Detection of Malicious Nodes in Wireless Sensor Network Through Neural Network

A Thesis

Submitted

In Partial Fulfillment of the Requirements

for the Degree of

MASTER OF TECHNOLOGY

In

COMPUTER SCIENCE & ENGINEERING

Submitted by

Nagma Shakeel

(1801622006)

Under the Supervision of

Dr. Mohd. Haroon

Department of Computer Science & Engineering

INTEGRAL UNIVERSITY, LUCKNOW, INDIA

August, 2021

CERTIFICATE

This is to certify that **Ms. Nagma Shakeel** (Roll No.1801622006) has carried out the research work presented in the dissertation titled **“Detection of Malicious Nodes in Wireless Sensor Network Through Neural Network”** submitted for partial fulfillment for the award of the **Master of Technology in Computer Science & Engineering** from **Integral University, Lucknow** under my supervision.

It is also certified that:

i. This dissertation embodies the original work of the candidate and has not been earlier submitted elsewhere for the award of any degree/diploma/certificate.

ii. The candidate has worked under my supervision for the prescribed period.

iii. The dissertation fulfills the requirements of the norms and standards prescribed by the University Grants Commission and Integral University, Lucknow, India.

iv. No published work (figure, data, table etc.) has been reproduced in the dissertation without express permission of the copyright owner(s).

Therefore, I deem this work fit and recommend for submission for the award of the aforesaid degree.

Signature of Supervisor
Full Name: Dr. Mohd. Haroon
Designation: Associate Professor
Address: Integral University, Lucknow

Date:

Place: Lucknow

DECLARATION

I hereby declare that the dissertation titled **“Detection of Malicious Nodes in Wireless Sensor Network Through Neural Network”** submitted to Computer Science and Engineering Department, Integral University, Lucknow in partial fulfillment of the requirements for the award of the Master of Technology degree, is an authentic record of the research work carried out by me under the supervision of **Dr. Mohd. Haroon**, Department of Computer Science & Engineering, for the period from August, 2020 to August, 2021 at Integral University, Lucknow. No part of this dissertation has been presented elsewhere for any other degree or diploma earlier.

I declare that I have faithfully acknowledged and referred to the works of other researchers wherever their published works have been cited in the dissertation. I further certify that I have not willfully taken other's work, para, text, data, results, tables, figures etc. reported in the journals, books, magazines, reports, dissertations, theses, etc., or available at web-sites without their permission, and have not included those in this M. Tech thesis citing as my own work.

In case, this undertaking is found incorrect, I accept that my degree may be unconditionally withdrawn.

Date:

Signature

Name: Nagma Shakeel

Roll. No. 1801622006

RECOMMENDATION

On the basis of the declaration submitted by **“Nagma Shakeel”**, a student of M.Tech CSE (Evening), successful completion of Pre presentation on **20/07/2021** and the certificate issued by the supervisor **Dr. Mohd. Haroon**, Associate Professor, Computer Science and Engineering Department, Integral University, the work entitled **“Detection of Malicious Nodes in Wireless Sensor Network Through Neural Network”**, submitted to department of CSE, in partial fulfilment of the requirement for award of the degree of Master of Technology in Computer Science & Engineering, is recommended for examination.

Program Coordinator Signature

Dr. Faiyaz Ahmad

Dept. of Computer Science & Engineering

Date:____________

HOD Signature

Dr. M Akheela Khanum

Dept. of Computer Science & Engineering

Date: ________________________

COPYRIGHT TRANSFER CERTIFICATE

Title of the Dissertation: **Detection of Malicious Nodes in Wireless Sensor Network Through Neural Network.**

Candidate Name: **Nagma Shakeel**

The undersigned hereby assigns to Integral University all rights under copyright that may exist in and for the above dissertation, authorized by the undersigned and submitted to the University for the Award of the M.Tech degree.

The Candidate may reproduce or authorize others to reproduce material extracted verbatim from the dissertation or derivative of the dissertation for personal and/or publication purpose(s) provided that the source and the University's copyright notices are indicated.

NAGMA SHAKEEL

ACKNOWLEDGEMENT

I am highly grateful to the Head of Department of Computer Science and Engineering for giving me proper guidance and advice and facility for the successful completion of my dissertation.

