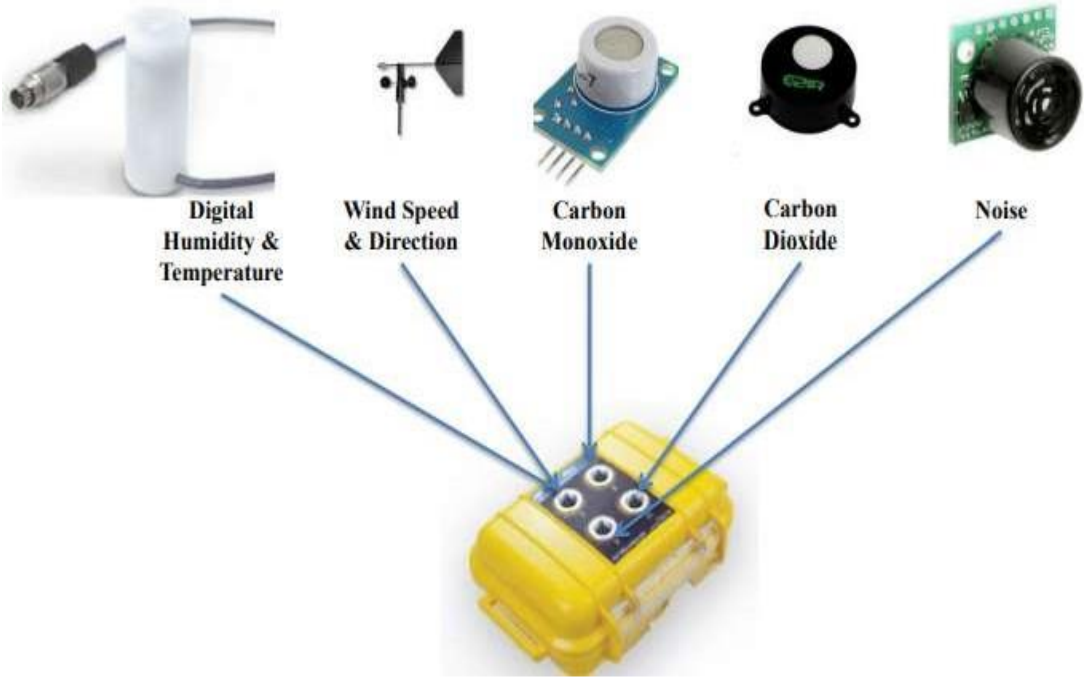

Figure 1.14 Small wireless node with different sensors

To monitor different kinds of parameters many sensors are fixed in a small sensor node. Each sensor senses its own parameters. Each node is deployed randomly with some distance. The maximum distance of nodes in urban areas is reduced to 500 meters. Information is collected by each sink from the group of nodes within its range and store it or send to the server that is in remote place for further analysis. (Rainham *2016*).

1.5.3 Weather monitoring

Various type of sensors such as temperature, dampness etc. are deployed. The real time values are sensed and transferred to base station on regular intervals.The figure shows the microcontroller system equipped with many sensors. The sensors attached to the microcontroller sense the temperature, dampness and speed of the sky.

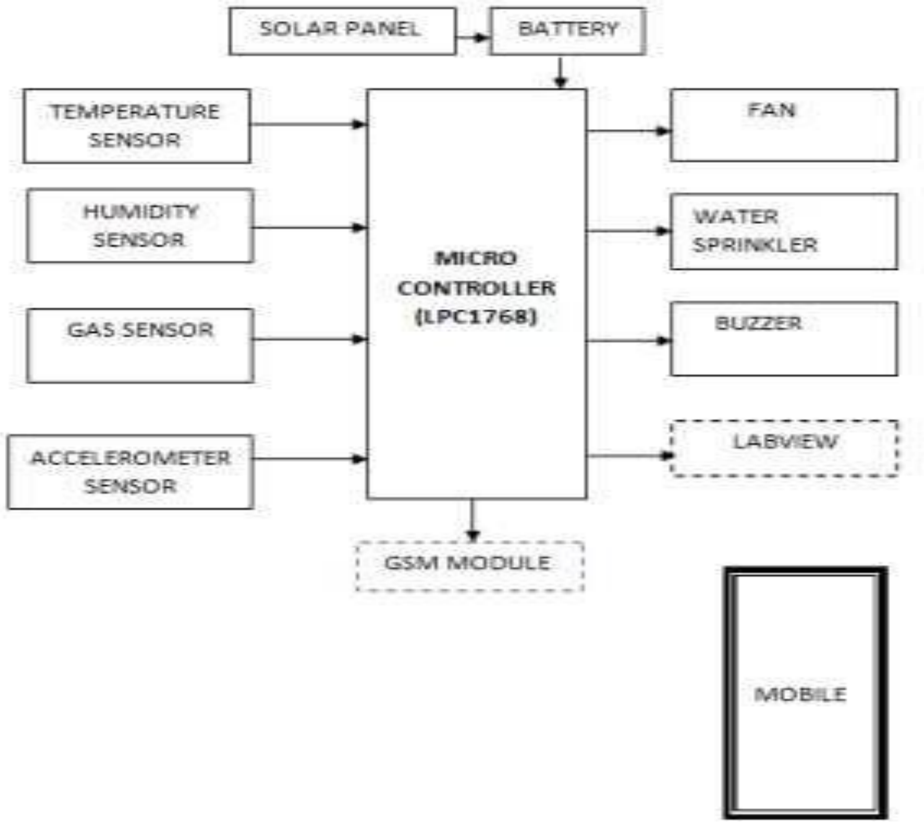

Figure 1.15 Sensor architecture for weather monitoring

The sensed analog signals are converted into digital signal by the sensors. This digital signal is given to the microcontroller. The microcontroller analyzes the data and alerts the user (Madhuri *et al. 2016*).

1.5.4 Flood observant system: Sensor nodes are deployed in the corresponding sensor fields to sense the flow and level of water in the river. These nodes constitute a wireless sensor network (WSN) and transmit data collected to a base station located near waterways. Meteorological department announces weather forecasting report periodically in real time scenario. The Information Processing Center (IPC) collects forecasting report from the meteorological department. IPC collects the level and flow of water in the river from WSN through base station.

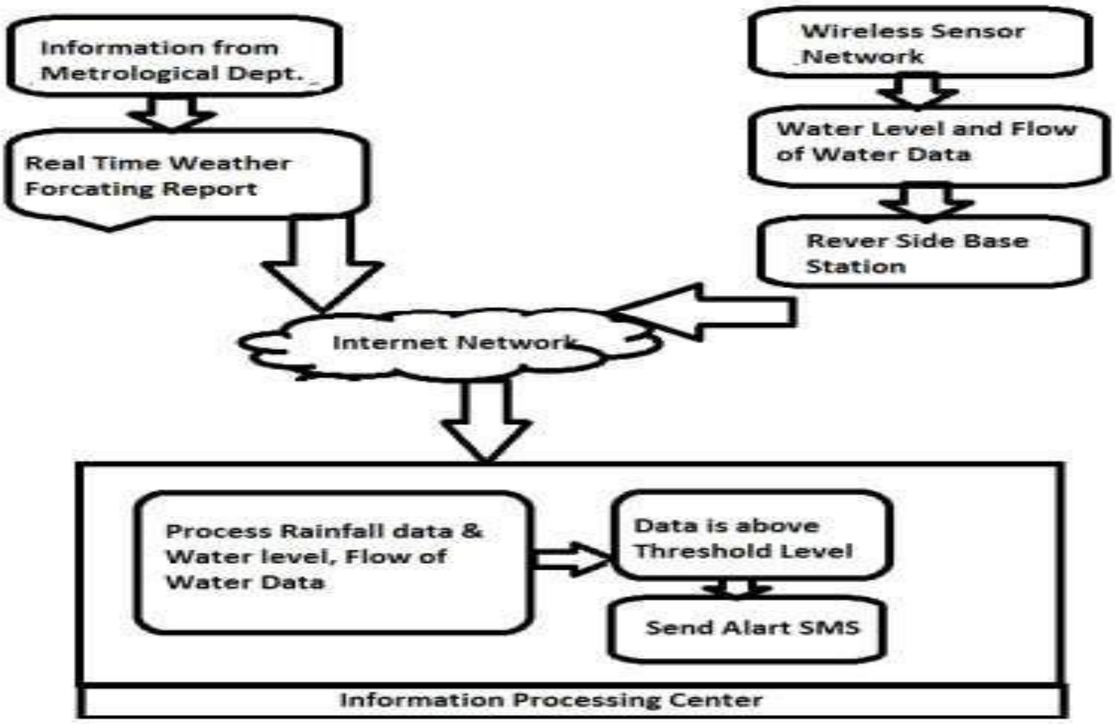
Information from Metrological Dept.
Real Time Weather Forcating Report
Wireless Sensor Network
Water Level and Flow of Water Data
Rever Side Base Station
Internet Network
Process Rainfall data & Water level, Flow of Water Data
Data is above Threshold Level
Send Alart SMS
Information Processing Center

Figure 1.16 Food observant system

The threshold value is fixed for all the parameters with three values low, high and very high. For humidity, it fixes the threshold values 16% to 30.99% as low, 31% to 47.99% as high and >=48.00% as very high. For temperature, it fixes <=23.99 degree Celsius as low, 24 degree Celsius to 24.99 degree Celsius as moderate, 25 degree Celsius to 31.99 degree Celsius as warm, 32 degree Celsius to 32.99 degree Celsius as hot and >=33 degree Celsius as very hot. For rain fall, it fixes the threshold values <=100.99 mm as low, 101 mm to 299.99 mm as moderate and >=300 mm heavy. For water level, it fixes the threshold values <0.8 M as low, >=0.81M to <1.2M as high

>=1.2M as very high.

IPC analyzes the rainfall report generated by meteorological department and flow and level of water received from WSN with the fixed thresholds. When the data exceeds the threshold, then the IPC system will immediately send the SMS to riverside base station and riverside people (Sandeep Shiravale *et al. 2015*)

1.5.5 Wildlife Tracking

Monitoring the activities of animals in a zoo with vast area is a very difficult task that can be done using WSN. The system needs four different devices to accomplish the task. Collars, sensor nodes or motes, base stations and sniffer device.

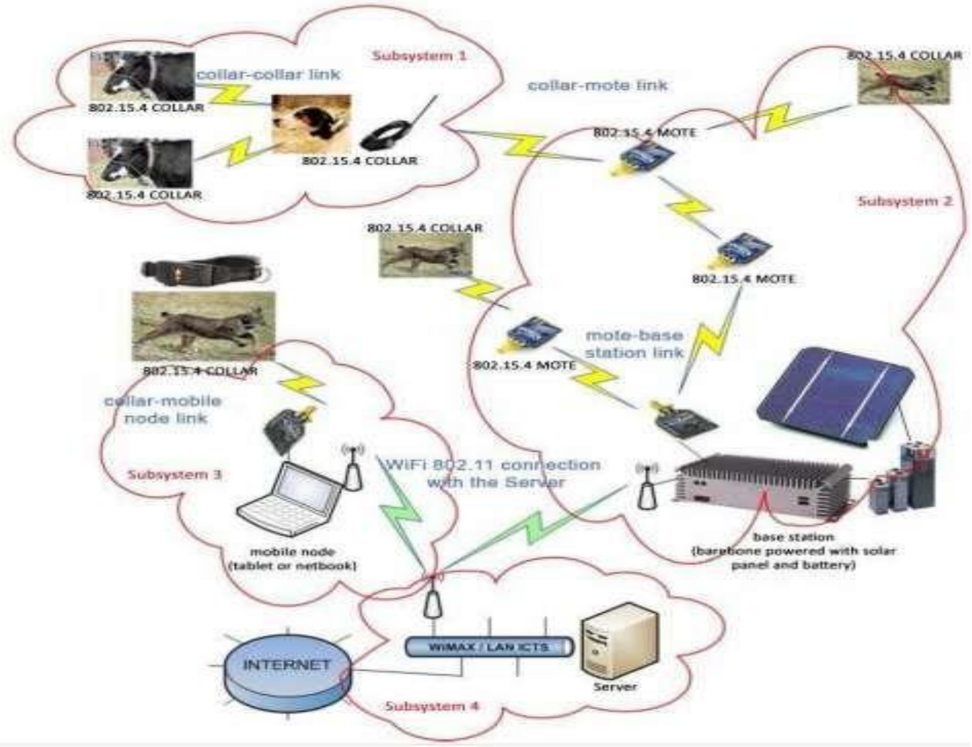

Figure 1.17 Wildlife tracking

Collar is a device like a band inbuilt with sensors. It will be attached to the intended animals that need to be monitored. The task of a collar is to sense the different behavioral patterns. Microcontroller is used to access the periodically measured data from the sensors. The microcontroller can switch over to sleep mode when it is not collecting information to increase the life time of battery. It employs ZigBee technology and transmits data through WSN to the nearest base station. The animal is out of the network's coverage region if the collar is not reachable. For such a situation, the SD memory card is attached; the sensed data will be stored in SD card when it is not reachable. When the animal comes inside the coverage area, the data stored in the SD card will be sent to base station. The collar does not continuously send the data. It is pre trained with neural network. It receives variation in the data from different sensors and analyzes the data. If anything is distinctive, then it sends

1.5.6 Agricultural Monitoring

Farmer's plant different types of seeds in their land. The crop size, quantity of fertilizer and water are monitored with the help of WSN. For each hour, the data is collected from sensors because frequent data collection results in power drain of sensor nodes. Data collection could be increased for more hours if the crop grows slowly in a uniform climate. Agricultural monitoring uses three different sensors. The first one is to know the level of water. It is a cylindrical or spherical shaped object designed with flexible or rigid objects. Second is LM35 which is used to measure the temperature of agricultural land. Third is humidity sensor HR202 which is used to measure the water particles present in the land. It reads the data using the sensors. If they are in the given range then it will automatically switch on the motor using Internet of Things (IoT). Based on the threshold value, the motor is controlled and the measured data values are stored in cloud using IoT. The farmer easily identifies what is required for the crops at the correct time and production can be increased (Infantial Rubala *et al. 2017*). Water irrigation system is also done using WSN. The water level and flow of water must be sensed in real time. If the reservoir has less water then it will be filled with some other water sources. This method saves lot of water, as well as the physical effort of labor. If it is very hard to take decision on irrigation system, then the fuzzy based decision is taken (Arun *et al. 2012*). Mango production is improved by using sensor system which transmits the sensed data to the remote location by SMS with the help of GSM network (Mujeeb Ur Rehman *2016*).

1.6 Disaster Management

Disasters are of different forms.

1.6.1 Volcanic Eruption

The Volcanic Eruption is the explosion of the melting rock with enormous amount of heat. The hot melting rock inside the volcano is called magma. When the magma explodes and comes out of the open rock, it is referred to as lava. When volcanic emission starts, lava erupts with ash, dusts, dangerous gases, etc. Temperature of lava is very high. Even it cannot be imagined. Anything comes on the way of flow of lava will be immediately burnt. It may be any animal, tree, building etc. Volcano generates type of "A" or "B" waves. Parameters such as temperature, pressure under the earth, tectonic plates movements will be measured in the volcano disaster. Four different sensors gas sensor, thermal sensor, cloud sensor and hydrology sensor are used. They use Enhanced Distributed Energy Efficient Clustering Protocol.

1.6.2 Storm

Storm is another disaster. The storm produces lightening from the sky, heavy rain with thunder including ice balls. Tornado is a type of storm which has a speed of 480 kilometer per hour. Hurricane is another type of dangerous storm which can come with the speed greater than 117 kilometer per hour. The waves generated by the storm appear in the shape of a cone. The sensors used for measuring the storm is temperature sensor, direction sensor, speed sensor and humidity sensor. They use a radar instrument for monitoring weather employing the same protocol used in volcano.

1.6.3 Earthquake

The earth is made of large sized rocks which are technically referred to as tectonic plates. Earthquake occurs due to the movement of the rock plates or unexpected breakage of tectonic plates. Sudden movement of the tectonic plates leads to a shake in the earth. The buildings will be collapsed. Earthquake generates seismic waves. Parameters like pressure under the earth and tectonic plate movement are measured using seismometer. This also uses the same protocol used in volcano and storm (Devasena et al. 2015) the data to the base station.

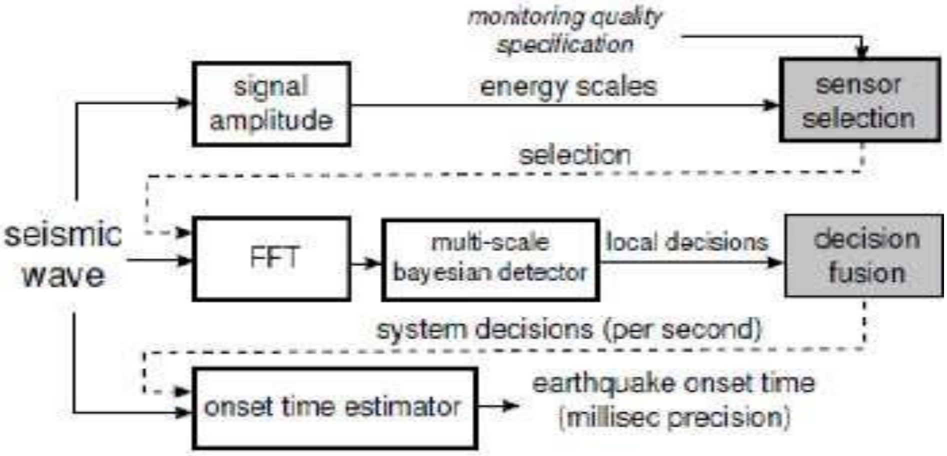
monitoring quality specification
signal amplitude
energy scales
sensor selection
selection
seismic wave
FFT
multi-scale bayesian detector
local decisions
decision fusion
system decisions (per second)
onset time estimator
earthquake onset time (millisec precision)

Figure 1.18 Earthquake detection architecture

Seismic waves are produced at the time of earthquake. These waves are sent to sensor selection through signal amplitude. The sensor selection portion selects the sensor nodes on the particular area based on the amplitude of seismic waves and then the frequency value of seismic waves on the selected sensor nodes are calculated with the help of fast Fourier transform method. Using the calculated values, it will take a decision locally and send the decision to the base station for localizing nodes at a particular time (Ankur Mangla *et al. 2016*).

1.6.4 Tsunami

Tsunami is also a type of earthquake but happened under the sea. Sudden movement of tectonic plates under the earth of sea area generates shock waves on the water. These waves are more powerful. Such massive waves spread to the vast area of ocean. This is called as tsunami. The speed of Tsunami is about 800 kilometers per hour. The wave length of Tsunami is up to 200 kilometer long. The type of waves generated is called harbor waves. The height of the tides, water level, and pressure under the sea and rock movements are measured using the instrument named deep ocean tsunami buoys. It makes use of the BEENISH Protocol (Balanced Energy Efficient Network Integrated Super Heterogeneous) (Devasena et al. 2015).

For tsunami management a good alarm system is given. It consists of three nodes called sensor node, friendly node and controller node.

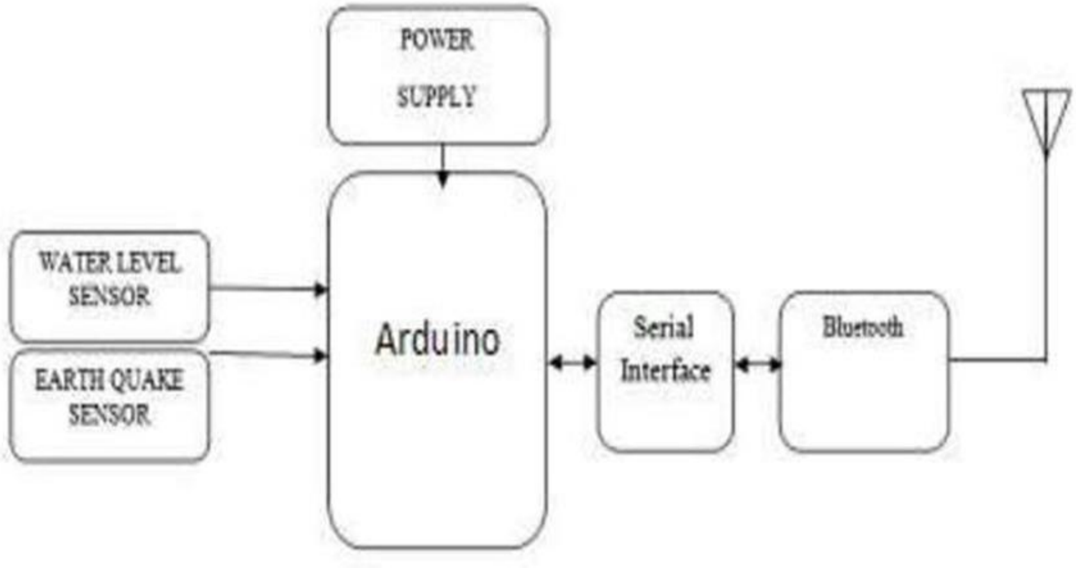

Figure 1.19 Sensor node

The node is deployed in the ocean and attached with two sensors for sensing level of water in the sea and earth quake. Microcontroller ATMEGA328 is also attached and it uses serial communication. With the help of Bluetooth, sensed data is transmitted to the friendly node.