It gives me a great pleasure to express my deep sense of gratitude and indebtedness to my guide **Dr. Mohd. Haroon, Associate Professor, Department of Computer Science and Engineering,** for his valuable support and encouraging mentality throughout the project. I am highly obliged to him for providing me this opportunity to carry out the ideas and work during my project period and helping me to gain the successful completion of my Project.

I am also highly obliged to the Head of department, **Dr. Mohammadi Akheela Khanum (Associate Professor, Department of Computer Science and Engineering)** and PG Program Coordinator **Dr. Faiyaz Ahmad, Assistant Professor, Department of Computer Science and Engineering,** for providing me all the facilities in all activities and for his support and valuable encouragement throughout my project.

My special thanks are going to all of the faculties for encouraging me constantly to work hard in this project. I pay my respect and love to my parents and all other family members and friends for their help and encouragement throughout this course of project work.

Date:

Place:
Lucknow

Table of Contents

LIST OF FIGURES

LIST OF TABLES

Abstract

Machine learning also inspires numerous practical ideas that help you make the most of your resources while also extending the life of your network. During the period 2002-2018, we provide a comprehensive evaluation of machine learning techniques that have been utilized to address common issues in wireless sensor networks, as shown in this article (WSNs). When applied to the relevant issue, the benefits and drawbacks of each suggested method are compared and contrasted. An overview of the available machine learning solutions is provided to assist WSN designers in developing the most appropriate machine learning solution for their particular application problems. It is the purpose of this research to give an overview of embedded network applications and to explain the needs that have been created as a result of this investigation. In addition, we reviewed the various in-network processing methods that were chosen and pointed out the similarity between the Hopfield neural network and the back propagation network that was discovered. Using a hop-field neural network, we were able to calculate the throughput, latency, and packet delivery ratio of networks in relation to the number of packets sent. We have compared the results of the back-propagation method with the results of the Hop-field neural network in this paper. Further complete simulations were carried out on the MATLAB-2013 command prompt as well as on the GUI that was developed during the course of the research. It was discovered that the value of all parameters, including transmission, throughput, E2Edelay, and PDR, is typically increasing with time. The use of neural networks with high iterating values in order to identify packet drops and therefore prevent packet drops would, therefore, result in a more effective solution for WSN test randomization, which will further reduce packet losses. In the suggested research, it was discovered in the first seven testing of the GUI and recommended seven times, which is consistent with the findings. Because just a small number of packets were lost in a single packet, it is obvious that a specific number of packets were transmitted in the first place when certain packets were sent. As a consequence, when it comes to digital data, the effects of the suggested effort are very apparent. When compared to the previous year, it has almost doubled. As a result, it is apparent that when neural networks use large iteration values, they perform much better in terms of packet loss minimization, owing to the employment of highly active pattern recognition methods, which will also repair packet loss issues. Because of this, latency and throughput from end-to-end are only marginally improved. As a result, the suggested system performs admirably in terms of Packet Drop During Transmission and Packet Drop Estimation.

Key Word: Throughput, E2Edelay and PDR, WSN, Packet Drop, MATLAB-2013

CHAPTER 1

INTRODUCTION

Wireless sensor networks (WSNs) are a relatively new technology that has attracted a great deal of interest from academics. Typically, a WSN environment consists of low-power, low-cost sensors that are dispersed randomly across the target area or that are manually redeployed to a new position. Wireless sensor networks have emerged as a strong and well-known technology as a result of its potential characteristics and uses in areas such as healthcare, monitoring, domestic applications, surveillance systems, and disaster management, among others. Wireless sensor nodes are limited in their ability to communicate, compute, and store energy, among other things. When it comes to wireless sensor networks, the broadcast message is a successful and widely used prototype because it allows many users to combine and disseminate message packets across the network efficiently in order to get the data, they are interested in. A WSN diagram is shown in the illustration below as an example.

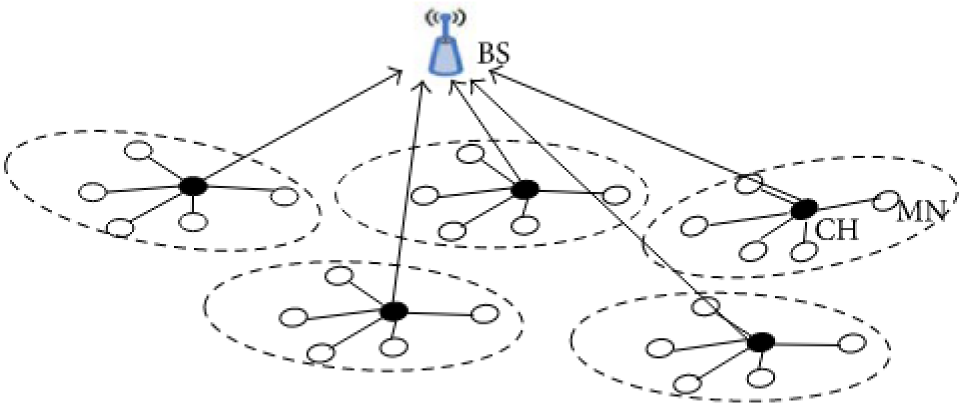


Figure 1. 1 Cluster-based WSN architecture

An example of a self-organizing network with a large number of sensor nodes is a wireless sensor network, which uses less power and is relatively inexpensive. Wi-Fi sensor networks are used in a variety of applications, including civil and military applications that require detection and security, as well as identifying environmental conditions and weather monitoring, such as sunray detection and movement of dust particles, sound and temperature monitoring, object identification and prediction, disaster sensing, and other applications. Because this kind of network has limited battery storage for the nodes, effective and correct use of the energy in WSN nodes is very important in order to extend the network's lifetime and increase its reliability.

These sensor nodes are characterized as lightweight and transferable devices that are capable of transmitting, detecting, and processing data as it is transferred from one node to another in a larger network of interconnected nodes. They have a limited transmission range and, as a result, transmit the data straight to the intended user, despite the fact that the transmission range is limited. Because WSNs are susceptible to both internal and external outbreaks, data transmission over greater distances may be accomplished via the use of intermediary nodes. Most of the time, they are unable to deal with a difficult adversary because of their limited resource availability. It is necessary in this situation to implement a secondary layer of security, often referred to as an Intrusion Detection System (IDS), in order to safeguard the system from the attackers. It is possible to identify the wide array of assault methods created by the attackers by using effective intrusion detection systems (IDS). Unfortunately, because of the characteristics of WSNs, the vast majority of sensor networks are extremely vulnerable to attack, and adversaries can simply generate network traffic, which can also cause heavy packet drop during the broadcasting of the packets or change the original content of the message in the packets, as well as cause network traffic to be generated. As a result, authentication methods are deployed in the network in order to provide safe communication between the nodes themselves. It is critical in wireless sensor networks (WSNs) to ensure that data transfer between nodes is safe.

The modern communication system requires high level standards for transferring information between one end to another end. This is possible only through wireless communication where as digital era is used nowadays for reliable communication. The wireless open channel environment is used as transferring medium between source and destination nodes. This wireless communication is categorized into Wireless Sensor Networks (WSN) and Wireless Body Area Networks (WBAN). The WBAN networks are implemented in humans and it senses the body conditions from various parts of human body and sends these information’s to the remote unit. In case of WSN networks, the numbers of sensors are deployed in a random manner and it collects the information from all sensors. This sensed information is sent to remote unit as sink. The number of sensors are grouped under the single node is called as cluster head. The cluster head collects all sensed information from its clustered nodes and each cluster head send these information's to remote sink.