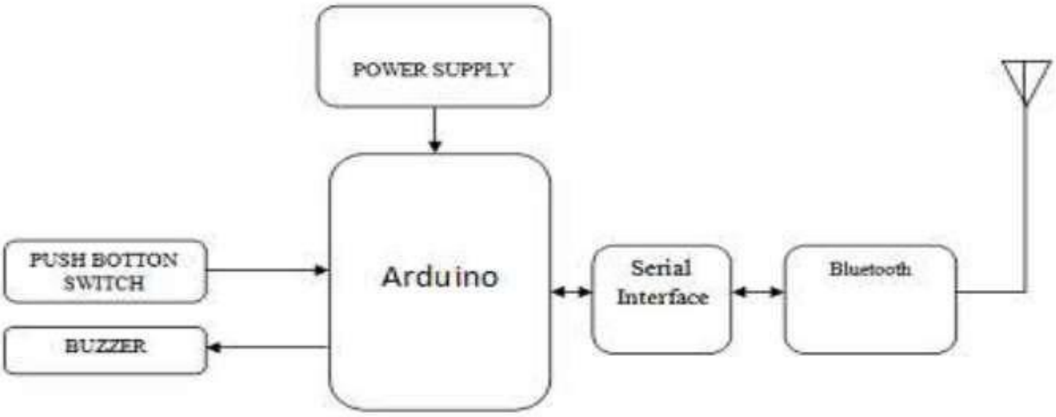

Figure 1.20 Friendly node

Friendly node is deployed near the coastal area. The reason for deploying it nearby coastal area is to help the victims who are surrounded by flood during tsunami. When they press the button attached to the friendly node, it makes an alarm through the buzzer and sends the information to the controller node. Rescue process will start immediately.

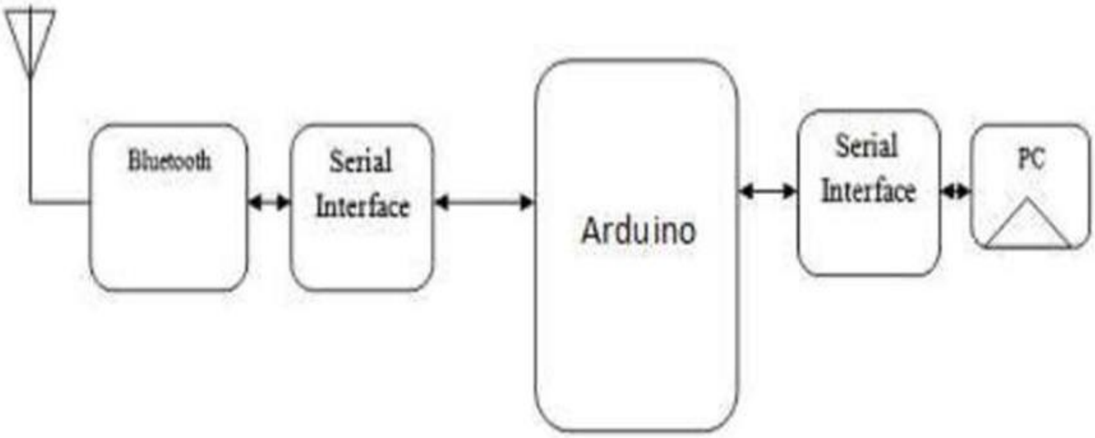

Figure 1.21 Controller node

The controller node is deployed on the base station. When it gets the data from friendly node it makes an alarm to rescuers as well as the people available on the base station area (Shaik Karimunnisa et al. 2017).

The controller node is deployed on the base station. When it gets the data from friendly node it makes an alarm to rescuers as well as the people available on the base station area (Shaik Karimunnisa et al. 2017).

1.7 Landslide Management

Landslides destroy properties of people and snatch their lives. The area is classified into different zones hierarchically and the sensor nodes are deployed in different zones. Weight of the water in all pores, humidity of soil, vibration, sprain on the particular area etc. will be measured. Based on the analysis of all the measurements, decision will be taken to issue (Ankur Mangla *et al. 2016*).

1.8 Traffic Management System

Now a days, traffic is a main problem in the cities due to rapid growth in the counts of vehicles whereas the road and arrangements for transportation lack improvement. Traditional signaling mechanism is not suitable for emergency situations. For example, the signal turns red on a particular road, an ambulance that uses road has to stop. This situation cannot be handled by traditional system. Using wireless sensor network, the priority can be assigned to such emergency vehicles. It uses three units besides the sensors. First one is Traffic Management Centre (TMC) which is attached to the signal. Second one is Road Side Unit (RSU) that is placed near the communication range of TMC and two sides of the road. Last one is called On Board Units (OBUs) which is fitted on the vehicles.

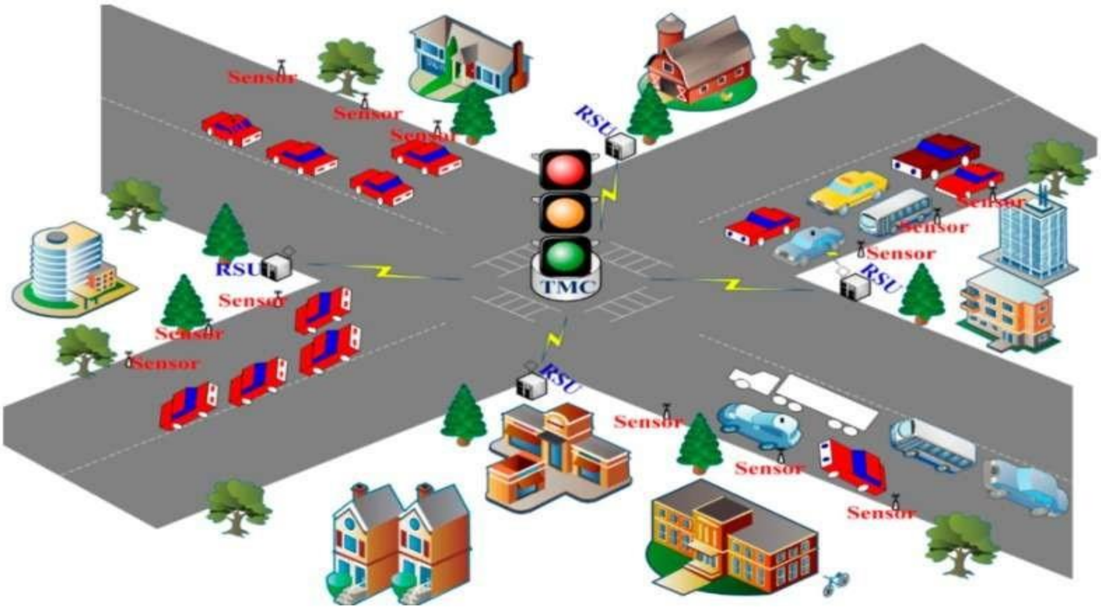

Figure 1.22 Traffic signal using WSN

Sensors are deployed up to some distance on the road side with regular intervals. Sensors sense

The details of the vehicles such as type, density etc. with the help of OBU in vehicle and send that information to RSU. RSU sends the information to TMC. TMC consists of two parts namely information gathering unit and signal controlling unit. The information gathering unit collects information from RSU and hands over to signal controlling unit. The controlling unit analyzes the information and takes intelligent decision for vehicles used for emergency purpose and VIPs. It will stop the current task and give the priority vehicles mentioned above. After ensuring the passage of these vehicles, it continues routine signaling (Kapileswar Nellore et al. 2016).

Inter-vehicle communication in traffic management system: The vehicles can use any wireless technologies such as Bluetooth, ZigBee etc. Bluetooth communication is the best method for short distances as the traffic is restricted to the junction point that is relatively small. A Bluetooth device can easily recognize the availability of more devices within its communication range by enquiry. The sender device makes the enquiry for a greater number of devices at the same time. Listeners get the enquiry type messages and acknowledge the received message. Sender acts as a master and listener acts as slave. If a Bluetooth device gets acknowledgement from seven Bluetooth devices, then it forms a network called piconet. If there are more than seven connections for a Bluetooth device are available then for communicating with the 8th Bluetooth device, it needs to halt and leave temporarily any one of the active Bluetooth devices in the piconet. After completing the communication with the 8th Bluetooth device, it halts and leaves the 8th Bluetooth device temporarily and connects with the already halted Bluetooth device.

If there are more piconets, then all the piconets are combined to form ad-hoc network called scatter-net. In the Bluetooth technology, a device need not be part of only one network. It may be part of more than one network. At the same time, a Bluetooth device is a master for one piconet and slave for one or more piconets. It may be part of any number of piconets. But at a time, it will be active in only one piconet.

Assume that the green signal is for horizontal road and red signal is for vertical road. Car A driver wishes to move on the left road and car C driver wishes to move on the straight road. Now car B is in between A and C. The drivers in cars A and C will not know the position of other cars and their movement. Definitely without seeing the other car, if both drivers move their cars, it will result in a collision.

If all cars are equipped with the Bluetooth devices and sensors are deployed in the traffic signals, then the sensor senses the details and stores the same in the base station. The cars themselves communicate via Bluetooth mechanism. If car A sends the inquiry, then it will act as a master and it says to car C that I will go first and you can move next or you can go first and I will move next. The collisions can be avoided (Vivek Katiyar *et al. 2011*).

1.9 ISSUES AND CHALLENGES IN WSN Fault manageability

In general, WSN applications have sensor nodes deployed in an unplanned manner just like throwing the nodes on the particular regions. So the fault is not uniform from place to place.

Scalability: Even after increasing the number of hardware's, the system is expected to provide the same performance. But it is difficult in WSN. Because some times the number of sensor nodes deployed may be beyond thousand. If nodes are deployed very densely, then there is a possibility for collision.

Communication medium: If the WSN uses multi-hop for its communication, it has wireless connection between the nodes. It has only restricted bandwidth. The wireless medium is unreliable medium, error rate may be high and attack is highly possible. The communication may be affected by fading.

Latency: Many WSN applications are emergency applications like rescuing operation in building / forest fire. The sensor nodes sense the data or track the object which will be immediately communicated to the sink for emergency action.

Area coverage: Designing WSN by covering all the area is still problematic in a few scenarios.

Routing Holes: If the node is not recognized by the routing process, it is called as routing hole. The reason is either the node is dead or due to performing other tasks there is no participation in the routing process. But, identifying such nodes or holes is a difficult task.

Energy: Sensor nodes need power for sensing, forwarding and computation. Due to idle listening, collision and error control mechanism, the MAC layer consumes more energy. Sensor nodes work with limited battery power. Energy should be used efficiently. For example, sensor nodes must be in sleeping state when they are not in use and wakeup whenever it has work. Some alternate way may be invented like recharging battery using solar, etc.

Self-management After the deployment of the sensor nodes in WSN, It should work without any human interference.

Limited memory

The sensor nodes are very small in nature. A normal type of sensor node has only 48k program memory. So, the software must be designed with minimum number of programming lines.

Limited processing: The typical sensor node has only 10k RAM. So, it has only limited processing capacity.

Multimedia communication

Multimedia is a combination of variety of data from text to video with audio files. The sensors have only limited storage, processing capability and limited bandwidth. But multimedia needs larger bandwidth.

Synchronization

Synchronization of time for sensor network is an important criterion. Global time will be referred using Global Positioning System (GPS) and Network Time Protocol (NTP). But the use of GPS receivers and NTP will consume more energy (Khushboo Gupta et al. 2015; Indu et al. 2014; Sukhwinder et al. 2013 and Karthik et al. 2015).

1.10 Problem Statement

The field of wireless sensor networks is an expanding sector in terms of research and development. It continues to see a pattern of growth in regards to new applications and development. The complications of developing a reliable and fault free network encourages efforts and actions in the direction of work focusing on developing large wireless networks. Literature, however, lacks rigorous and consistent definitions for terminology relevant to reliability and fault-tolerance as applied to WSN. This, in turn, confuses the problem space when seeking to develop and evaluate protocols for dependable wireless communication networks. In spite of the considerable work over the past decades to rigorously define the language for fault-tolerance and reliability of components and systems [4], current literature neither defines nor applies fault-tolerance terminology in a manner consistent with counterparts in computing system networks. This leaves the topic mired with vague language and conflicting interpretations of the capabilities of proposed algorithms and techniques. [3], further investigated by [2], propose a network partitioned with a routing hierarchy and protocol which seeks to minimization of energy consumption. The energy of the nodes in the core range of the sink node depletes over time, this leads to the disconnection of the main node from the rest of the network. None of the paper, characterizes the network's remaining accessible energy after the center ring has been depleted adequately. Two concerns about the proposed WSN class have been raised. The first is the uniform and unambiguous usage of language when it comes to faulty nodes and WSNs in general. This paper solves this flaw by recognizing reliability and dependability of the WSN. The second concern is unique to single type of wireless networks [2, 3], and it involves the loss of energy in the middle ring surrounding the sink caused by the existing network protocol. The characterization of the energy the network is left with after extinction of core ring is the subject of this research. Then, in reaction to network degradation, a modified protocol is analyzed and proposed to incorporate the effect of fault nodes in the network by reorganizing it. The modified ANFIS protocol, combined with the depiction of rest of the energy left in network, aims to extend the network's usable life by enhancing utility and efficiency in terms of longevity and energy used, while decreasing residual energy after network extinction.

1.11Motivation

Workplace motivation Surveillance, vehicle tracking, temperature and ecosystem monitoring, intelligence, medical, and acoustic data collection are all common uses for sensor nodes. Because data accuracy is critical to the overall system's performance, finding nodes with incorrect readings is a critical issue in network administration. The difficulty of detecting malfunctioning nodes in the WSN drove the work in this dissertation. The Work's Objective The requirement for a defect detection method for WSNs prompted this research (Wireless Sensor Network),

The work's goal is as follows:

- To Implement WSN based on ANFIS and fuzzy
- To simulate and test the suggested fault detection technique in MATLAB.
- Compare the ANFIS and fuzzy approaches.

CHAPTER 2

LITERATURE SURVEY

To estimate a node's sensor measurement, the Takagi-Sugeno-Kang (TSK) fuzzy inference system and sensor data from nearby nodes are used (FIS). A previous estimate of the node's value was used to approximate sensor data, which was based on real measurements taken at neighboring nodes. Redundancy in data collection is used to deal with any sensor measurement or transmission issues that may arise. If a sensor chip on a node is connected to a WSN mote, it may stop working. If a sensor chip is exposed to the elements, it may produce false readings. Broken sensors aren't thrown away because they can still communicate data between nodes. Sensor readings from the surrounding environment are used as input and output for the construction of fuzzy models for each node. Any sensor output that differs significantly from the actual sensor data, regardless of how slight, is considered faulty. An application uses a fuzzy logic toolbox. The results are compared using recurrent neural networks and synthetic feed-forward networks.

Fault-tolerance of nodes can be improved by adding more sensors; however more sensors equal more nodes, which raises the cost of the node as well as the complication of the sensor network and the power consumption. It leads to, the network getting benefitted from it. That's why researchers are currently looking at sensor measurement redundancy and comparing mathematical models to scientific data in their work [Leushen et al., 2002; S.C.Lee, 1994]. Modeling each WSN node instead of installing additional hardware utilizes the Takagi Sugeno Kang (TSK) fuzzy inference technique (FIS). In resource-constrained environments, sensed data cannot be delivered when a link breaks. Mobile Ad-Hoc networks suffer greatly when links break due to channel interference and dynamic impediments. Accurately predicting an outage and carrying out local rerouting are difficult tasks. These issues are dealt as, this study proposes a two-tiered approach: Sectionary Junction Failure Recovery (SJFR) is a new method for finding items utilizing wireless sensor networks (WSN). Rather than relying on global position data to identify events (such as a connection failure), engineers are turning to metrics like information gradient, least number of hops, low transmission cost, and high residual energy to help them figure out the best route for data transfer (Shiva Murthy Ga et al. 2012). Links fail all the time, hence the standard AODV strategy involves moving traffic from the origin node to a new destination, increasing the nodes' overhead. Furthermore, if one or more of the connections fails, data packets may be lost. Long-term data transfers via an audio stream present specific challenges since the theoretical network state needs to be dynamically maintained after a connection breakdown." Another difficult topic to overcome is identifying and thwarting threats to data transfer. Gradient broadcast routing ensures consistent delivery of the data across the error vulnerable zones in the channels; hence it may be beneficial in a large wireless sensor network.

Sensor nodes are worried about the considerable power consumption that could result from using this protocol's broadcasting functionality. This thesis investigates and suggests several energy-efficient forwarding mechanisms. Algorithms like this one attempts establishment of balance between use of resource and consistency. When wireless networks or sensor nodes go down, message failure must be prevented. As a result of this research, the system can hunt for other routes to ensure that the data received from the node is properly transferred to the sink (Sookyoung Lee et al. 2010). In recent years, numerous applications have fueled WSN research. Risky vocations such as coast and border defense and search-and-rescue stand out for their commitment to saving lives. If tiny sensors were employed to work in such a hostile environment without connection failure, the application's cost would be lower and the risk to human life would be lessened. A sensor node is often powered by batteries while interacting with other sensors (Sookyoung Lee et al. 2010).

Static and portable agents are both used when employing WSN's location-aware event-driven multipath routing (LEDMPR). Two types of software companies manage the detection and configuration of numerous pathways in WSNs. Each sensor node is assigned an agency, and each sink agency is assigned a sink/base station (SA). The following is a breakdown of how it works: Using location information, the event node calculates an arbitrary midpoint between the event and sink nodes. Position data and a mobile agent assist the affair node in determining the quickest route from its current location to the sink node, which it then uses as a guide. Along the journey, it collects and provides path information and node parameters to the sink node. Half-way location information is used by sensor nodes to compute the arbitrary position of a particular (middle) intermediate node (Sutagundar et al. 2013). We are striving to create a dependable geographic routing strategy for locating dispersed Wireless Sensor Networks. Keep in mind that energy efficiency and load balance should be considered when building the algorithm. The proposed technique incorporates two critical components for increasing network energy efficiency: an estimation strategy for Packet Reception Rate (PRR) links and a learning mechanism for local network load balance. These elements enhance delivery quality while also bolstering the network's long-term viability (Ramadoss et al. 2014).

The design of a network route from a source node to multiple destinations, the WSN employs a link stability-based multiple routing technique. Transmission of data from source node to a recipient unit, stable connections create a multicast mesh. Each stage of the procedure is divided into the following categories. Mesh networks use two packet types: route request and route reply (1). It is used to explore paths between source and destination node pairs that comply with the link stability criterion for selecting stable forwarding nodes (SFNs). To deal with broken couplings, the mesh must be modified.

According to LSMRM, both SFN nodes and multicast sources/receivers experienced connection problems. When a link between two SFNs fails, the node that discovers it attempts to locate the mesh's next reliable link and delivers the packet over it.

Any forwarding node that loses contact with the source will receive a RE message instructing it to relearn the routes (Abedalmotaleb Zadin et al. 2013). As the foundation for EENDMRP, the route maintenance analytical model focuses on node level redundancies across a single path, multi-node over a single path, and multiple-level nodes in a single path (Sheng Liu et al. 2013).

To gain a faster routing result in B-AODV, utilize BRREQ instead of PREP. The use of a two-hop IP trace in control messages and routing tables can speed up route repair and reduce route finding time. It also improves the Ad Hoc network's operation. Because the AODV protocol is in short supply, a new protocol is required to minimize route failure, message loss, and network disturbance. The network link is considered to be bidirectional in the B-AODV approach, meaning that the source and destination nodes can be reached via a single path (Thuy et al. 2013). Two heuristic approaches are employed in SJFR to prioritize the number of new nodes and the length of the pathway over other parameters.

This method is not without its difficulties. While attempting to apply it, the agent will encounter infertile routes and broken radio connections. As a result of new information, the initial plans will need to be revised. When it comes to changing your plans, you have two options. Re-planning is required when new information is obtained that increases the cost of the previous plan or renders it impracticable. If there are significant changes to the current course, this strategy will revert to a complete re-planning.

To determine which options, operate best, different densities of connection difficulties and harm are imposed on a simulated situation. Thorough planning produces better results but takes significantly longer to complete as damage and densities increase. Because the entire time required to implement the plan is known, comprehensive re-planning becomes competitive. Slower moving agents will have their journey shortened by the route heuristic, whereas faster moving agents will have their path extended. The node heuristic with complete re-planning, on the other hand, becomes more efficient as damage accumulates, even for objects that move swiftly. As a result, the programme must choose between reducing node spending and expediting repair operations. The findings demonstrate how it accomplishes this (Wang Guodong et al. 2010). A brand-new QoS routing design is provided to alleviate congestion, balance load, and reduce data loss. As a result, communication costs may be reduced while network quality is maintained (Ramadoss et al. 2014). Self-route selection methods were developed by Thomas Babbitt et al. (2009). In this routing system, a data is enrouted from a source to a destination, and each node competes for self-selection based on backoff delay. There are various options for disconnecting and reconnecting, each with its own set of constraints. To reduce route finding costs, ad-hoc routing systems must improve their QoS characteristics by localizing connection failure recovery (Anya Apavatjrut 2012).

2.1 Wireless communication networks

According to industry analysts, wireless communication networks is going to play a significant role in the upcoming times. Recent advancements in wireless communication and low-power technical capabilities have ignited spark in revolutionizing Industrial Wireless Sensor Networks (IWSNs), which provide a number of benefits, including ease of installation. Factory automation, industrial process monitoring, and plant monitoring are all examples of IWSN applications. Traditional routing protocols such as AODV (Perkins et al., 1999), AOMDV (Marina et al., 2001), and DSR may not be suitable for usage in industrial settings due to extreme situations, interference concerns, and other constraints (Johnson et al. 1996). Single power unit is used to make the entire wireless sensor network up and running, using single-hop or multi-hop communication.

A damaged link in a sensor network might cause packet loss or delay. Missing a control deadline is unacceptable in most industrial applications since it can generate confusion in the automation or even cause it to stop, both of which result in financial losses. The collected data must be correct and provided to the sink node in a timely manner. As a result, reliability and energy efficiency are crucial for a WSN's efficient operation. It is challenging to deliver sensed data to the sink in a resource-constrained setting. A multitude of causes, including channel obstructions and interferences, can cause connection failure. As is always the case, predicting where the connection will break and then rerouting the operation is impossible.

Wireless channel conditions change over time, resulting in sensor node failures and network topology changes, making it difficult to transfer a packet safely at each stage. It is possible to retransmit data through the communication network. Unwanted delays arise, and as a result, the network consumes more energy. OR has been presented as a realistic cross-layer strategy to combat fading wireless networks, boosting the robustness and energy efficiency of the networks as a whole (Biswas et al. 2005).