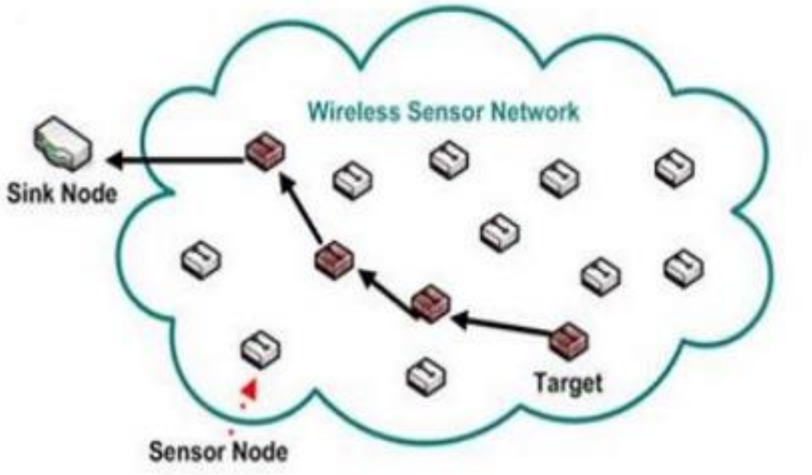


Figure 1. 2 Node's deployment in WSN network

In WSN networks, there may be number of cluster heads available with single sink node. Each node in WSN have sensor, analog to digital converter and processor. The sensor senses the surrounding parameters in analog mode and these sensed analog data are converted into digital data by means of analog to digital converter. This converted digital data is processed through processor unit and this processed data is transferred to another node by means of inbuilt wire antenna which is connected to node. Fig.2 shows the sensor nodes deployed in WSN environment with sink node connected to the WSN networks. The nodes behavior is changed by external attacker or hacker and these nodes become malicious/ hidden nodes. The performance efficiency of present WSN networks is degraded by number of malicious/hidden nodes. Hence, this paper proposes an efficient technique for identifying theses nodes in WSN in order to improve the performance.

1.1 Malicious Node Detection using Neural Networks

With the use of a neural network-based predictor, a method for identifying fraudulent sensor nodes and reducing their impacts has been developed. Using analytical redundancy, this approach estimates the value supplied by a sensor by considering the values provided by nearby sensors in the past and in the present, respectively. This estimate is compared to the actual value of the sensor in order to determine if the sensor's trust factor has increased or decreased.

1.2 Sensor Network Model

In relation to the sensor network, we assume the following assumptions:

As a result, the sensor network is static, which means that the sensor nodes are not movable; each sensor node is aware of its own position, regardless of whether it was distributed via aerial dispersion or through physical installation. If this is not the case, the nodes may acquire their own location by using the location process to do so. Furthermore, all of the sensors passed a one-time authentication process that was performed immediately after they were deployed in the field.

It is also important to note that the sensor nodes are comparable in terms of their computing and communication capabilities, as well as their power resources, to the current generation of sensor nodes, such as the Berkeley MICA motes, for example. When using symmetric cryptography, we presume that each node has enough storage capacity to store keying materials that may be hundreds of bytes in size in order to safeguard the transmission of information.

Assume that the base station, also known as an access point, which serves as both a controller and a key server, is of the laptop class and that it is provided with long-lasting power. It is also assumed that the base station would not be affected in any way.

In order to do this, we depend on the wireless cellular network (WCN) design. The base stations for this architecture have already been installed in the field, according to the design. Each base station creates a cell around itself that encompasses a portion of the surrounding region.

If the mobile wireless nodes and other appliances are within the range of a single cell, they may communicate wirelessly with one another. The primary difference between cellular network architecture and other network architectures is that base stations are considered to be mobile, so each cell has varying boundaries. This means that mobile wireless nodes and other appliances can communicate wirelessly as long as they are at least within the range of the mobile access point.

There are many key characteristics of the two kinds of sensor network designs described below (WCN and SENMA) that will be considered when building a secure sensor network: Nodes communicate with base stations directly; there is no need for node-to-node communication; there is no need for multi-hop data transfer; sensor synchronization is not required; sensors do not listen, but only transmit when polled; complicated protocols are avoided; the reliability of individual sensors is less critical; and system reconfiguration for mobile nodes is not required.

1.3 WSN Infrastructure and peripherals Basic

A new technology that has drawn considerable attention from scientists is Wireless Sensor Networks (WSN). Generally, the WSN environment needs low power, low overhead, and a large number of sensors that are randomly distributed at the target position or manually redeployed. Wireless sensor nodes are underpowered in terms of networking, computing, and energy. The transmitted message is an efficient and common wireless sensor network prototype that enables several users to quickly combine and relay packets of messages.