Routers utilize opportunistic strategies to take use of wireless communication's broadcast feature, which has multiple sender neighbors. Because the wireless channel is shared, each node may hear data packets broadcast by its neighbors. The network layer will utilize the priority of the data packet to determine which forwarding candidate the packet is forwarded to. The MAC layer chooses only one node as the real forwarder a posteriori.

Wireless communication is a key performance bottleneck in WSNs. When a connection breaks, it has a negative impact on the network's performance, reliability, and availability. If a connection in a WSN fails, data must be sent via an extended channel. As a result, transmission times are extended and energy consumption is increased. There is a problem as soon as the sensor and sink are too near together. Wireless networks are highly susceptible to factors like node power consumption, battery life and interference along with fading. The process of determining the position of sensor nodes is referred as localization. The distance or angle between nodes in a communication network determines their position. Range-based or range-free techniques can be used, as well as anchor-based or anchor-free localization schemes, fine- or coarse-grained localization schemes, GPS-based or GPS-free localization schemes, central or distributed systems, and static or mobile nodes. There are a number of options.

The placement of sensor nodes is essential in WSNs (Kulaib et al. 2011). Based on where the computer work is done, WSN localization methods may be categorized as centralized or dispersed. In the world of distributed WSNs, node localization is a difficult and critical topic. In many applications, such as item tracking and monitoring and location routing, knowing where sensor nodes are in relation to one another is critical.

The localization method of WSNs is a crucial issue in development and operation (Sayadnavard et al. 2010). Many WSN applications need accurate localization techniques, and standard node localization algorithms fall short of the mark. Learning Automata is used to create and incorporate a technique for predicting node placement.

WSN has created a range-free localization system based on directional antennas. The mobile beacon node utilizes multiple directional antennas to send out packets in K directions as it travels (Zhuhong You et al. 2007). Ordinary sensor nodes can only detect their position by using the signals from a single virtual beacon. It can broadcast signals of different power levels to calculate the approximate distance between nodes. The algorithm's two most major advantages are its simplicity and cost-effectiveness.

Using position data obtained from several nodes, a WSN localization technique was created (Pei et al. 2011). This localization approach is well-suited for WSNs of various sizes because to its efficiency, high accuracy, and ease of computation. Furthermore, based on this algorithm and the requirements of the medical monitoring system, this paper proposes a dependable and efficient WSN structure. Survivability of multi-domain networks is a difficult and critical topic in optical WDM networks (Bhas Raj Pathak et al. 2013). The major goal is priority-based data flow with an emphasis on network quality-of-service (QoS). This method combines the P-cycle and wavelength allocations of the network.

The battery discharge model, sensor node power consumption in various modes, and wireless channel conditions are all included into a time-dependent link failure model (Zonouz et al. 2014). While transmitting data to main node via various routing techniques, the effects of a connection failure on communication reliability, network coverage, network architecture and energy consumption must be assessed. Because of its better accuracy, the shortest path distance approach outperforms the shortest path hop methodology. When they converse, they use more energy.

Due to dynamic multi-hop topologies, lossy and noisy communication channels, and intermittent connections, wireless multi-hop ad-hoc networks are plagued by link failures (Valera et al. 2010). Network routing systems must be able to recognize connection failures quickly and correctly in order to function effectively and productively. Link layer feedback is used in a unified link failure detection and recovery architecture for fast failure diagnosis and packet salvage for packet recovery. Models and basic experiments were used to investigate link layer feedback and packet salvage. In existing network simulations, link layer feedback performs worse than hello beacon owing to the huge number of false failure detections it generates. This approach aids in reducing the number of false positives. It decreases erroneous detections; therefore the veto approach enhances link layer feedback performance in respect to packet delivery, latency and routing efficiency.

Nodes capability to move is inversely proportional to their speed. The network gets more unstable as nodes move faster. The connection failure rate, on the other hand, is frequently employed in theoretical research to forecast wireless network stability (Shu et al. 2007). The failure rate of connections grows as there is increase in the average speed of the nodes. However, simulations have demonstrated that this conclusion holds true whether the usual random waypoint and random direction models are used. This was achieved by employing a mobility model with a number of constraints.

This article examines all optical networks, including fibre optics, for potential failure points (Ahuja et al. 2009). Monitoring refers to the monitoring cycles and monitoring pathways used to detect single link failures (MPs). There must be one or more monitoring locations for MCs and MPs to pass through. They are constructed in such a way that when a single connection fails, a unique mix of MCs and MPs fail, which then flow via the monitoring station. Building MCs that uniquely detect a single link failure in a network with only one monitoring point, according to the results, needs a three-edge connection.

As a result, MCs are created as an Integer Linear Program that is represented as a problem (ILP). In the presence of one or more monitoring stations, heuristic approaches for MC construction have been developed. A defect localization approach based on MPs and MCs, as well as a profusion of monitoring sites, is given for each network.

When designing the future generation of communication networks, network resiliency must be taken into account (Kavian et al. 2010). When several links in an optical network break at the same time, a multi-link failure scenario might be useful as a modelling tool. A genetic algorithm is used in Dense Wavelength Division Multiplexing (DWDM) optical networks with dual link failure coverage. The Dedicated Path Protection (DPP) design is used in the demand matrix to connect disconnected light lines between O-D pairs. It is the first and shortest light path utilized for work, and all other light channels are employed to protect it. A genetic algorithm may be used to create an optical mesh network with excellent fault tolerance.

When developing a monitoring system, unreliable local measurements are taken into consideration. Maximum A-Posteriori (MAP) detection of link failure is utilized as long as the network monitor has previous information of the network's starting condition (Dhal et al. 2013).

The detector and its performance are explained using three characterizations: algebraic, spectral, and graph theoretic. This is especially true when a connection fails or when there is insufficient data to identify it correctly.

2.2 PROTOCOL

The wireless sensor network differs from other networks in that it is an event-based network. The amount of nodes in wireless sensor networks is higher. The sensor nodes are all small, light, and easy to move from one location to another. The main battery provides electricity to the nodes (Penella et al. 2009). The amount of electricity drawn from the nodes' batteries determines their capacity (Thakar et al. 2015). It is possible for the network to be flat or clustered. A flat network fails when it comes to supporting huge number of nodes the control overhead is directly proportional to the network's size. It will have a negative impact on the overall functioning of the network (Mamoon et al. 2016). Sensor nodes in a flat-based network all have the same roles and tasks. Their roles and tasks, however, differ in a cluster network. A cluster-based network is the ideal choice if the network requires the best communication even after scaling up (Singh et al. 2015).

Mamun et al. evaluated flat and cluster networks for topology management (2012). They looked at things like overall energy usage, energy distribution, load distribution, communication redundancy, and data dependability. The cluster network wins with a score of 32, while the flat network loses with a score of 23. According to, a cluster-based network outperforms a flat network (Jamatia et al. 2015 and Din et al. 2007).

Cluster networks were created to improve network performance. Cluster networks may be divided into two types: centralized and scattered. A single node controls all nodes in a centralized cluster, but all nodes in a dispersed cluster have the same priority. When flat and cluster network designs are compared, cluster network architecture has the longer network life (Aslam et al. 2016 and Song et al. 2007).

Both even and asymmetrical clustering are possible. The count of nodes in each cluster is same under equal clustering. Uneven clustering indicates that nodes are not spread evenly. Clustering can occur in larger networks due to uneven clustering. Uneven clustering will help the network last longer (Arjunan et al. 2017; Li et al. 2005; Jiang et al. 2009 and Zhang et al. 2017).

There are two types of cluster formation: static cluster formation and dynamic cluster creation. Dynamic clustering may be classified into two types: centralized and scattered. When using the terms homogeneous and heterogeneous, it is possible to refer to either centralized or distributed clustering (Aslam et al. 2016). The cluster network employs a plethora of routing methods. The use of a cluster-based system is used to teach multipath routing (Sharma et al. 2015). There has also been discussion of adopting a clustered QoS routing protocol (Lakshmi et al. 2016). Because of a broken temporal link, a WSN with a dynamically dispersed topology fails (Singh et al. 2015).

The Ingle et a approach dynamically authenticates users in wireless networks for security concerns (2015). If the network's topology changes, a new authentication method will be necessary. The time it takes to complete things has grown, as has the time it takes to begin them. To solve database-related issues, a cluster architecture for dynamic wireless networks-based data replication is given. This method improves scalability and dependability at the same time. Two difficulties occur in terms of network node dynamics and connection failure frequency (Qayyum et al. 2015).

When nodes may be relocated, a method based on a swarm intelligence approach to analysing location may be utilized to construct the best wireless network link feasible. Throughput will increase as the number of dropped objects decreases (Sumathy et al. 2015 and Penella et al. 2015). Another approach is to utilize clustering and multipathing as a sensor network routing strategy. The network's overall energy consumption will be decreased (Sharma et al. 2015). A dependable solution is necessary to address mobility concerns while also increasing network performance (Atani et al. 2015). Green cluster technology was utilized to create energy-efficient wireless clusters that also extended network life and enhanced battery performance (Tseng et al. 2015).

Sensor nodes in a wireless sensor network are randomly distributed and connected through wireless links based on well-proven routing algorithms, providing effective ways for linking many distinct geographical areas in a single network. We can track and analyze a wide various physical and environmental variables that have a major impact on national growth as long as this WSN is in place. These WSNs can monitor inventory flow, identify terrorist movements, and detect seismic activity in addition to listening for acoustic communications. They can also be utilized for medical monitoring, military surveillance, and intelligent environments. Tens of thousands of nodes utilize intermediary nodes to build communication links that allow them to exchange data across long distances. The creation of a global network requires coping with obstacles such as limited bandwidth, high failure rates, and power. This is a challenging task. Leading the network is important for a variety of reasons, including assisting the system in focusing on developing dependable and energy-efficient procedures after conquering challenging barriers. The consumption of energy by nodes should be optimized in order to extend the network's lifespan. The effectiveness of data tracking is determined by the sort of sensors used for various reasons. If we wish to avoid more crises, we should utilize these data to permanently reduce energy use. Nuclear reactor sensors must spend less energy in order to ensure the network's long-term viability. When developing a protocol, the type of the application is the most important aspect to be considered. Historically, most WSN routing strategies were intended to take use of WSN's unique characteristics.

Rather than examining everything that has come before, we concentrate on the studies that are most closely connected to our technique. This protocol makes use of hardware to assist with the energy issue. It is not compatible with large networks (Tianshu Wang et al. 2016). The use of a hybrid method aids in energy conservation. However, it lacks the energy required to be thrilling (Priya et al. 2016). This article investigates many alternative QoS-based routing methods (Chen et al. 2004). Sequential Assignment Routing (SAR) was the first routing system to provide Quality of Service (QoS). The research of Sohrabi et al.

A cluster-based QoS-aware routing protocol based on the queueing paradigm is described (Akkaya et al. 2003). This system has the advantage of being able to handle both real-time and batch data. Its major concern was end-to-end latency, which links networks based on cost functions. The K-least cost path technique was used, which evaluates all potential routes against end-to-end restrictions to determine the most economical option. The data will be transmitted from the origin to the destination through this path. The bandwidth ratio is the same for all network nodes. No additional network capacity will be required as a result of this. This protocol has a significant fault in that it fails to account for transmission delay and expenses, resulting in delays from end to end across the network.

SPEED4, a renowned QoS-based routing system at the time, provided an end-to-end latency solution for real-time traffic. It uses sensor node position data to determine the most cost-effective path. In order to achieve efficiency, end-to-end latency is determined by distributing the whole distance based on the packet delivery speeds of the nodes (Tian He et al. 2003). When the network becomes overloaded, jamming occurs.

It is feasible to obtain excellent QoS in wireless sensor networks using MMSPEED (Felemban et al. 2006). It was possible to provide various QoS supported by numerous routes by changing delivery speeds and forwarding data at a defined pace. The dependability of this procedure is questionable.

An MCMP protocol that uses the best available routes is being developed in order to send packets to target nodes as efficiently as feasible (Huang et al. 2008). This study looks at QoS in regards to latency and reliability. Delays from start to completion are created by a linear integer programming problem that must be resolved.

The ECMP protocol is designed to meet QoS requirements while consuming as little energy as feasible in regards to hop count and energy usage (Bagula et al. 2008 and Igor Ganichev et al. 2010). The EQSR multipath routing protocol (energy-efficient and QoS-aware) operates in a similar fashion, trying to balance network device energy consumption.

LEACH is a commonly used clustered wireless sensor network routing technology. To construct the cluster's head, the sensor nodes are chosen at random. LEACH does not have an energy gap since the cluster heads are located distant from the base stations. Delays are a concern (Heinzelman et al. 2000). It is feasible to choose the cluster head by combining the residual and reference energy connections in Hed8, a common clustering-based routing approach (Younis et al. 2004 and Daya Lobiyal et al. 2016).

The CACH protocol, which is based on the environment, was designed to aid in cluster formation. It was only concerned with network traffic and cluster header load balancing (Haque Md et al. 2009). The NSN routing technique is offered, although it solely takes into account energy consumption rather than Quality of Service (QoS) (Chaaran et al. 2010). The EEHC protocol was created for networks with just two hierarchies and heterogeneous clusters (Kumar et al. 2009). There is a QEMPAR protocol in place that considers both end-to-end latency and energy usage (Saeed Rasouli Heikalabad et al. 2011).

Sensors in a WSN are distributed across a broad area and may be used to analyse local conditions (Ameer Abbasi et al. 2013). Using the sensors as remote data gathering devices, performance artist hubs analyse sensor signals and take appropriate action (Akyildizand et al. 2004). All sensor systems are distinguished by the need for vitality, productivity, flexibility, and adaptability to slight failures (Arunanshu Mahapatro et al. 2012). When using sensor nodes as a network, you will need to solve certain very specific difficulties. One of these impediments is the management of a WSN's topology. Topology management is dependent on the ability to maintain a fully connected network throughout the life of a WSN (Stankovic et al. 2003).

Sensor systems require power protection since sensors have a limited quantity of power. Allowing a node to rest while not in use is one approach to maintain control. Topology management organises nodes that have disabled their radios in order to maintain movement transmission attractive while decreasing system power consumption (Schurgers et al. 2002 and Tsiatsis et al. 2002). When dealing with connected networks, the decision of which node to let rest and for how long must be made. As a result, time-sensitive data is never lost or delayed (Subasini et al. 2015). For sensor systems, a distributed failure plot has been proposed (Chen et al. 2006).

For dealing with node problems, the LeDiR technique is recommended (Abbasi et al. 2013). Tree Topology combines star and bus topologies. Because of the tree structure, we may have several servers on the system that are distributed in different directions. Many network providers and equipment manufacturers support this concept as well.

When the system is extensively spread and endlessly fragmented, a tree structure with many branches is preferable. The benefits and drawbacks of tree topology are the same as for any other topology. Using a tree structure for small networks may be a waste of connections because it may not adapt adequately. Tree Topology includes various constraints, which must be considered throughout the configuration. Tree networks can be utilized in building a point-to-point link. Every node interacts with the central node and the ad hoc networks that arise. The length of the network is defined by the type of link used.

The following features are seen in tree topologies: Trees typically have at least three layers of hierarchy, with each branch interacting with the root node to carry out its duties. For associating with nodes, the tree architecture demands the employment of the star and straight methods. The cumulative count of nodes in the system is considered rather than the count of nodes at each level of the tree topology. There are no limitations on the number of nodes that may be added to any degree of importance in the chain considering the total count of nodes is not exceeding a particular quantity.

Meanwhile, all nodes receive signals from the root node. As a consequence, you'll have a better grasp on how everything fits together. To be successful, the tree topology's capacity to extend outward must be unrestricted. To join the network as a whole and add new root nodes (Subasini et al. 2015). Node disappointments and environmental hazards create topological changes, communication failures, and network dispersion. These problems are far more common than they would be with a normal remote control. More than 80% of real framework difficulties are caused by discontinuous defects (Horst et al. 1993 and Siewiorek et al. 1982).

The intention behind this project is to develop a programmable online broadcast system for detecting sensor network problems (Arunanshu Mahapatro1 et al. 2014). The arrival time of packets in the queue identifies the issue node (Manisha Wadhwa et al. 2014). Administrators who desire a dependable network that is not interrupted by external causes will require effective network execution monitoring (Ma et al. 2015).

In sensor networks, edges are the connections between nodes. It's possible that interference, bad weather, and field obstacles can contribute to channel loss. Sensors can fail for a variety of causes, including insufficient battery power, catastrophic occurrences, severe weather, or violent attack. Transmissions between nodes may be hindered or stopped in the same way. It's critical to understand how sensors work in these situations.

A larger battery limit is helpful in some applications, such as electric automobiles, to alleviate consumer concerns regarding driving range. The high self-release and fast corrosion of lithium-sulfur batteries are still being investigated (Propp et al. 2017 and Mikhaylik et al. 2010).

The following battery characteristics must be addressed in improving operational management, according to the kinetic battery concept: Based on its charge state, ht char is the maximum amount of energy a battery can absorb in each discrete time step t. (kWh). Maximum nominal voltage V, which is the manufacturer's indicator voltage; minimal condition of charge S, where the battery should not be depleted to avoid irreparable harm; S (kWh) is the minimum charge condition. The battery has been entirely drained when it reaches its ht dis (kWh) capacity. The highest charge current I (A) is the most severe charge current under all charging situations; the nominal voltage (V) is the manufacturer's indicator voltage; and, lastly, ht dis (A). The battery's apparent Q-max limit shows its evaluated limit (kWh). The battery's roundtrip effectiveness E (percentage) shows the battery's inherent health (Manwell et al. 1993).

Coulomb counting is a method for determining the number of items in a given space. SOC may be calculated by observing the charge flowing into and coming out of the battery. This is an easy approach to use. Calculating the SoC from the equation below is fairly simple given a starting stage SoC0 and its corresponding capacity.

Aishwarya Karmarkar (2020) et.al WSNs are recently used to solve a broad range of physical world concerns, including environmental monitoring, home automation, and medical monitoring. Small wireless nodes in these systems are susceptible to failure due to hardware and software issues, as well as excessive energy consumption. Faulty sensor nodes may provide incorrect data, reducing WSN performance. Finding and diagnosing problems is a major issue with WSNs. A Support-Vector Machine enhanced in this study provides wireless sensor network defect assessment (SVM). To detect sensor node failures and inform the user, the suggested technique employs a Grey Wolf Optimization (GWO)-based SVM classifier. It has also been recommended that a cluster-based architecture, which consumes less energy, be used. Using a large number of computer simulations, the suggested fault detection approach was tested in a range of network topologies.

Rakesh Ranjan Swain (2017) et.al, a particle swarm optimization (PSO) approach was used to create a soft fault detection model for wireless sensor networks (WSNs) in actual time. The three phases of the diagnostic process that the suggested technique isolates in order to discover sensor network composite defects are initialization, fault detection, and fault categorization (combined problems of soft permanent, intermittent, and transitory nature). An study of variance may assist you in locating the network's troublesome nodes (ANOVA). The feed forward neural network (FFNN) and the PSO learning algorithm are used to classify defective nodes. In a controlled indoor environment, we will put our theory to the test.

Yasir Abdullah (2021) et.al In wireless sensor networks, there is a lot of emphasis on data consistency (WSN). Sensor nodes that are left unattended are subject to harm from a variety of sources owing to changing environmental conditions. Some sensor nodes may also be hacked, with original detected data taken and changed, resulting in inconsistent data from failed or compromised sensor nodes. The data discrepancy may be traced back to the network's incorrect detection of abnormal data. An adaptive mountain clustering approach for detecting anomalous data is given, which decreases unnecessary data transmission to the end user while improving data accuracy. The suggested approach is successful in detecting anomalies as long as the false alarm rate is low.

Li Liu (2020) et.al Border tracking is an essential issue for industrial wireless sensor networks when working with continuous products (such as gaseous chemical compounds, oil spills, and radioactive waste) (IWSNs). To build an IWSN continuous object boundary tracking method, we employ sensor node collective intelligence and machine learning capabilities. The method recommends beginning with an upper limit on the event zone covered by continuous objects. The coarse-grained border areas can be mapped using a complete binary tree-based split of the event region. To learn more about the irregularities of continuous objects, a binary classification problem is utilized. According to the simulation results, employing the proposed technique, good tracking accuracy may be achieved with fewer border nodes. Because of the fault-tolerant algorithms, the suggested solution is resistant to erroneous sensor readings when used in industrial settings, even if a small number of nodes fail.

Pialy Biswas (2019) et.al Data aggregation, fusion, and collecting techniques are rapidly being used in wireless sensor networks (WSN). The wireless node receives information and sends it to the final point for analysis and storage as part of a WSN network. WSN's utility is limited by insufficient battery and costing of the nodes also limits its usage. Due to resource constraints, flaws in WSN sensor nodes can be easily exploited. Detection by prediction models using data fusion may be a great option for locating the issue more efficiently. Because of the sensor node's limited storage and processing capacity, an Extreme learning machine/Kalman filter hybrid predictive classification technique is developed. Instead of utilizing more data, the Kalman filter trains the sink node with the erroneous data pattern. In the discussed study, random anomalies are injected into standard WSN data to examine how they impact the outcomes. Performance is measured by factors such as detection accuracy and computation time.

Sachin Dhanoriya (2017) et.al recent advancements in sensor nodes and sensor networks have had a tremendous influence on the society we live in today. Sensor nodes and sensor networks will become increasingly important in sectors such as research, health, and the military as our daily lives become more automated. As sensor nodes and sensor networks develop, a rising number of anomalies and errors are associated with them. These discrepancies jeopardize the consistency and dependability of sensor networks. This review article for sensor nodes examines many fault-tolerant methods for sensor nodes and networks that deal with failures, bridges, and radiation effects.

CHAPTER 3

METHODOLOGY

Faulty nodes may degrade the functioning of the WSN sink node by delivering erroneous data to it [5, 6]. Rapid and precise fault detection and management methods are required to ensure WSN QoS and resilience [7]. WSN issues may be identified and addressed in a variety of ways, including self-diagnosis done by the system, distribution techniques and centralized solutions methods (e.g., Centralized fault identification methods, one or more sink nodes are in charge of fault handling [9]. These sensors are more powerful and quicker than standard sensor nodes. Sink nodes in cloud-assisted WSNs have been proven to transfer captured information to the servers conductive to processing and analysis [10–12]. WSNs that utilize centralized methods attempt to conserve energy by outsourcing fault management to the sink node, however this consumes energy that would otherwise be used by the sensor nodes [13]. Extra storage is necessary to preserve the sensor's gathered data. The amount of energy needed to transmit defect data to the target node increases as the network expands. Every single fault management activities are done by some particular nodes in distributed fault detection systems [2, 14], and no data relevant to the problem is provided to the sink node. Using cluster heads as an example, cluster representatives in clustered WSNs can obtain fault tackling information from cluster heads and participate in fault handling procedures and data [15, 16]. Distributed fault detection systems are more adaptive to big networks than centralized ones.

3.1Fuzzy system

Uncertainty, indecision, vagueness, and ambiguity are all terms that describe fuzzy situations. The degree of truth is used in fuzzy logic, which is a computer approach. To generate a specific output, the degree of truth between input and linguistic variables is used by fuzzy logic. The output's nature is determined by this input's condition. Unlike Boolean logic, which only uses two categories, this method uses three (true or false). Objects are described using 0 and 1 in boolean representation of the logic. The temperature of water in a glass, for example, could be High (1) or Low (2). (0). More fuzzy logic categories are used to describe the water, but they all fall into the same two groups. The water could be extremely cold, extremely warm, or really warm in this scenario. Let's look at a different scenario. Let's pretend we're asked a question. The answer is either yes or no according to Boolean logic. The answer could fall into one of these two categories in fuzzy logic. In this reasoning, possible yes, possible no, and definitely no are some of the possible answers. In the two instances above, we see that fuzzy logic systems use degrees of possibility instead of precise categories. Following are used in regards to formulating a straightforward output,

Fuzzy logic: The complication arising due to unsureness in the engineering sphere is addressed by fuzzy.

- When accurate reasoning is not available, it provides a degree of thinking that is close to accurate.
- Fuzzy logic has a straightforward framework that is simple to comprehend.
- The method of controlling machines is extremely effective.
- There are solutions to a variety of industrial difficulties provided by this company (especially decision making).
- It only takes a small amount of data.

Below diagram depicts the architecture of fuzzy logic.

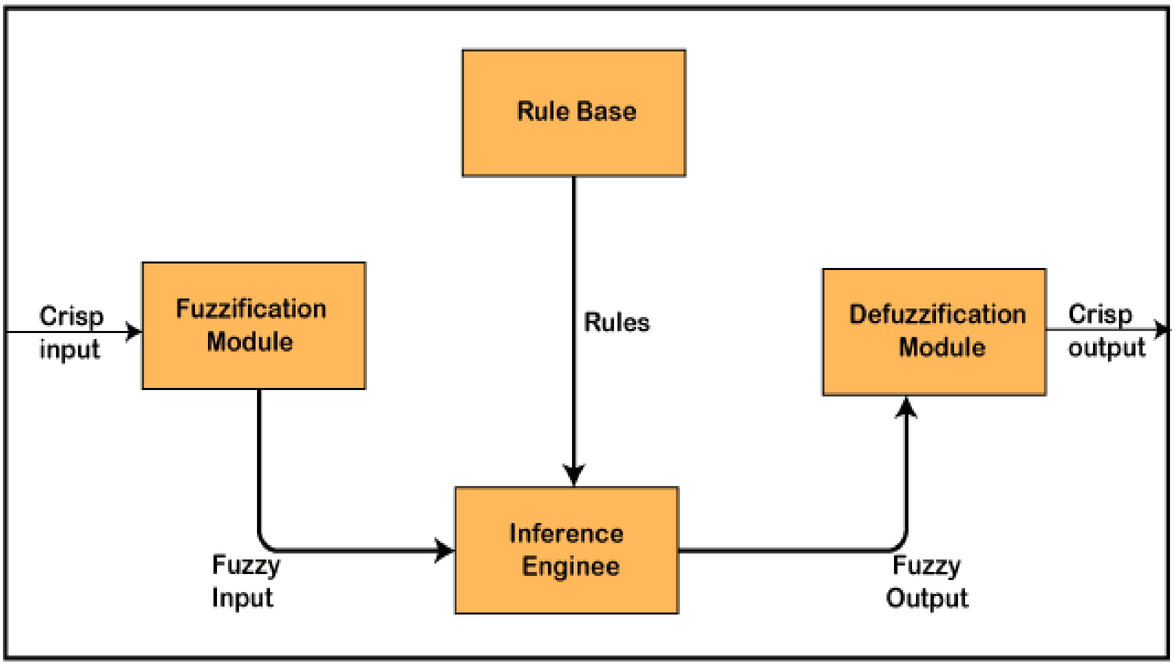

Figure 3.1 fuzzy interference system

The components can be explained as follows:

- **Rule Base:** fuzzy logic is controlled by two main factors which are termed as rules and membership functions. These are responsible for the control over decision making or governing aspects. It consists of a series of IF-THEN statement conditions required for provisional programming and controlling system.
- **Fuzzifier:** Fuzzy sets are generated from the raw inputs by this component. A control system further processes the fuzzy sets before sending them on to the next step

- **Inference Engine:** This part is responsible for determining the best input rules. To get fuzzier result, it applies the guidelines above to the input data.
- **Defuzzifier:** This is a tool for figuring out which input rules are the most effective. The input data is fuzzier by following the following principles.

3.1.1 Fuzzy logic membership function

A fuzzy set's membership function is represented graphically by a membership function. It demonstrates the mapping of inputs to values in the 0–1 range. The most common input format is Universe (U). The fuzzy set's membership function has the form:

$$\mu A:X\rightarrow[0,1]\ \mu A:X\rightarrow[0,1]$$

Here, A is an undefined set, and X is everything. Any number between 0 and 1 represents the level of membership. Each X-element (Universe element) is assigned a membership degree. To put it another way, the membership function estimates or computes the amount of ownership and compliance of a specific input entry in a particular fuzzy set. The x-axis represents the Universe, and the y-axis represents the degrees of membership.

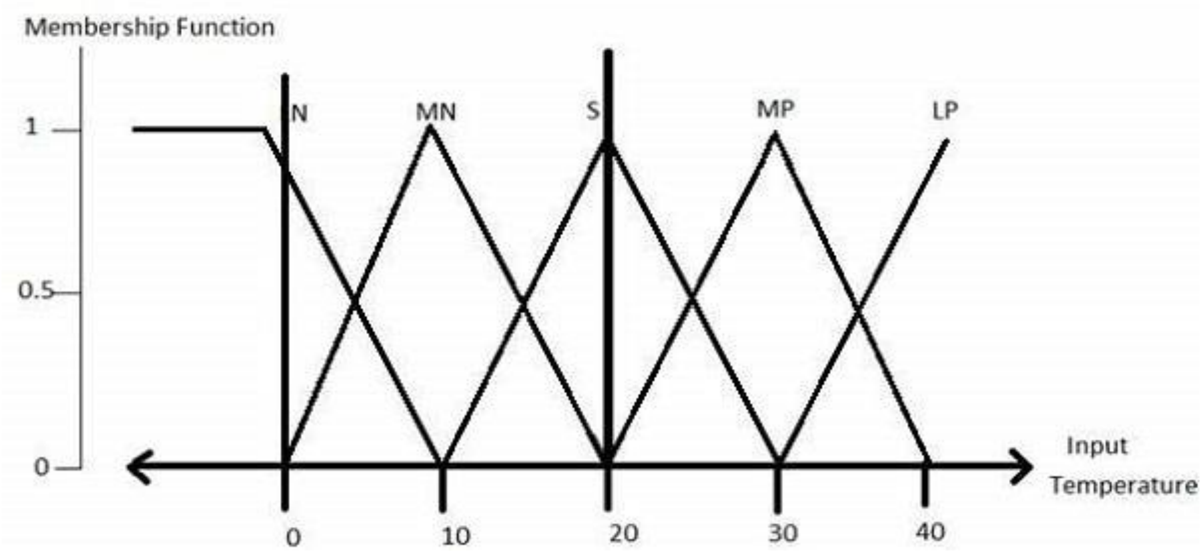

Figure 3.2 fuzzy membership function

3.2 TYPES OF FIS SYSTEMS

Fuzzy inference systems are classified into following models:

- Mamdani fuzzy model
- Takagi –Sugeno fuzzy model

- Tsukamoto Model fuzzy model

3.2.1 Mamdani fuzzy Model:

Mamdani fuzzy inference was first presented by E. H. Mamdani, as a way to regulate engine operated by steam with the help of a set of linguistic control rules gathered from the relative experience of human operative. Input and output membership functions are linguistic variables in this approach. The steps below must be followed for the implementation:

Step 1: The set of conditional statements that describes specific type of engagement between the input and output membership functions is termed as fuzzy rules. Categories or level of engagement is described by low, medium and high values assigned to the inputs are referred to as linguistic variables or membership functions. This is accomplished by the use of expert knowledge.

Step 2: The process of conversion of discrete data to fuzzy data is termed ad fuzzification.

Step 3: The rule strength is established by combining the fuzzified inputs in correspondence to the set of fuzzy rules defined. This is accomplished by the use of fuzzy combinations or T-norms such as fuzzy and, fuzzy or, and Boolean or.

Step 4: The rule's consequence is the result of the combination of rule strength with the output membership function.

Step 5: Combination of every output from all the fuzzy rules for the formation of distribution.

Step 6: In the majority of applications, a sharp output is necessary. The process of converting fuzzified information fuzzy data to crisp data is known as defuzzification (single value). There are numerous approaches that can be employed for this.

3.3 ADAPTIVE NEURO FUZZY INFERENCE SYSTEM (ANFIS)

The adaptive neural fuzzy inference system (FIS) is the system that formulates the input-output mapping (ANFIS). Fuzzy logic (FL) and artificial neural networks are utilized (ANN) for mapping between inputs to outputs. Obtaining and distributing membership functions and implementing fuzzy rules represents some major challenges in aspects of FIS. These values were determined using an elimination and testing procedure. ANFIS modifies the parameters using neural networks. The ANFIS ANN component facilitates error reduction and parameter tuning. FL distinguishes itself via its ability to deal with ambiguity and organize knowledge. ANN is capable of learning. ANFIS benefits both FL and ANN. As a result, FIS is already being used as a critical research step in disciplines namely automated control, data categorization and classification, decision making analysis, development of expert systems and cutting edge technology of computer vision. The major goal of ANFIS is to employ fuzzy inference systems to discover near-optimal membership functions and other parameters utilising a hybrid learning method and input-output data sets [13].

The layered structure of ANFIS is comparable to that of neural networks. The ANFIS system is divided into five tiers. These layers contain nodes that are both flexible and stiff. The representation of adaptive nodes is done by using squares in the design and fixed nodes are denoted by circles. Figure 3 depicts the overall structure of ANFIS. A first-order sugeno with two inputs is used to describe the architecture (x and y).

The strengths of both artificial intelligence techniques are optimized while the flaws of each approach are minimized when utilizing ANFIS to produce an adaptive system that excels them both in terms of performance and intelligence [25]. Because the reasons that may lead to handover in mobile networks are unpredictable along with being irregular in nature, the ANFIS method is utilized in investigation of patterns of these parameters changing with respect to time and establishing a network that can be trained to imply handover decisions in regards to change in the data during due process of training. ANFIS can supervise learning while also constructing fuzzy membership criteria based on previously gathered input and output data by combining an artificial neural network with a fuzzy inference system [26]. [26, 27] formalized paraphrase

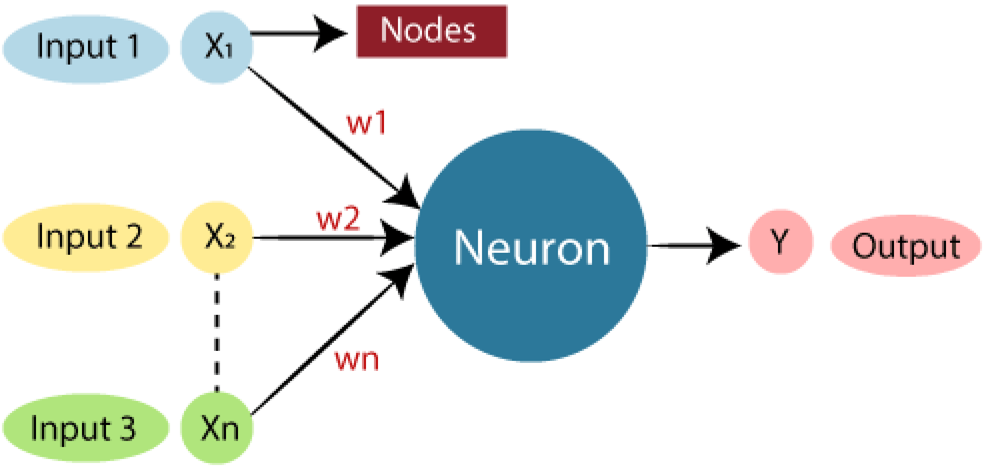

Figure 3.3 function block of Adaptive Neuro Fuzzy Inference System (ANFIS)

The role of dendrites in biological neural networks, has been taken by the collection of the inputs in artificial neural networks. The biological network's most important part is cell nuclei which is represented by Nodes, the synapse being represented by weights and axon as outputs. How biological and artificial neural networks are related

With the use of an ANN, computers will have the ability to understand and make judgments like humans because it aims to imitate a functioning human brain's network of large number of interconnected neurons. The human brain is made up of about thousands of billion neurons. Every neuron has between thousands and hundred thousands of association points. Info is scattered all across the brain, and multiple pieces of this data can be pulled from our memory memories as needed. The human brain is said to be made up of very powerful parallel processors.

3.3.1 Architecture of an artificial neural network:

For a better understanding of the artificial neural network design, it is important to develop an understanding of basic components of a neural network. The neural network is composed of huge number of artificial neurons that are layered together. Consider the numerous layers that comprise an artificial neural network.

Three layers depicted under artificial neural networks:

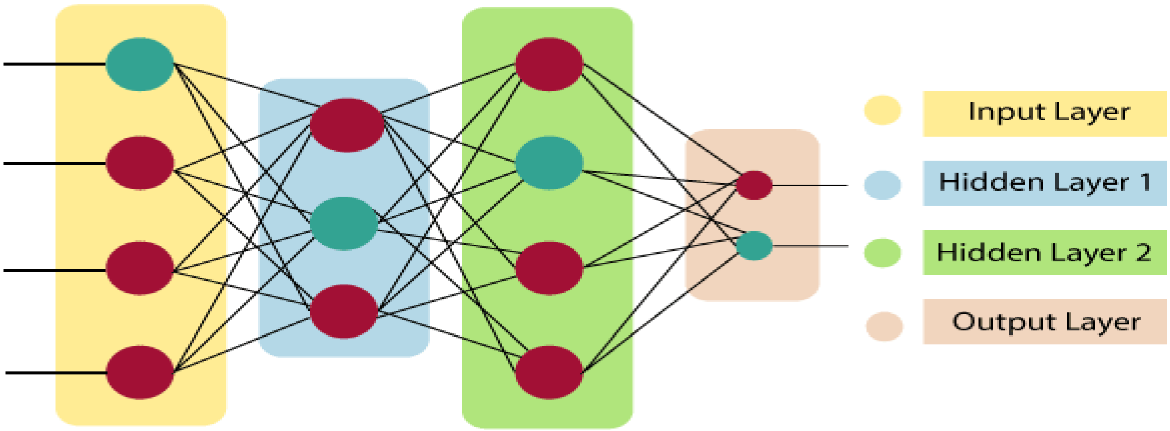

Figure 3.4 layer architecture of an artificial neural network:

Input Layer: A layer of inputs from environment.

Hidden Layer: Its role is to perform all the necessary and required mathematical calculations in order to obtain some of the hidden patterns and features.

Output Layer: The final outcome is provided by this layer as result of mathematical calculations performed in preceding layers. The artificial neural network accepts inputs and weighted total associated with these inputs are calculated, which contains a bias. This calculation is denoted by a transfer function.

$$\sum_{i=1}^{n} Wi * Xi + b$$

The output is generated by supplying weighted total in the form of input to the activation function. The role of the activation functions is to determine the response of the node, whether it needs to fire or not. Only the fired nodes are accepted in the output layer and rest are rejected. Specific to the application the choice of active functions differ in the system.

3.3.2 **OPERATION OF ANN**

The Artificial Neural Network is best represented in terms of directed graph with some weight associated with them, representing artificial neurons in the form of nodes. The relationship between neuron inputs and output is represented by the directed weights. An outside or environmental signal in the shape of a sample and a graphically represented data is received in the form of a vector by the ANN.

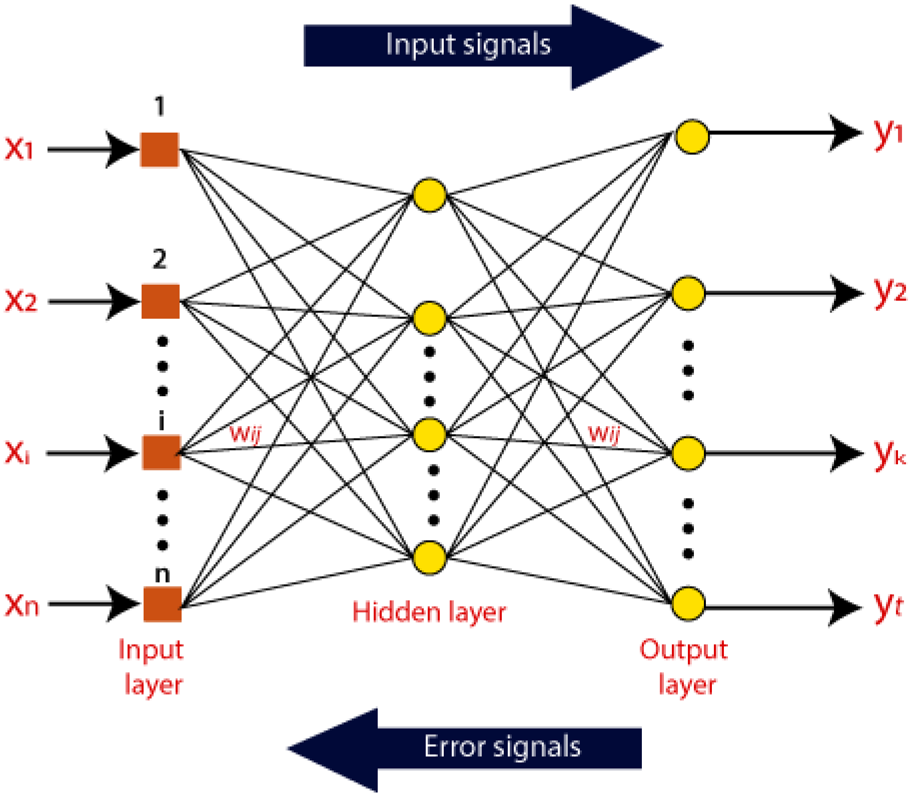

Figure 3.5 Neural Network layout

Following that, each input is subjected to multiplication with the associated weights to it. The responsibility of these weights is to describe the power of the connections between neurons in broad terms. The internals of the computing unit consists of summing up all the weighted inputs. If the weighted total is 0, a factor known as bias needs to added for getting a non-zero output. Weight equals 1, and bias has the same input. The range of the total weighted inputs can vary from 0 to positive infinity. A pre-established maximum value is benchmarked, the total of weighted inputs is being fed through the activation function to keep the response under the boundaries of the desired value. The activation function is an assembly of transfer functions whose utilization is required to reach the final desired result. Several types of activation functions exists, but broadly classified into linear or non-linear.

3.4 ARTIFICIAL NEURAL NETWORKS INFERENCE SYSTEM

Neural Networks (Artificial) (ANN). The human nervous system processes information in the same manner that an ANN does [27]. The network is combination of a series of distributed neurons that collaborate to figure a certain problem statement. The artificial neural network mimics how the nervous system (neurons) in the human brain process information. The neuron has the ability to process facts and figures, and there are some parallels between neurons and artificial neural networks: • Neuron dendrites are similar to artificial neural network input. • The axon, holds similarity with the output of the artificial neural network • the cell body, find similarity with the structure of the network. Artificial neural networks use neurons as computing units, which combine weighted inputs and apply an activation function to the resultant value, which is the neuron's output [27]. The link between two neurons is given a weight [28]. B. Artificial Neural Networks (ANNs) Training The weight of network connections must be adjusted using training data. One method of training an artificial neural network is to provide it with a pattern or series of learning using different algorithms and then allowing the network to develop and grow its behavior based on a learning rule [27]. When it comes to supervised learning, both the inputs and outputs are being subject of utilization for training the network, whereas the unsupervised learning, involves output being trained to recognize some definite patterns in the input data [27].

The procedures involved in a fuzzy inference system are depicted in Figure 3.3. Some of the basic components of the fuzzy inference system: • a rule base made up of fuzzy rules, • a detailed set that depicts the fuzzy rules' membership functions, and • finally a decision-conducting and processing unit that works with the fuzzy rules • a fuzzification interface responsible for the conversion of crisp input into a fuzzy set • a defuzzification interface that converts the fuzzy set result back into the form of environmental specific output [24].

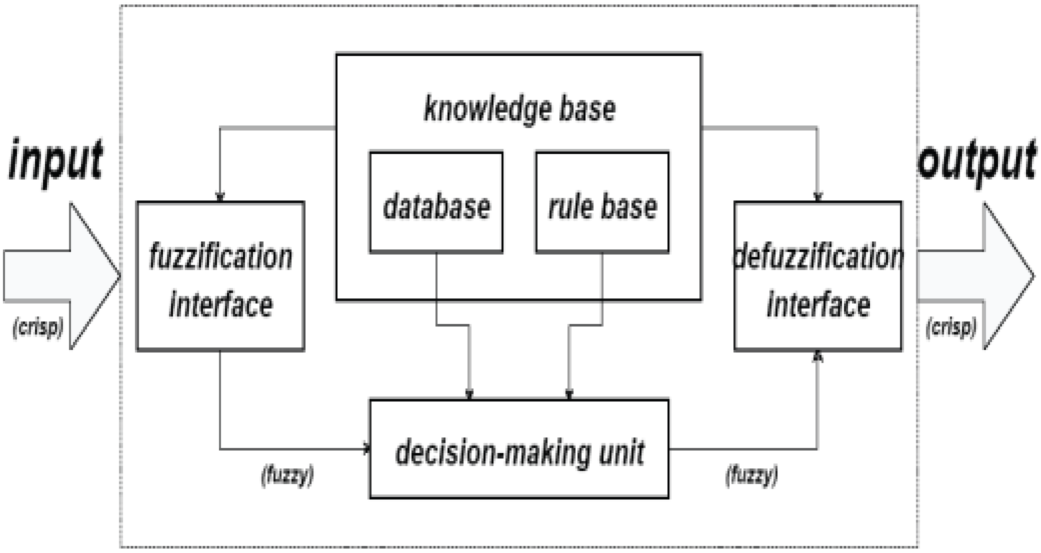

Figure 3.6 Processes involved in Fuzzy inference system.

The Fuzzy Inference System [29] can help with data classification, as well as automatic control and expert systems for decision-making. Fuzzy inference methods are used by Mamdani and Sugeno. This approach works effectively in nonlinear systems because it allows for optimizations and flexible models while keeping calculations under control. Despite its computational complexity, the Mamdani approach gathers expert input in a natural and sympathetic manner [27]. The primary difference between Mamdani- and Sugeno-type FIS in terms of fuzzy inputs is how they generate crisp outputs. To give crisp results, Sugeno-type FIS employs the method of weighted average, whereas Mamdani-type FIS employs deals with the problem statement by defuzzification. The weighted average replaces the time-indulging defuzzification phase of the Mamdani technique, allowing the Sugeno approach to analyze data more rapidly because of its ability of adding intuitiveness and ease of interpretation. Mamdani-type FIS is most often employed in enhancing and supporting the decisions in applications. Mamdani FIS provides output membership functions, but Sugeno FIS does not. Sugeno FIS is more versatile and flexible in terms of system design than Mamdani FIS. It also works well in conjunction with the ANFIS tool to boost outcomes.

ANFIS structural layers Figure 4 depicts the ANFIS model's three-input structure, which was created to reduce mobile network handover failures. Five layers make up the ANFIS model, notably the fuzzification layer, the rule layer, the normalization layer, the defuzification layer, and a single summing node [31]. SIR (Signal to Interference Ratio), Traffic Difference (TR), and Mobile Speed are the three input signals for ANFIS models (VEL).

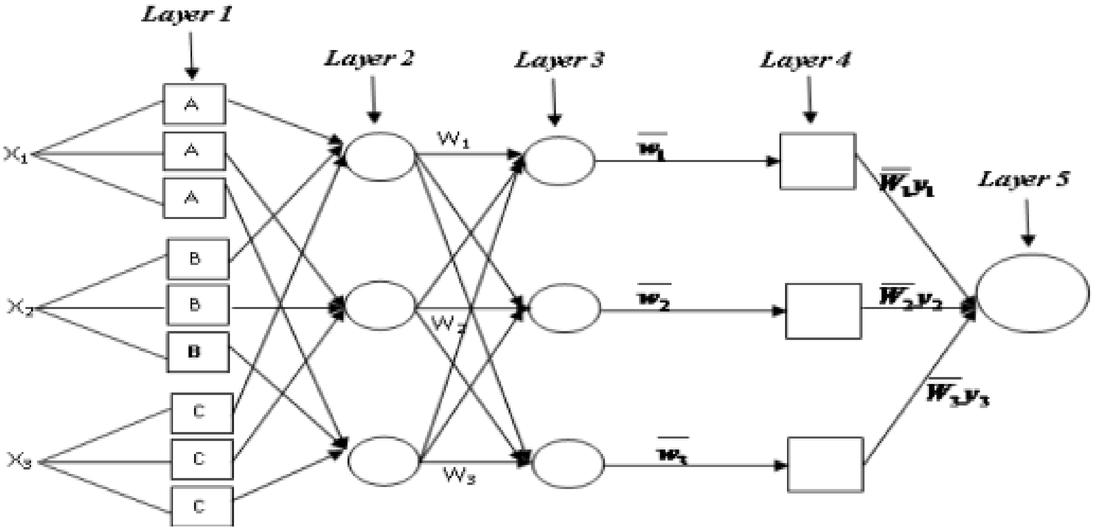

Figure 3.7 Shows the three input structure of ANFIS model

The given figure illustrates the typical diagram of Biological Neural Network.

$$\mu_A(x_i)=\frac{1}{1+\left|\frac{x_i-c_i}{a_i}\right|^{2b}}$$

x is the input signal µ A is the membership value of the input i a , b, i c , are premise parameters

Layer 2: This is called Rule layer and its nodes are fixed and labeled “W”. The output of the layer is the product of the incoming signals and the output of each node. The Mathematical model of this layer is:

$$O_{2,i}=w_i=\mu_{A_i}\ (x_1)=\mu_{Bi}(x_2)\quad for\,i=1,2$$

Layer 3: This is referred to as normalization layer. The nodes in this layer are fixed node labeled '$\overline{w}$"

The output of the node is called normalized output node which is the division of if rule's firing strength to the sum of the entire rule's firing strength [32]. Its mathematical model is given as:

Layer 4: Layer 4 is referred to as defuzzification layer with each of its adaptive node. The output of this node is called consequent parameters

Layer 5: This layer is known as summation node and this is where the overall output of the ANFIS structure is given.

3.5 FIS AND ANFIS

General Architecture of Rule based Fuzzy model

The general architecture [15] of a rule based fuzzy model consists of five modules as shown inFigure 2. They are

- Input interface
- Rule base
- Data base
- Fuzzy inference
- Output interface

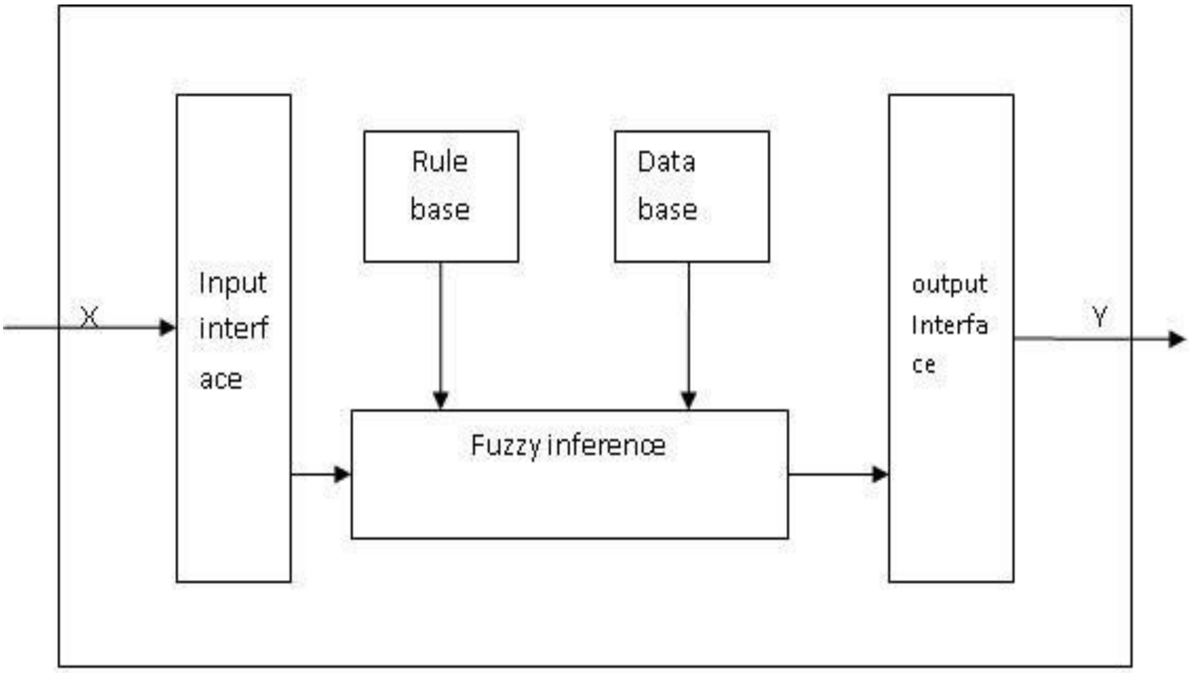

Figure 3.8 Rule based Fuzzy model

A user can enter data into the interface, and that data is converted into a format that the fuzzy inference can utilise to activate and process the fuzzy rules. In general, the input is a nebulous collection of numbers.

The rule foundation is made up of a series of if-then rules with fuzziness. You can think of it as describing how things are related between input and output.

These values are stored in a database, which also contains complete definitions of all input and output variables, as well as information on how membership functions work.

The module for fuzzy inference uses the rule base and approximate reasoning methods to process the inputs. Fuzzy inference uses fuzzy rules to develop outputs from transformed inputs.

The output interface converts the fuzzy inference's output into the format needed by the application environment.

Fuzzy inference in MATLAB is creating a fuzzy logic mapping from an input to an output. Decisions can be made or patterns discovered using the mapping. A wide variety of fuzzy inferences fall under the broad heading of fuzzy logic. Automation, decision analysis, expert systems, and computer vision all use fuzzy inference systems successfully.

CHAPTER 4

ANFIS APPROACH

This thesis suggested a fuzzy rule-based approach for classifying and managing faulty sensor nodes in WSNs that can detect and reuse faulty sensor nodes based on their failure status. To overcome the inherent uncertainties in the WSN environment, a fuzzy logic-based technique is used. The fuzzy interface engine classifies nodes according to the membership function selected, and the defuzzifier creates a non-fuzzy control for retrieving the various node kinds. Additionally, we used a routing technique that reused the problematic nodes that were retrieved during the data routing process.

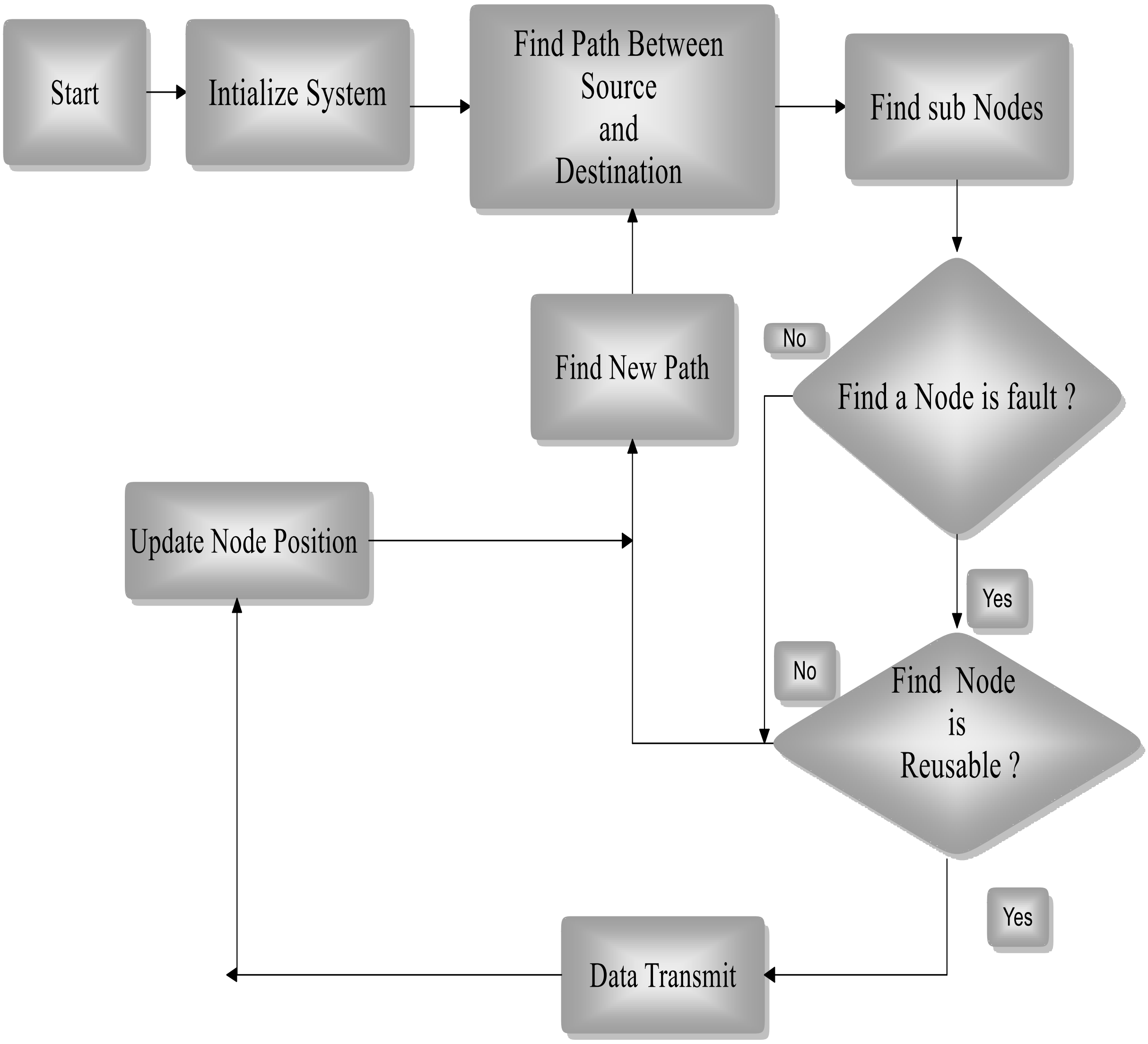

Figure 4.1 Approach Flow diagram

The routing protocol uses the AntHocNet algorithm, which is a hybrid multipath algorithm based on ACO routing concepts. It is composed of reactive as well as proactive components. We conducted extensive testing with the suggested approach in a variety of network configurations. The experimental results are compared to those of existing algorithms in order to demonstrate the proposed algorithm's usefulness in terms of a variety of critical performance metrics. In this simulation, we will assume the following sensor network model: I Deployed 271 sensor nodes are static; once deployed, sensor nodes must 272 operate independently.

The hardware status of the sensor node is evaluated in this work using fuzzy logic principles. Fig. 4.1 illustrates three input FIS for defective node identification. A fuzzy logic system is composed of four components: a fuzzifier, a fuzzy information system, a fuzzy rule base, and a defuzzifier. FIS receives information about the battery, transmitter, and receiver conditions of each sensor node. The FIS output indicates the status of individual sensor nodes. FIS may produce a normal node, an end node, or a dead node.

4.1 AntHocNet

AntHocNet is a hybrid multipath method based on ACO routing concepts. It is composed of reactive as well as proactive components. It does not maintain pathways to all destinations continuously (like the ACO algorithms for wired networks do), but establishes paths as needed at the start of a session. This is accomplished during a reactive path setup phase, during which the source launches ant agents known as reactive forward ants to discover multiple paths to the destination, and backward ants return to establish the paths. The pathways are denoted by pheromone tables that indicate their quality. Following path configuration, data packets are stochastically routed as datagrams over the various paths utilizing these pheromone tables. While a data session is in progress, the pathways are proactively investigated, maintained, and upgraded utilizing a variety of agents dubbed proactive forward ants. The algorithm responds to connection failures in one of two ways: by repairing local paths or by warning preceding nodes on the paths.

Description of the algorithm AntHocNet is a hybrid algorithm that combines reactive and proactive capabilities. The method is reactive in that it collects routing information about destinations only during communication sessions. It is proactive in that it attempts to retain and improve information about existing paths throughout the communication session (unlike purely reactive algorithms, which do not search for routing information until the currently known routes are no longer valid). The routing data is maintained in pheromone tables similar to those used by other ACO routing algorithms. Control and data packets are forwarded stochastically utilizing these tables. Specific reactive procedures are used to address link failures, such as local route repair and the usage of warning messages.

What is the operation of a roadside unit?

A roadside unit (RSU) captures traffic data along a road's static sensing region and communicates it to traffic control devices and a central traffic management centre. Additionally, these devices act as a data source for autonomous vehicles to capture future traffic data [18].

Network nodes are everyday vehicles on the road that are capable of communicating with one another via radio. The lowest level of security is provided by network nodes. The roadside infrastructure consists of a collection of RSUs. RSUs are authority agents stationed along the roadside; for example, traffic lights or road signs can be repurposed as RSUs following restoration. An RSU might be a highly sophisticated gadget or a relatively simple one. RSI is a semi-trustworthy algorithm with a medium level of security [7

Initial Parameters

Number of Nodes=105;

Source node=5;

Destination node=35;

Network size =120 x 120

Citysize=150;

Mobile heterogeneous sensor nodes are deployed uniformly in the WSN.

• The WSN is complete. The received signal intensity can be used to calculate the distance between nodes without a GPS.

• The WSN has malfunctioning nodes, although they are few and spread randomly.

• Each sensor node's detecting region has numerous nodes.

• Sensor node sensing range is fixed.

• The sensors' transmission range Trans Range (Si) is more than their sensing range (Si), and advanced nodes' sensing range is greater than standard nodes. WSN has events like free. Event Radius is the radius. It is expected that sensor Nodes have spatial connection within a physical vicinity. Nodes may detect comparable values from the environment.

4.2 EXECUTION OF NETWORK

Let take 20th node is source node and 45th node is destination

We need to transfer data from source to destination through other nodes

(In any nodes from 100, let consider, from 20th node to 34th node to 42nd node to 45th node ,so link path is 20-34-42-45)

The Fuzzy or ANFIS will find out

- If 34th node is fault or not
- If it is fault then we can reuse or not - for this process we repeat to 42nd node
- The above is one transmission
- Likewise we transmit data from source to destination
- There will only 20 to 40 paths

4.3 SIMULATION RESULTS

MATLAB is used to simulate the self-diagnosing defective node detection system that has been presented. The effectiveness of the suggested strategy is evaluated by randomly distributing 105 nodes. 120 X 120 m is the size of the simulation area. There is full energy backup for all nodes, and they are all aware of their location. The proposed approach's performance is compared to currently used approaches like threshold-based Network lifetime and energy usage are taken into account while calculating the performance. Fault node detection accuracy is the most critical statistic because it is used to test the proposed approach's basic functionality. The ANFIS approach is compared to the fuzzy approach as stated in to determine whether one has higher faulty node detection accuracy

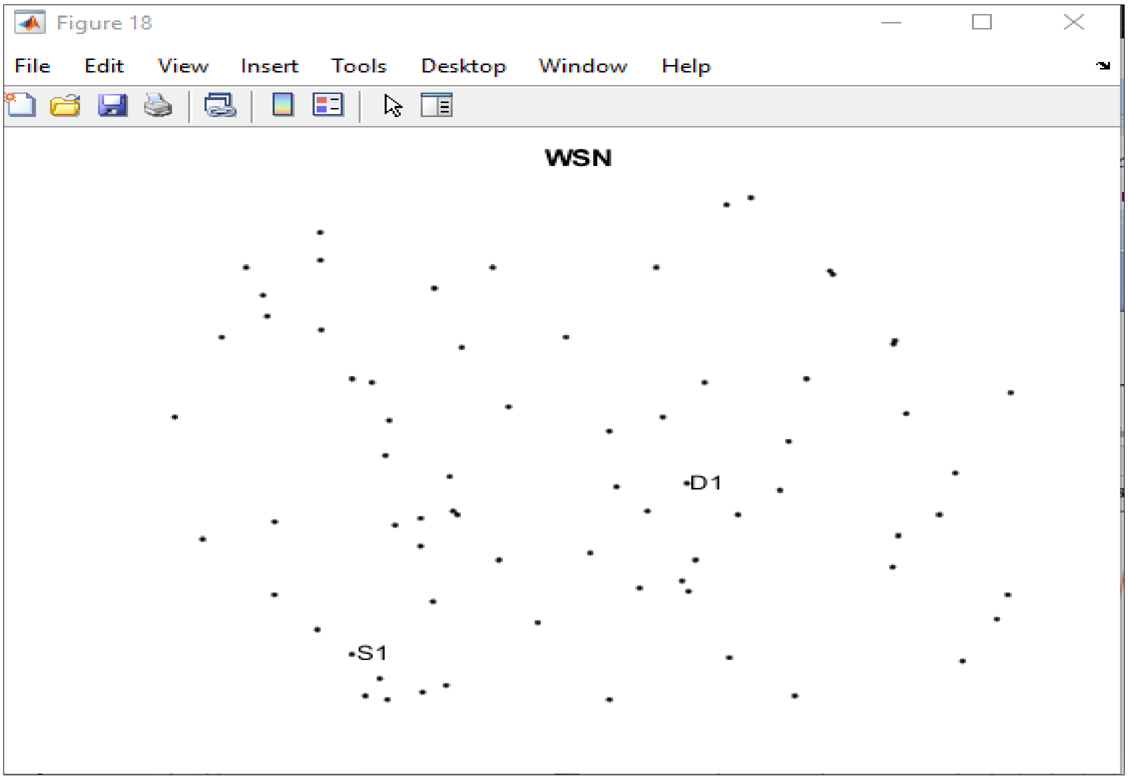

Figure 4.2 WSN System

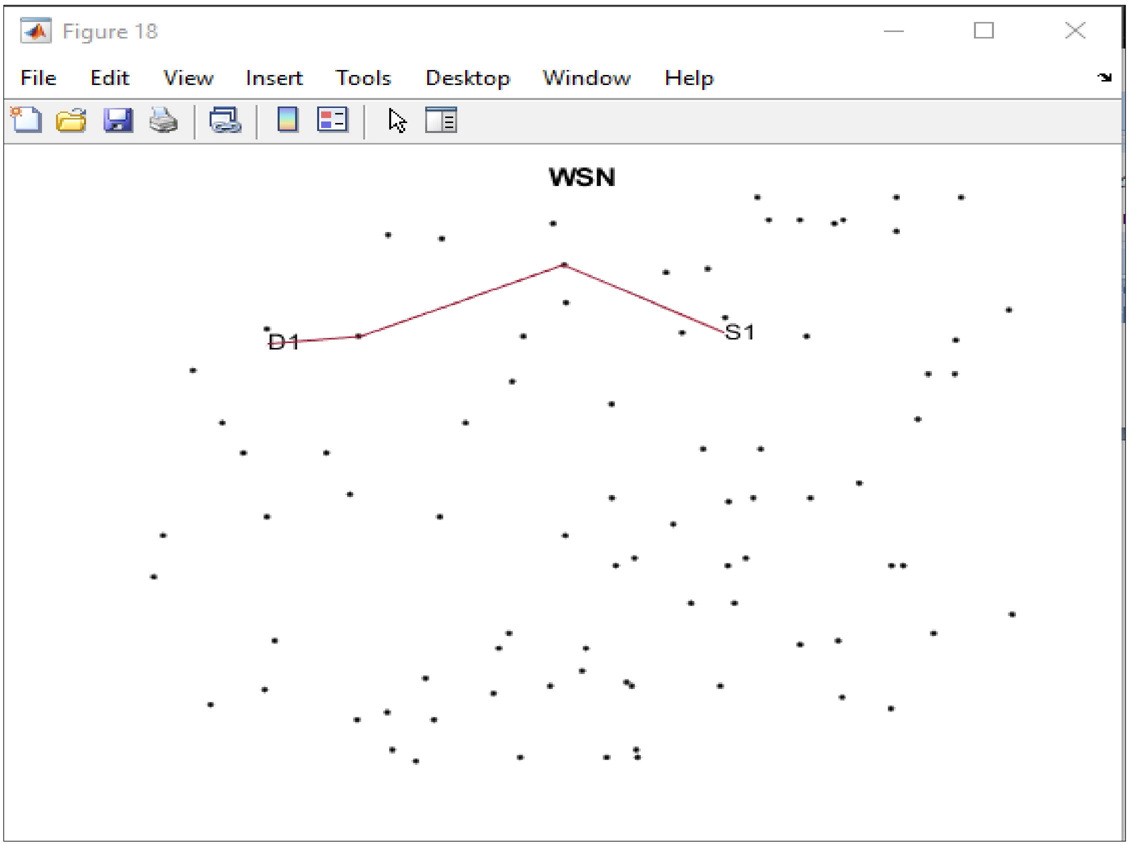

Figure 4.3 data transfer source to destination

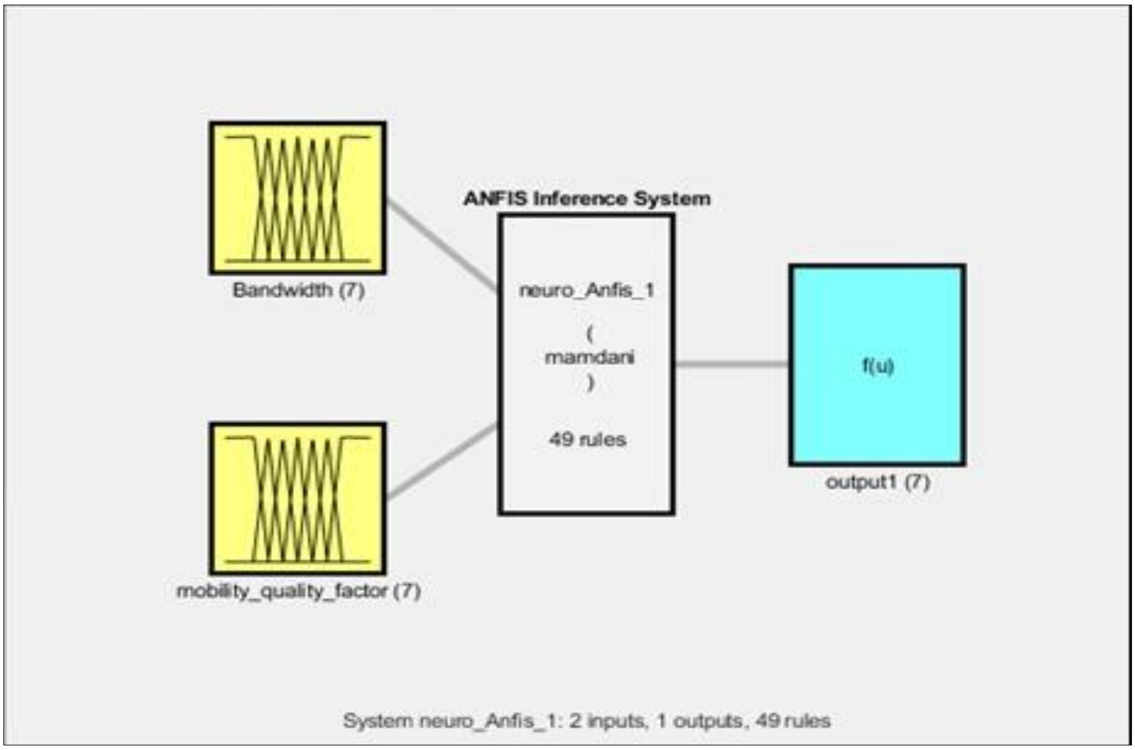

Figure 4.4 ANFIS interference system

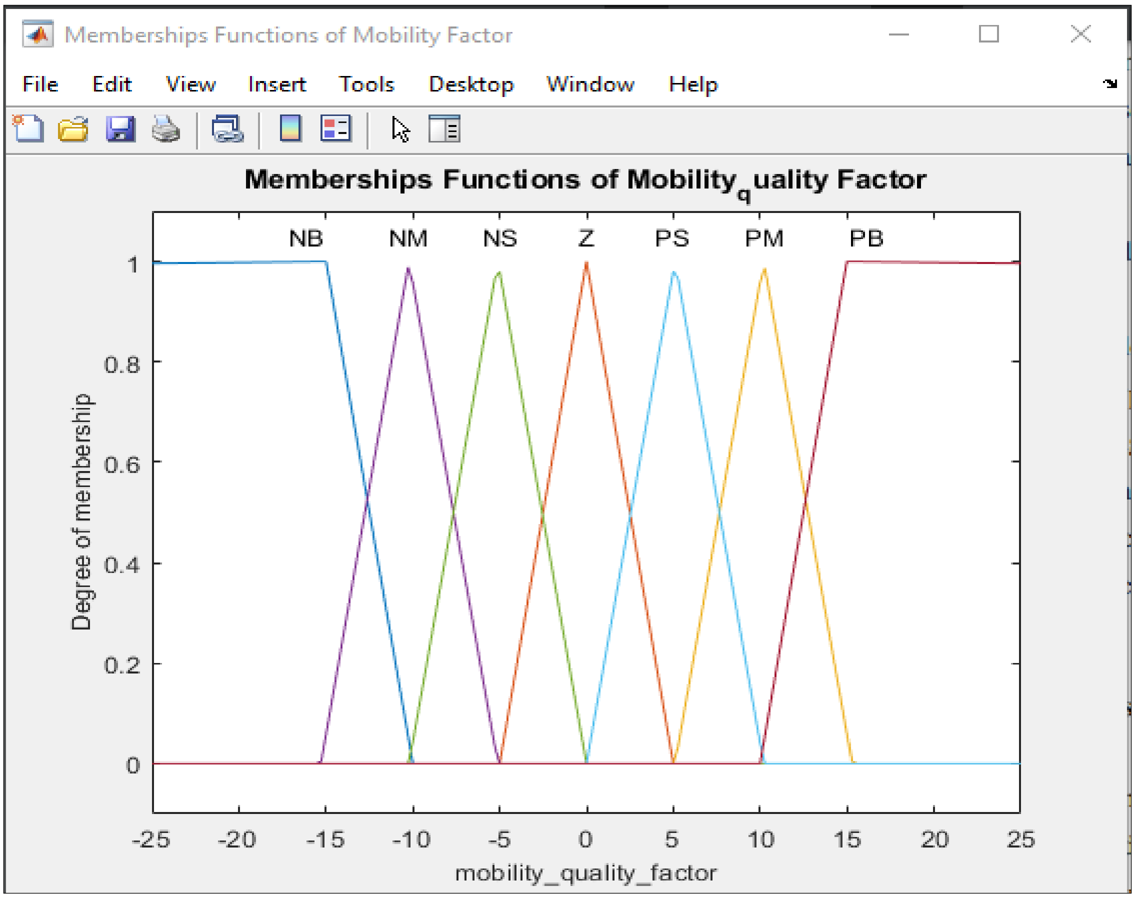

Figure 4.5 Membership function of ANFIS

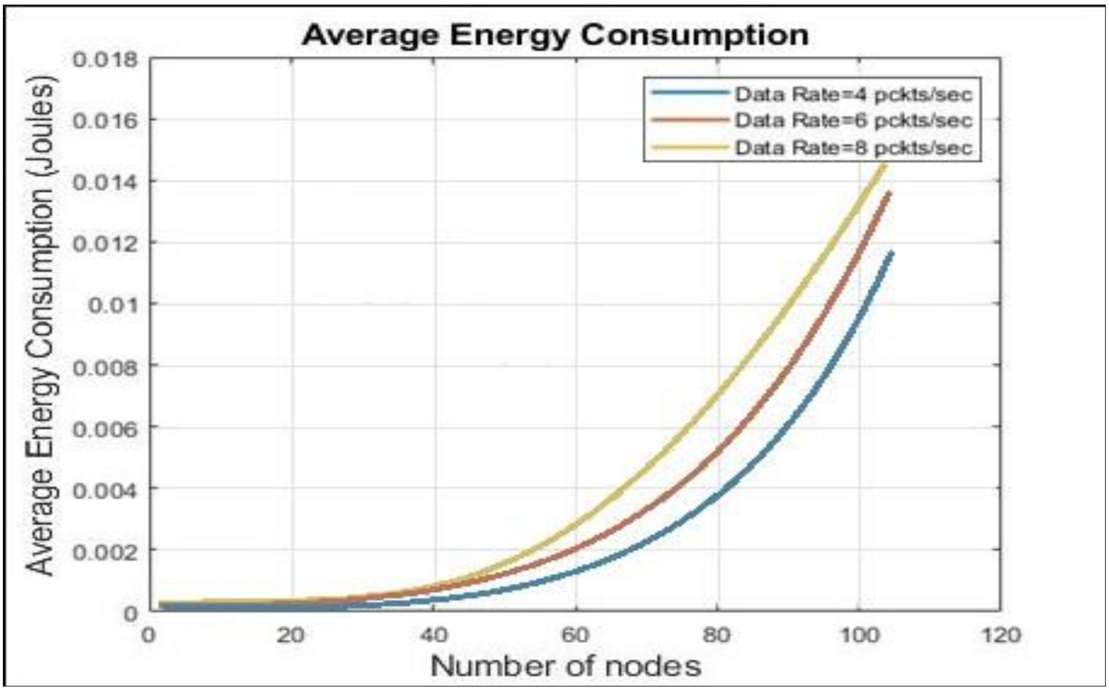

Figure 4.6 Average Energy Consumption of ANFIS network

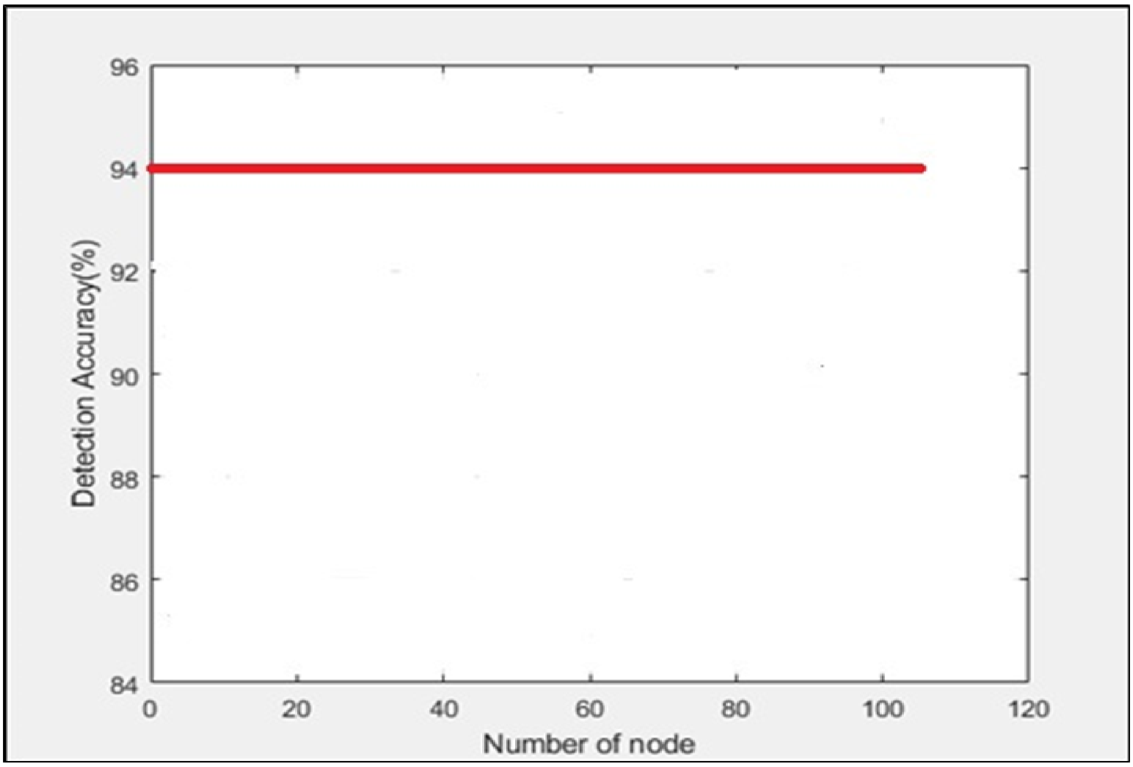

Figure 4.7 Detection Accuracy of ANFIS network

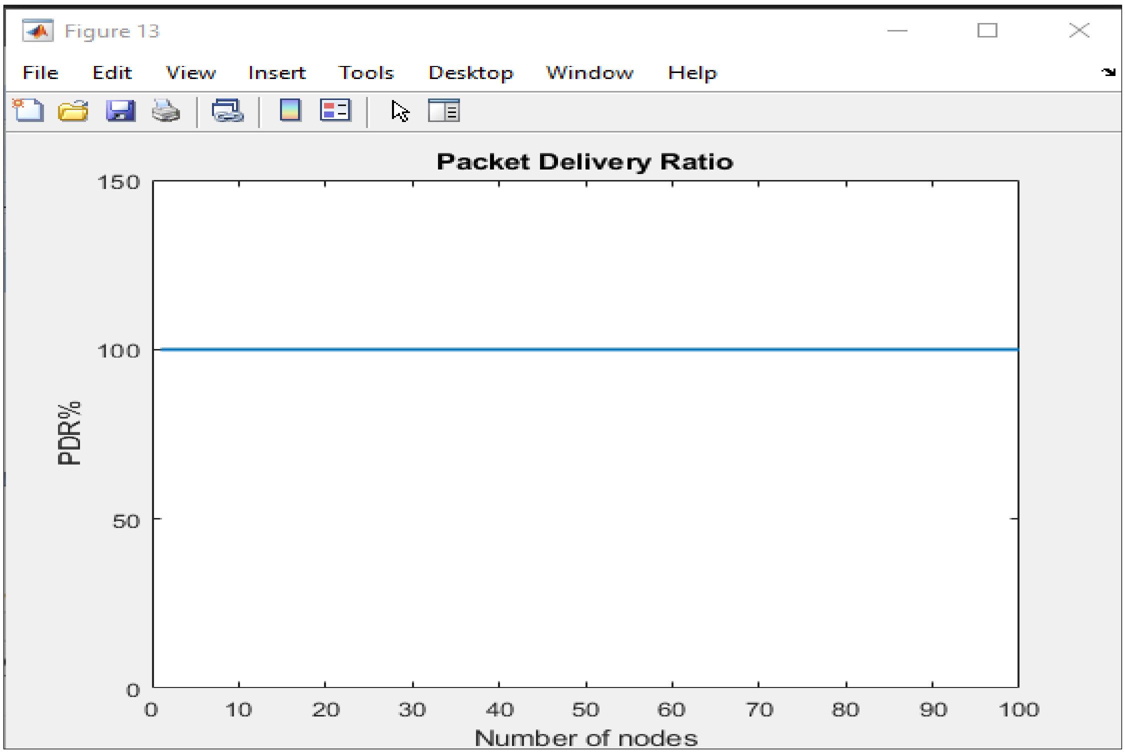

Figure 4.8 packet delivery ratio of ANFIS based network

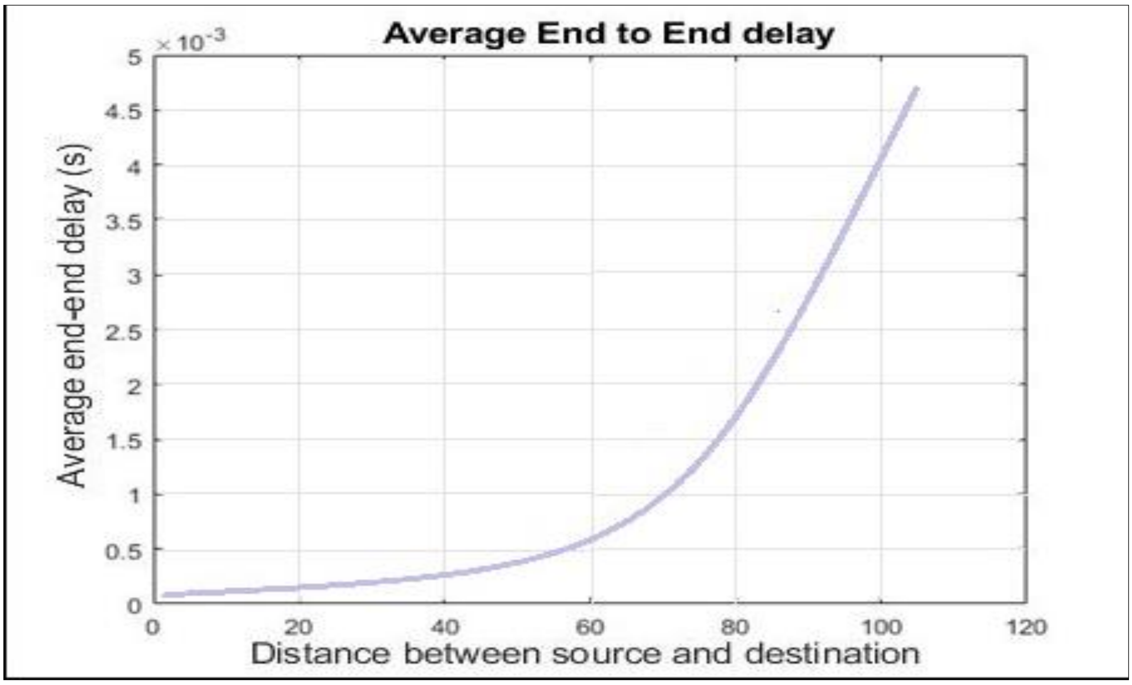

Figure 4.9 Average end to end delay of ANFIS based network

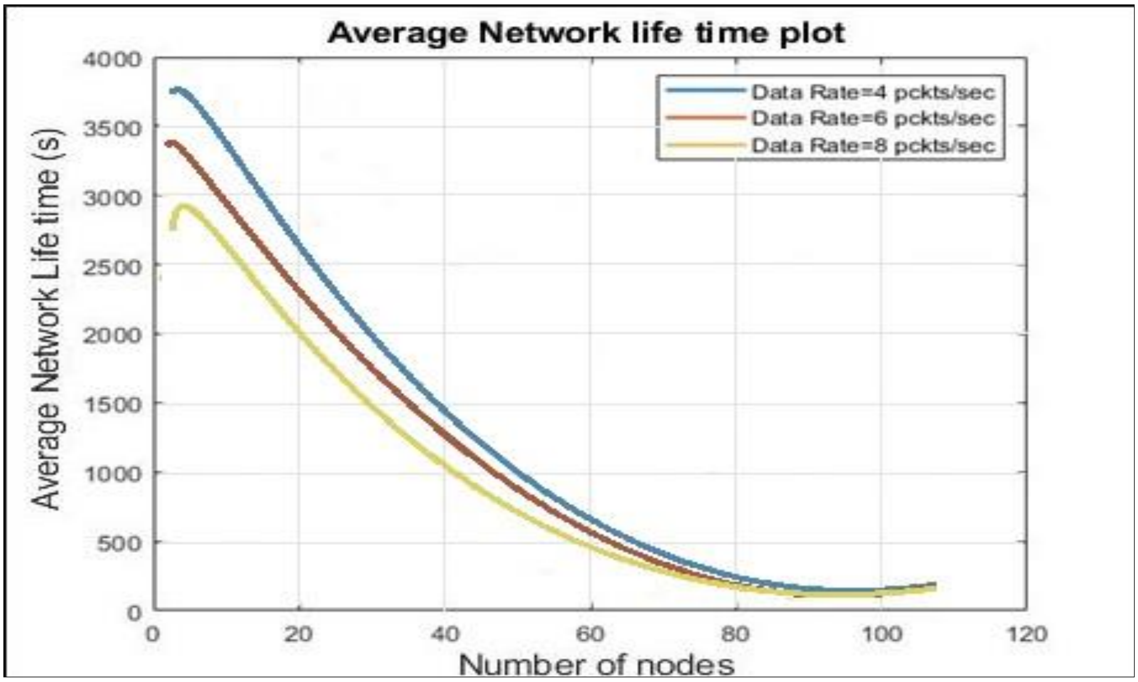

Figure 4.10 Average network life time of ANFIS based network

Fuzzy system execution

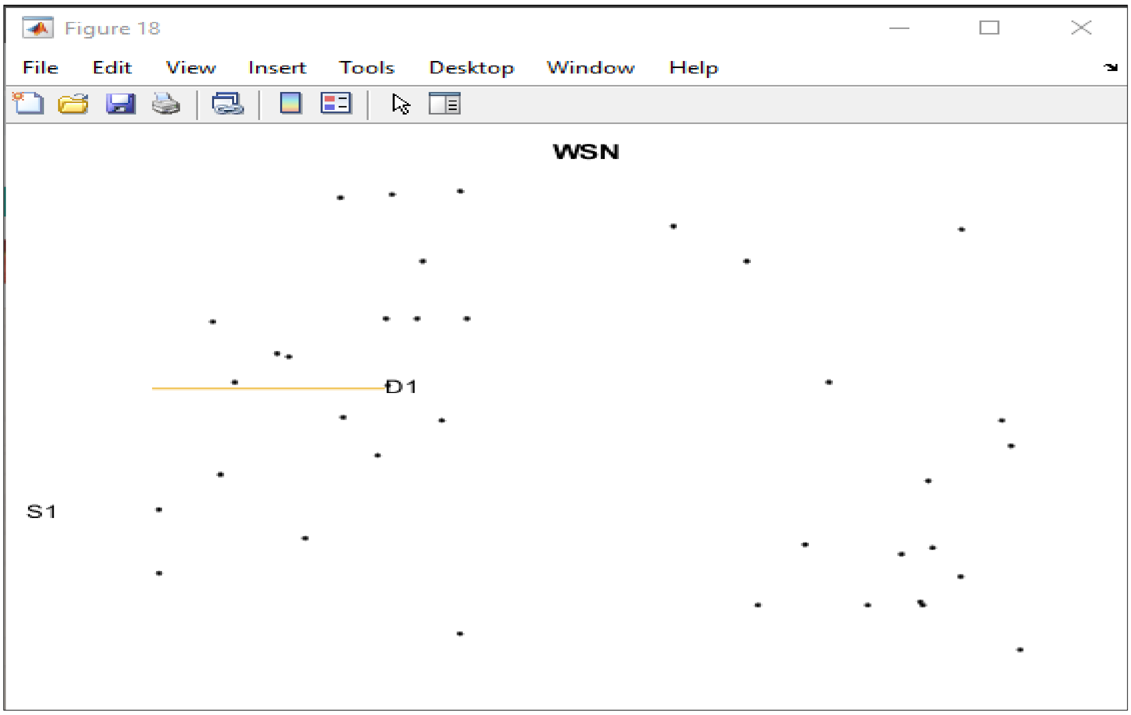

Figure 4.11 data transfer of Fuzzy based network

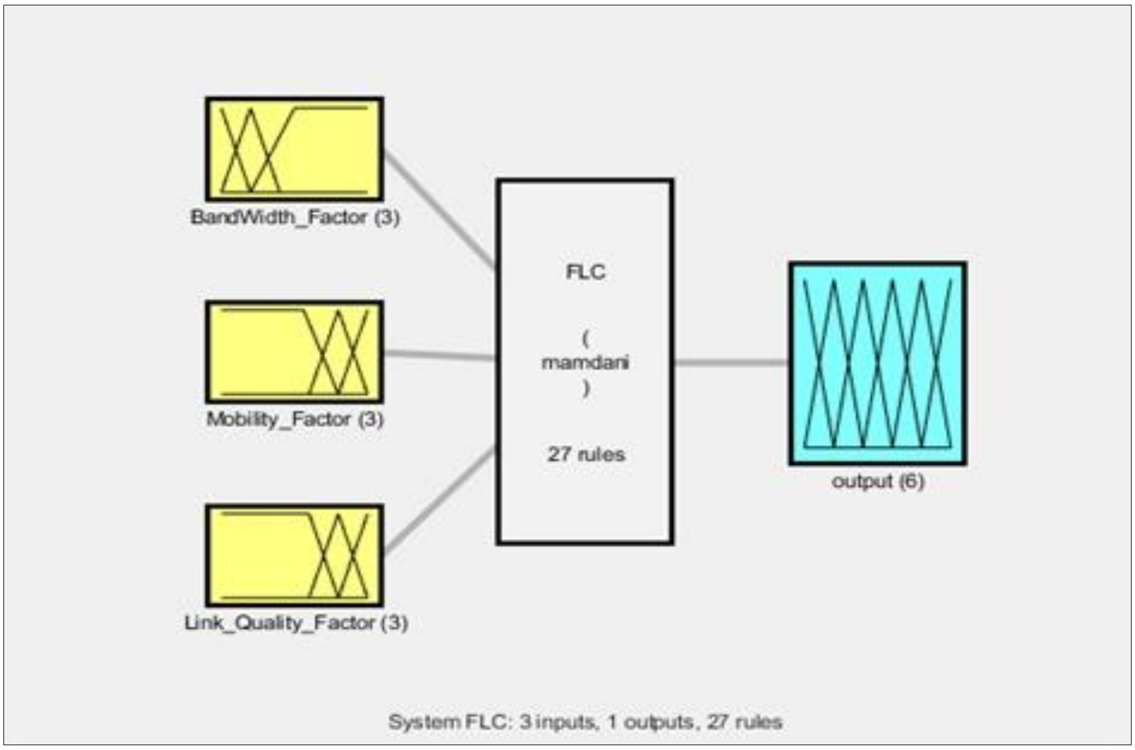

Figure 4.12 Fuzzy interference system

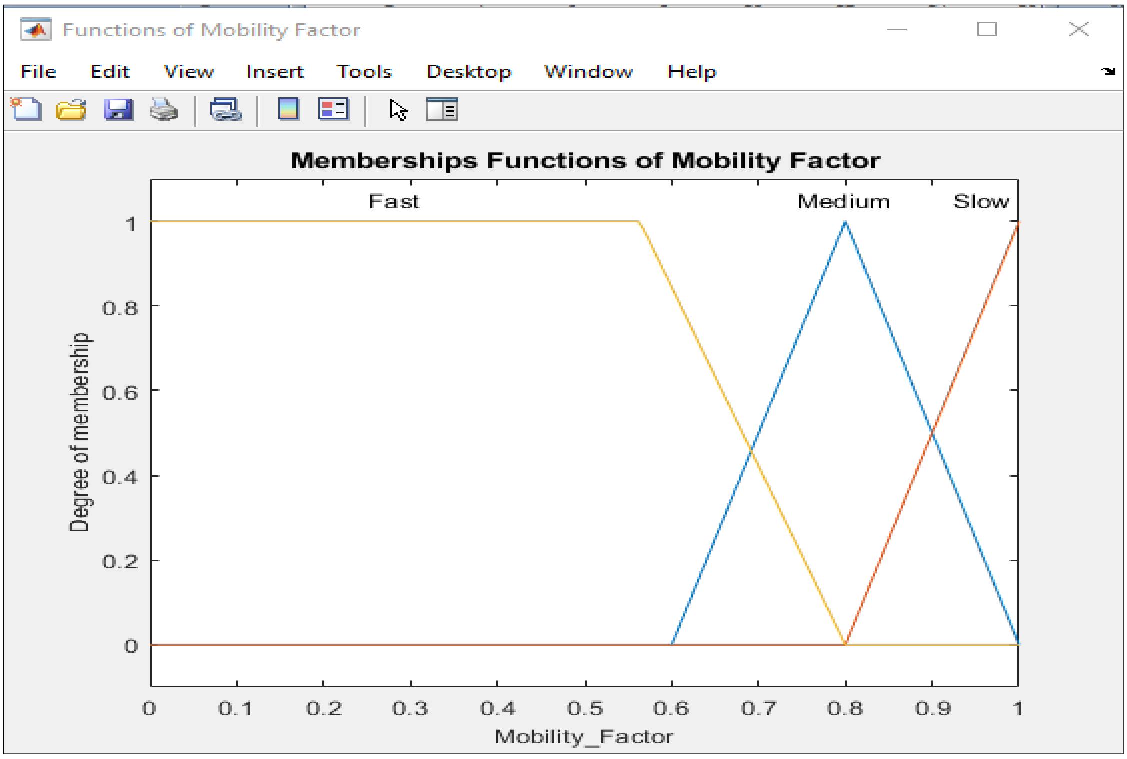

Figure 4.13 Membership function of fuzzy system

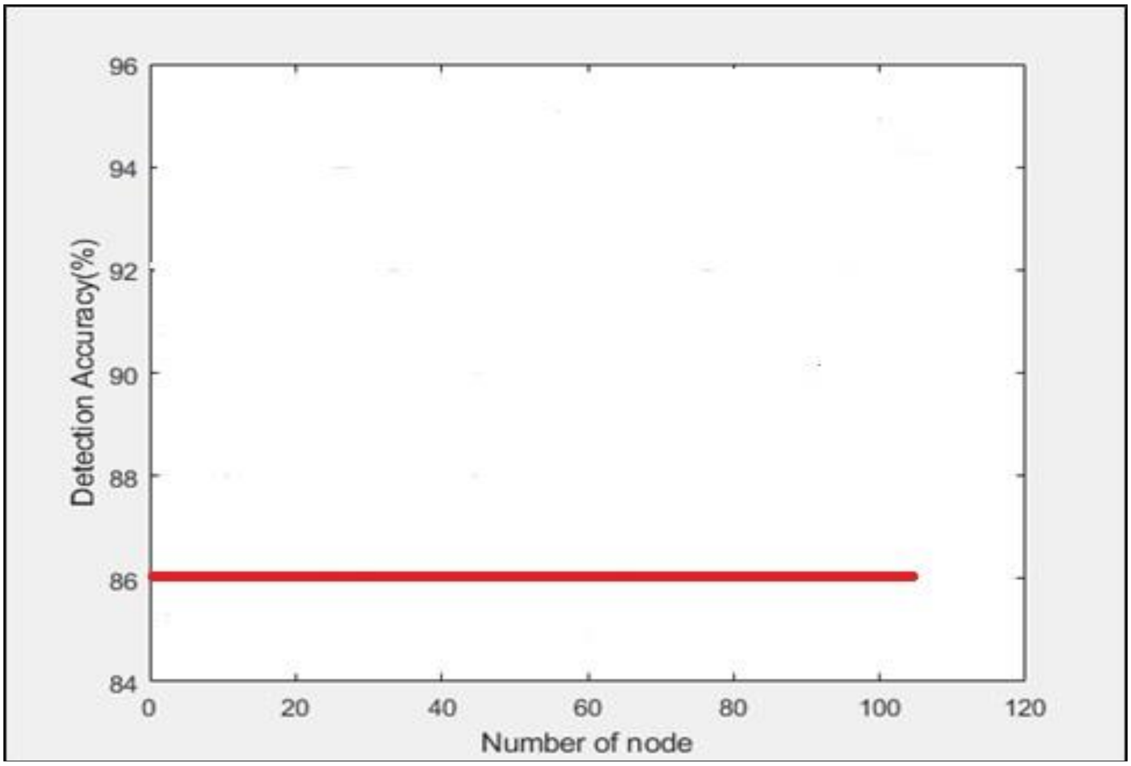

Figure 4.14 Detection accuracy of Fuzzy based network

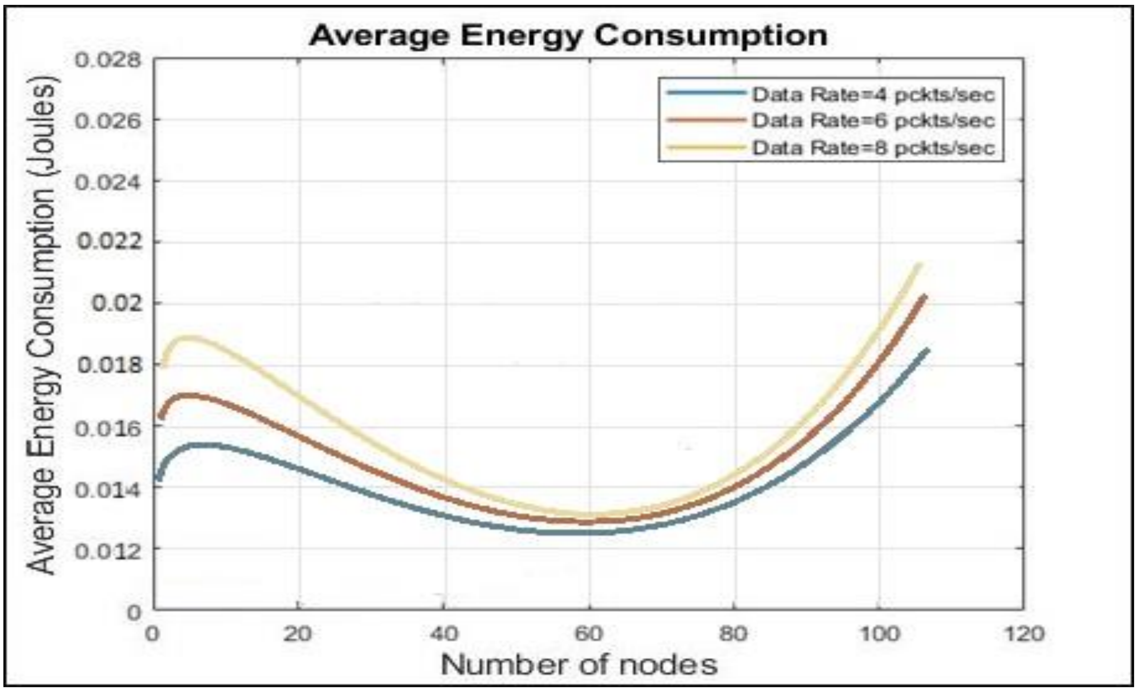

Figure 4.15 Average energy consumption of Fuzzy based network

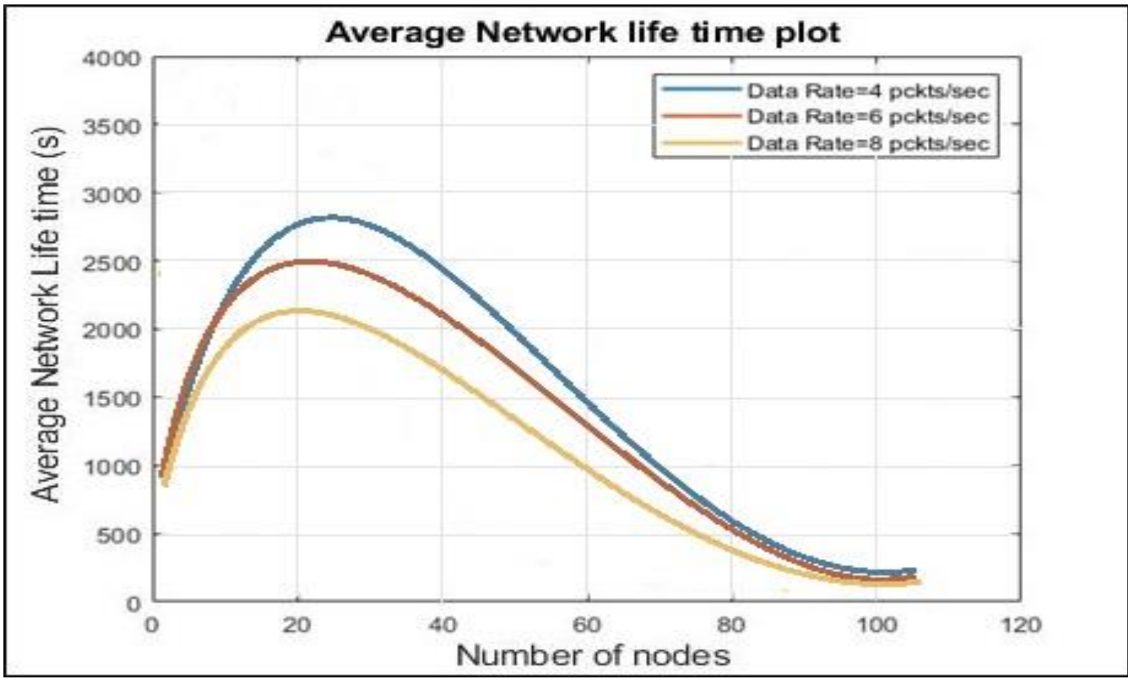

Figure 4.16 Average network life time of fuzzy based system

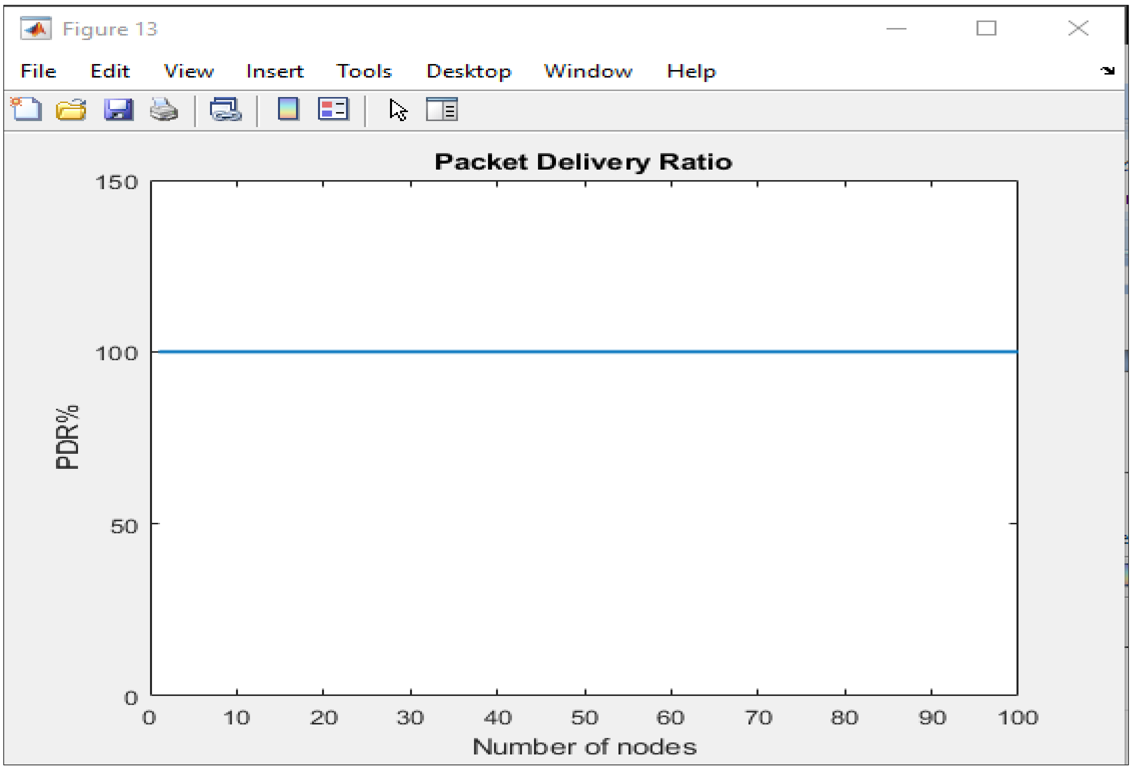

Figure 4.17 Packet delivery ratio of Fuzzy based network

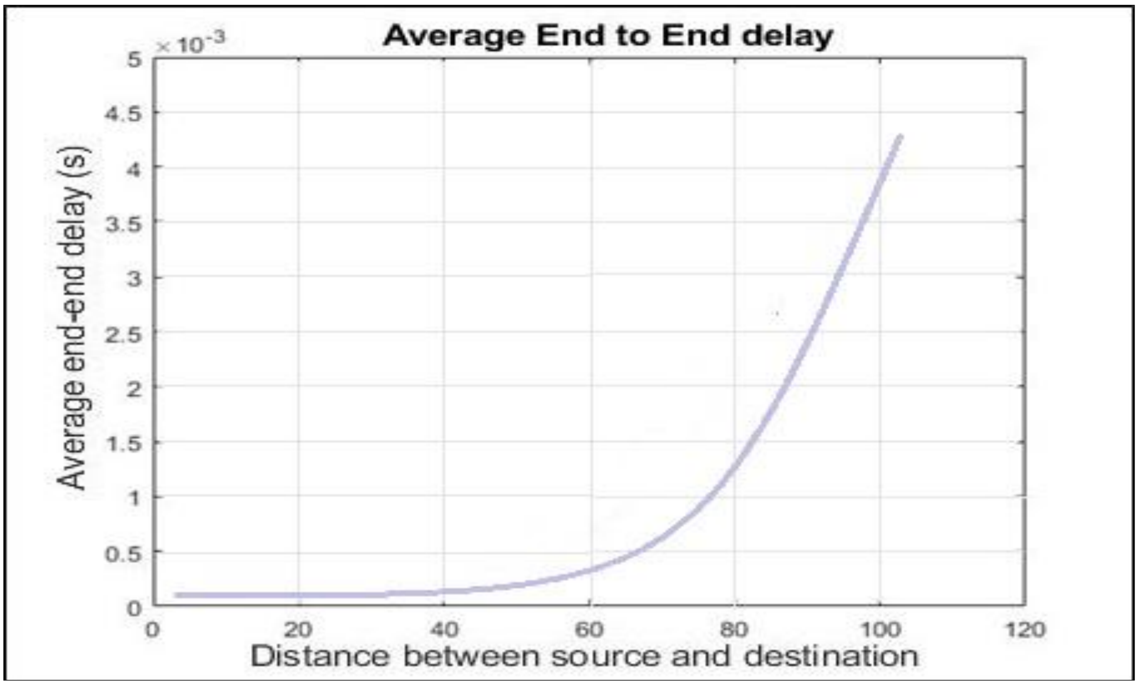

Figure 4.18 End to end of Fuzzy based network

Table 4.1 Performances of ANFIS and Fuzzy System

	Network Life Time (T)	PDR (%)	Energy Consumption (joule)	Delay (ms)
ANFIS network	4500	100	0.016	4.7
Fuzzy network	3700	100	0.019	4.9

Table 4.2 Comparison of exiting work

Techniques	Detection Accuracy
ANFIS	94%
Fuzzy	86%

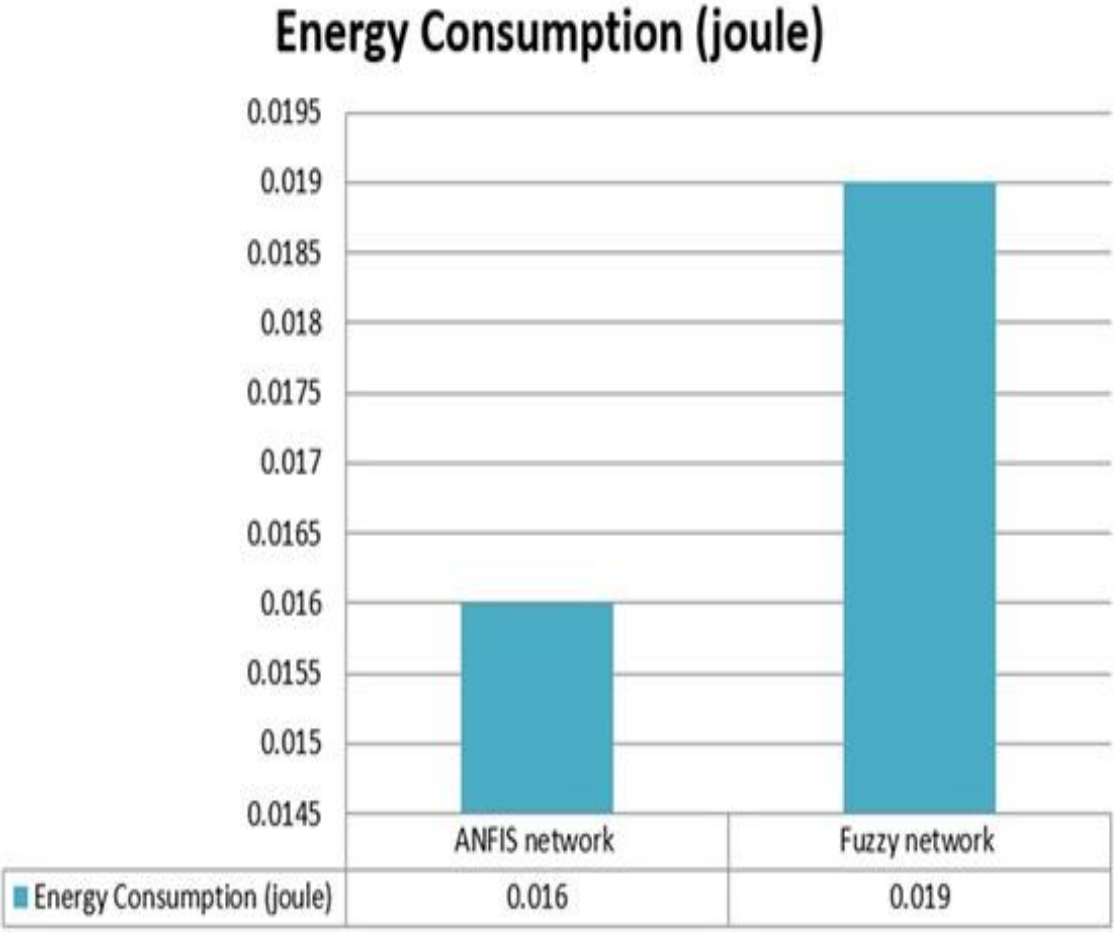

Table 4.3 Performance graph of Energy consumption

CHAPTER 5

5 CONCLSUION AND FUTURE SCOPE

5.1 Conclusion

Sensor nodes are low-cost devices with a high failure rate. If nodes are installed in hostile or severe settings, their failure rate may be very high. In such environments, detecting faulty nodes is one of the most important tasks that ensures the sensor nodes' reliable monitoring of the environment.

This study presented a faulty node classification and management scheme (FNCM) based on fuzzy rules that can be used in an intelligent monitoring and warning system. It can be used to detect physical or environmental factors in a variety of applications, including livestock management, home automation, and road monitoring. In compared to earlier methods, the suggested method provides four advantages. First, the ANFIS approach uses an efficient data routing mechanism to improve the reusability of the recovered defective nodes. As a result, the FNCM method can save a significant amount of energy. Second, the use of ANFIS aids in overcoming the WSN's uncertainty. Finally, the FNCM system assigns tasks to a working node based on its hardware status. Because the ANFIS approach saves energy and improves service quality, it is a good choice. Finally, the node management strategy not only enhances overall network performance but also provides a fast data routing system. The following is a list of the ANFIS work's limitations. First, because the network structure of a WSN changes often due to its inherent self-organization property, prior information about the node status is difficult to include into a fuzzy inference model. Second, this study only identifies and reuses malfunctioning up to 80 sensor nodes for improved network performance, but it ignores load management to balance the energy consumption of the deployed sensor nodes. Third, sensor nodes are installed to monitor separate areas in some applications, which should be addressed to improve network performance. Sensor nodes are densely deployed and connected in each region, whereas sensors from other areas may be disconnected. Due to network disconnection, the suggested approach takes substantially longer to diagnose node status in such applications. Several unique concepts should be considered in the future. First, we'll aim to implement a mobile sink-based system for collecting node status reports, so that network topology changes don't affect the fault detection process. Second, network problems are considered to be included in the fuzzy interference model for future reasoning due to environmental interference. Third, defect measurements must be improved in terms of computation efficiency and resilience.

5.2 Future Work

- Network simulators such as ns-3 can be used to validate the simulation results achieved using Matlab. Extending the outcomes of the experiment to include more scenarios and larger deployments.
- In addition, several subjects developed from the research provided in each chapter will be pursued in the future.
- Combining various multi-channel and multi-power techniques with low signaling cost and RPL would be fascinating to investigate. Furthermore, a bigger WSN testbed might be used to investigate the sensor collision problem.
- KP-RPL has been explored for mobile nodes following a preset trajectory, and its performance in settings with unpredictable moving patterns could be fascinating to see. Furthermore, there has yet to be an experimental evaluation of KP-RPL in a commercial WSN testbed.
- A more distributed C-RPL that uses the cooperative game among nodes rather than groups of nodes would be interesting to investigate. This would lower the cost of signaling while simultaneously improving the granularity of its solutions. Furthermore, an experimental comparison of RPL with C-RPL would be quite useful.

REFERENCES

1. Aishwarya Karmarkar;Prasenjit Chanak;Neetesh Kumar An Optimized SVM based Fault Diagnosis Scheme for Wireless Sensor Networks 2020 IEEE International Students' Conference on Electrical,Electronics and Computer Science (SCEECS) Year: 2020 | Conference Paper | Publisher: IEEE DOI: 10.1109/SCEECS48394.2020.134
2. Rakesh Ranjan Swain;Pabitra Mohan Khilar Soft fault diagnosis in wireless sensor networks using PSO based classification TENCON 2017 - 2017 IEEE Region 10 Conference Year: 2017 | Conference Paper | Publisher: IEEE DOI: 10.1109/TENCON.2017.8228274
3. Yasir Abdullah. R;Mary Posonia. A;Barakkath Nisha. U An Adaptive Mountain Clustering based Anomaly Detection for Distributed Wireless Sensor Networks 2021 International Conference on Communication, Control and Information Sciences (ICCISc) Year: 2021 | Volume: 1 | Conference Paper | Publisher: IEEE DOI: 10.1109/ICCISc52257.2021.9484916
4. Li Liu;Guangjie Han;Zhengwei Xu;Jinfang Jiang;Lei Shu;Miguel Martinez-Garcia Boundary Tracking of Continuous Objects Based on Binary Tree Structured SVM for Industrial Wireless Sensor Networks IEEE Transactions on Mobile Computing Year: 2020 | Early Access Article | Publisher: IEEE DOI: 10.1109/TMC.2020.3019393
5. Pialy Biswas;Raghavaraju Charitha;Shashank Gavel;Ajay Singh Raghuvanshi Fault Detection using hybrid of KF-ELM for Wireless Sensor Networks 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) Year: 2019 | Conference Paper | Publisher: IEEE DOI: 10.1109/ICOEI.2019.8862687
6. Sachin Dhanoriya;Manish Pandey A survey on wireless sensor networks: Faults, misbehaviour and protection against them 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT) Year: 2017 | Conference Paper | Publisher: IEEE DOI: 10.1109/ICCCNT.2017.8204172
7. Akyildiz I. F., Su W., Sankarasubramaniam Y., and Cayirci E. Wireless sensor networks: A survey. Computer Networks, 38(4):393–422, March 2002. ISSN 1389- 1286. doi: 10.1016/S1389-1286(01)00302-4. URL http://dx.doi.org/10.1016/ S1389-1286(01)00302-4.
8. Chen Y. and Zhao Q. On the lifetime of wireless sensor networks. Communications Letters, IEEE, 9(11):976–978, 2005. ISSN 1089-7798. doi: 10.1109/LCOMM.2005. 11010.

9. Olariu S. and Xu Q. Information assurance in wireless sensor networks. In Proceedings of the IEEE International Symposium on Parallel and Distributed Processing, pages 5 pp.–. IEEE Computer Society, April 2005. ISBN 0-7695-2312-9. doi: 10.1109/IPDPS.2005.257.
10. Chen X., Makki K., Yen K., and Pissinou N. Sensor network security: A survey. IEEE Communications Surveys Tutorials, 11(2):52–73, 2009. ISSN 1553-877X. doi: 10.1109/SURV.2009.090205.
11. Walters J., Liang Z., Shi W., and Chaudhary V. Security in Distributed, Grid, and Pervasive Computing, chapter 17 Wireless Sensor Network securities: A survey, pages 1–51. CRC Press, 2007.
12. Zhang X., Heys H., and Cheng L. Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks. In 25th Biennial Symposium on Communications, QBSC '10, pages 168–172, 2010. doi: 10.1109/BSC.2010.5472979.
13. Wander A., Gura N., Eberle H., Gupta V., and Shantz S. Energy analysis of public-key cryptography for wireless sensor networks. In Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications, PERCOM '05, pages 324–328, Washington, DC, USA, 2005. IEEE Computer Society. ISBN 0-7695-2299-8. doi: 10.1109/PERCOM.2005.18. URL
14. Shamir A. Identity-based cryptosystems and signature schemes. In Advances in Cryptology, volume 196 of Lecture Notes in Computer Science, pages 47– 53. Springer Berlin Heidelberg, 1985. ISBN 978-3-540-15658-1. doi: 10.1007/ 3-540-39568-7 5. URL
15. Amin F., Jahangir H., and Rasifard H. Analysis of public-key cryptography for wireless sensor networks security. 2(5):403 – 408, 2008. ISSN 1307-6892. URL
16. Al-Riyami S. and Paterson K. Certificateless public key cryptography. In Advances in Cryptology - ASIACRYPT 2003, volume 2894 of Lecture Notes in Computer Science, pages 452–473. Springer Berlin Heidelberg, 2003. ISBN 978-3-540- 20592-0. doi: 10.1007/978-3-540-40061-5 29.
17. The evolution of wireless sensor networks. http://www.silabs.com/Support% 20Documents/TechnicalDocs/evolution-of-wireless-sensor-networks. pdf.
18. Du W., Deng J., Han Y., Varshney P., Katz J., and Khalili A. A pairwise key predistribution scheme for wireless sensor networks. ACM Transactions on Information and System Security (TISSEC), 8(2):228–258, 2005. ISSN 1094-9224. doi: 10.1145/1065545.1065548. URL http://doi.acm.org/10.1145/1065545. 1065548.
19. Perrig A., Stankovic J., and Wagner D. Security in wireless sensor networks. Commun.

ACM, 47(6):53–57, June 2004. ISSN 0001-0782. doi: 10.1145/990680. 990707. URL http://doi.acm.org/10.1145/990680.990707.

20. Liang N., Gongliang C., and Jianhua L. Escrowable identity-based authenticated key agreement protocol with strong security. Computers & Mathematics with Applications, 65(9):1339 – 1349, 2013. ISSN 0898-1221. doi: http://dx.doi.org/ 10.1016/j.camwa.2012.01.041.
21. Kim Y., Kim Y., Choe Y., and Hyong O. An efficient bilinear pairing-free certificateless two-party authenticated key agreement protocol in the eck model. In Journal of Theoretical Physics and Cryptography, volume 3, pages 1–10. 2013. URL
22. Lippold G., Boyd C., and Gonzalez J. Strongly secure certificateless key agreement. In Pairing-Based Cryptography Pairing 2009, volume 5671 of Lecture Notes in Bibliography 120 Computer Science, pages 206–230. Springer Berlin Heidelberg, 2009. ISBN 978-3-642-03297-4. doi: 10.1007/978-3-642-03298-1 14. URL
23. Rev A. Mpr-mib series user manual. http://www-db.ics.uci.edu/pages/ research/quasar/MPR-MIB%20Series%20User%20Manual%207430-0021-06_A. pdf, 2004.
24. Levis P., Madden S., Polastre J., Szewczyk R., Whitehouse K., Woo A., Gay D., Hill J., Welsh M., Brewer E., and Culler D. Tinyos: An operating system for sensor networks. In Ambient Intelligence, pages 115–148. Springer Berlin Heidelberg, 2005. ISBN 978-3-540-23867-6. doi: 10.1007/3-540-27139-2 7.
25. Gay D., Levis P., Behren R., Welsh M., Brewer E., and Culler D. The nesc language: A holistic approach to networked embedded systems. ACM SIGPLAN Notices, 38(5):1–11, May 2003. ISSN 0362-1340. doi: 10.1145/780822.781133.
26. Aranha D. and Gouvˆea C. RELIC is an Efficient LIbrary for Cryptography. http: //code.google.com/p/relic-toolkit/.
27. Titzer B, Lee D., and Palsberg J. Avrora: scalable sensor network simulation with precise timing. In Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, IPSN ’05, pages 477–482, 2005. doi: 10.1109/ IPSN.2005.1440978.
28. Perrig A., Szewczyk R., Tygar J., Wen V., and Culler D. Spins: Security protocols for sensor networks. Wireless Networks, 8(5):521–534, 2002. ISSN 1022- 0038. doi: 10.1023/A:1016598314198.
29. Pietro R., Mancini L., Yee L., Etalle S., and Havinga P. Lkhw: a directed diffusionbased secure multicast scheme for wireless sensor networks. In Parallel Processing Workshops,

2003. Proceedings. 2003 International Conference on, pages 397–406, Oct 2003. doi: 10.1109/ICPPW.2003.1240395.

30. Chan H. and Perrig A. Pike: peer intermediaries for key establishment in sensor networks. In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, volume 1, pages 524–535 vol. 1, March 2005. doi: 10.1109/INFCOM.2005.1497920. Bibliography 121
31. Lai B., Kim S., and Verbauwhede I. Scalable session key construction protocol for wireless sensor networks. In IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES, page 7, 2002.
32. Dutertre B., Cheung S., and Levy J. Lightweight key management in wireless sensor networks by leveraging initial trust, sdl. Technical report, Tech. Rep. SRISDL-04-02, System Design Laboratory, 2004.
33. Chan H., Perrig A., and Song D. Random key predistribution schemes for sensor networks. In Proceedings of the 2003 IEEE Symposium on Security and Privacy, SP ’03, pages 197– . IEEE Computer Society, 2003. ISBN 0-7695-1940-7. URL
34. Eschenauer L. and Gligor V. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS ’02, pages 41–47. ACM, 2002. ISBN 1-58113-612-9. doi: 10.1145/586110.586117. URL http://doi.acm.org/10.1145/586110.586117.
35. Liu D. and Ning P. Improving key predistribution with deployment knowledge in static sensor networks. ACM Trans. Sen. Netw., 1(2):204–239, 2005. ISSN 1550-4859. doi: 10.1145/1105688.1105691. URL http://doi.acm.org/10.1145/ 1105688.1105691.
36. Du W.,Deng J., Han Y., Chen S., and Varshney P. A key management scheme for wireless sensor networks using deployment knowledge. In INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, volume 1, pages –597, March 2004. doi: 10.1109/INFCOM.2004. 1354530.
37. Liu D. and Ning P. Establishing pairwise keys in distributed sensor networks. In Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS ’03, pages 52–61. ACM, 2003. ISBN 1-58113-738-9. doi: 10.1145/ 948109.948119. URL http://doi.acm.org/10.1145/948109.948119.
38. Blundo C., Alfredo S., Herzberg A., Kutten S., Vaccaro U., and Yung M. Perfectlysecure key distribution for dynamic conferences. In Advances in Cryptology CRYPTO 92, volume 740 of Lecture Notes in Computer Science, pages 471– 486. Springer Berlin

Heidelberg, 1993. ISBN 978-3-540-57340-1. doi: 10.1007/ 3-540-48071-

39. Liu D., Ning P., and Li R. Establishing pairwise keys in distributed sensor networks. ACM Trans. Inf. Syst. Secur., 8(1):41–77, 2005. ISSN 1094-9224. doi: 10. 1145/1053283.1053287. URL
40. Liu D. and Ning P. Location-based pairwise key establishments for static sensor networks. In Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN '03, pages 72–82. ACM, 2003. ISBN 1-58113-783-4. doi: 10.1145/986858.986869. URL http://doi.acm.org/10.1145/986858.986869.
41. Zhang W., Tran M., Zhu S., and Cao G. A random perturbation-based scheme for pairwise key establishment in sensor networks. In Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc '07, pages 90–99. ACM, 2007. ISBN 978-1-59593-684-4. doi: 10.1145/1288107. 1288120. URL http://doi.acm.org/10.1145/1288107.1288120.
42. Blom R. An optimal class of symmetric key generation systems. In Advances in Cryptology, volume 209 of Lecture Notes in Computer Science, pages 335– 338. Springer Berlin Heidelberg, 1985. ISBN 978-3-540-16076-2. doi: 10.1007/ 3-540-39757-4
43. Huang D., Mehta M., Medhi D., and Harn L. Location-aware key management scheme for wireless sensor networks. In Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN '04, pages 29–42. ACM, 2004. ISBN 1-58113-972-1. doi: 10.1145/1029102.1029110. URL http://doi.acm.org/ 10.1145/1029102.1029110.
44. Yu Z. and Yong G. A robust group-based key management scheme for wireless sensor networks. In Wireless Communications and Networking Conference, 2005 IEEE, volume 4, pages 1915–1920 Vol. 4, March 2005. doi: 10.1109/WCNC.2005. 1424812.
45. Yu C., Lu C., and Kuo S. A simple non-interactive pairwise key establishment scheme in sensor networks. In Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON '09. 6th Annual IEEE Communications Society Conference on, pages 1–9, June 2009. doi: 10.1109/SAHCN.2009.5168906.
46. Lee J. and Stinson D. Deterministic key predistribution schemes for distributed sensor networks. In Selected Areas in Cryptography, volume 3357 of Lecture Notes in Computer Science, pages 294–307. Springer Berlin Heidelberg, 2005. ISBN 978- 3-540-24327-4. doi: 10.1007/978-3-540-30564-4 21. URL http://dx.doi.org/ 10.1007/978-3-540-30564-4_21.
47. Zhu S., Setia S., and Jajodia S. Leap: Efficient security mechanisms for largescale

distributed sensor networks. In Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS ’03, pages 62–72, 2003. ISBN 1- 58113-738-9. doi: 10.1145/948109.948120. URL http://doi.acm.org/10.1145/ 948109.948120. Bibliography 123

48. Jang J., Kwon T., and Song J. A time-based key management protocol for wireless sensor networks. In Information Security Practice and Experience, volume 4464 of Lecture Notes in Computer Science, pages 314–328. Springer Berlin Heidelberg, 2007. ISBN 978-3-540-72159-8. doi: 10.1007/978-3-540-72163-5 24. URL http: //dx.doi.org/10.1007/978-3-540-72163-5_24
49. .Camtepe S. and Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks. IEEE/ACM Transactions on Networking, 15(2):346–358, April 2007. ISSN 1063-6692. doi: 10.1109/TNET.2007.892879.
50. Younis M., Ghumman K., and Eltoweissy M. Location-aware combinatorial key management scheme for clustered sensor networks. Parallel and Distributed Systems, IEEE Transactions on, 17(8):865–882, Aug 2006. ISSN 1045-9219. doi: 10.1109/TPDS.2006.106.
51. Eltoweissy M., Moharrum M., and Mukkamala R. Dynamic key management in sensor networks. Communications Magazine, IEEE, 44(4):122–130, April 2006. ISSN 0163-6804. doi: 10.1109/MCOM.2006.1632659.
52. Diffie W. and Hellman M. New directions in cryptography. IEEE Transactions on Information Theory, 22(6):644–654, Nov 1976. ISSN 0018-9448. doi: 10.1109/ TIT.1976.1055638.
53. Malan D., Welsh M., and Smith M. A public-key infrastructure for key distribution intinyos based on elliptic curve cryptography. In Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on, pages 71–80, Oct 2004. doi: 10.1109/SAHCN.2004.1381904.
54. Gura N., Patel A., Wander A., Eberle H., and Shantz S. Comparing elliptic curve cryptography and rsa on 8-bit cpus. In Cryptographic Hardware and Embedded Systems - CHES 2004, volume 3156 of Lecture Notes in Computer Science, pages 119–132. Springer Berlin Heidelberg, 2004. ISBN 978-3-540-22666-6. doi: 10.1007/ 978-3-540-28632-5 9. URL http://dx.doi.org/10.1007/978-3-540-28632-5_ 9.
55. Liu A. and Ning P. Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks. In Information Processing in Sensor Networks, 2008. IPSN ’08.

International Conference on, pages 245–256, April 2008. doi: 10.1109/ IPSN.2008.47. Bibliography 124

56. Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation, 48(177): 203–209, 1987. ISSN 1088-6842. doi: 10.2307/2007884. URL http://www.ams. org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/.