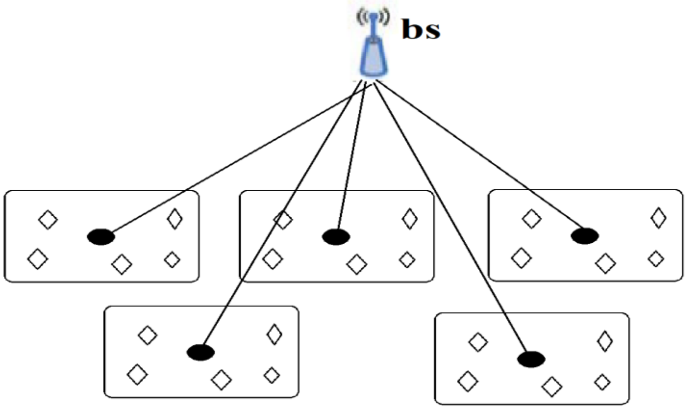


Figure 1. 3 WSN presenting Clustering formation

In a range of systems, wireless sensor networks are used, including mapping, surveillance, environmental reconnaissance, and weather forecasting for civil and military applications. There is inadequate storage capacity in the node battery for this type of network, so it is very important to utilize the resources in the WSN nodes efficiently and appropriately to improve the life of the network.

These sensor nodes are known as compact lightweight devices capable of interacting, sensing and analyzing data across a larger network than one node to the target node. They have a narrow contact range and therefore send the information directly to the desired consumer with the distribution of the transmission spectrum. Most commonly, because of their meagre means, they do not have the capacity to withstand a strong attacker. By making use of active IDS, it is possible to classify attackers who have planned huge attack techniques. Unfortunately, most sensor networks are quite sensitive to attacks due to the characteristics of WSN, and opponents may simply produce network traffic, and may even trigger substantial packet drops when transmitting the packet or changing the original material. For the packet to propagate. Authentication mechanisms are implemented on the network to ensure secure contact between nodes. Secure transmission of data between nodes within WSN networks is important.

The electronic network architecture needs strong standards for data transmission from one end to the other. This can be done only by a cellular network, since the internet era now uses encrypted contact. As a transmission mechanism, an open wireless channel environment is used between the source and destination nodes. This wireless connectivity is categorized by Wireless Sensor Networks (WSN) and Wireless Body Field Networks (BFN) over (WBAN). WBAN is used in humans and it senses body conditions in multiple parts of the human body and transmits this information to the remote computer. The sensor numbers are propagated randomly in the case of WSNs and information is collected from all the sensors. This sensed information is sent to the remote computer as a receiver. The number of sensors clustered together in a node is shown by the block head. The block header receives all the physical information from its clustered nodes and this information is transmitted to a distant watershed by each community chief.

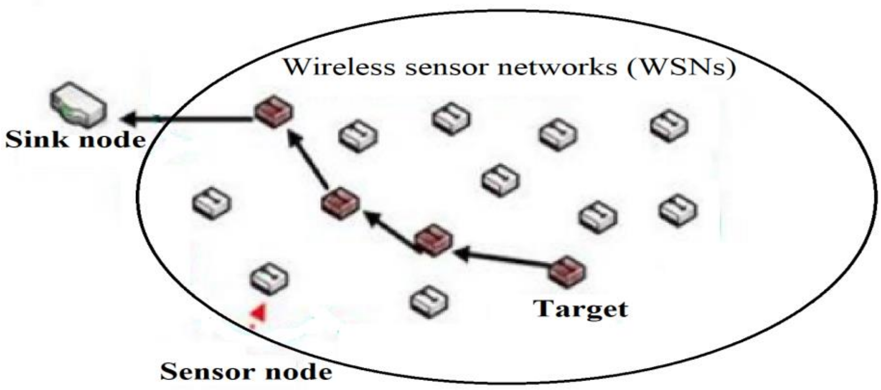


Figure 1. 4 Node's deployment in WSN network

A number of community headers can be reached on WSN networks with a single node in the basin. A sensor, an analog-to-digital converter, and a processor are all included with each WSN. The sensor senses the surrounding parameters in analogue mode and uses an analog-to-digital converter to transform this analogue sensor data into digital data. This transformed digital data is processed via a processor machine and this processed data is transmitted to another node via a built-in wired antenna attached to the node. Figure 1.2 displays the sensor nodes built in the WSN environment along with the basin nodes connected with the networks of the WSN. The activity of the nodes is changed by remote attackers or intruders and these nodes become malicious/stealth.

The efficiency of current WSNs' performance is decreased by the number of malicious/hidden nodes. Therefore, in order to increase performance, this paper suggests an important solution to WSN node discovery.

A network of wireless sensors is a form of wireless network comprising a wide number of devices called sensor nodes (called nodes). Circular, robotic, micro power and low-power systems are such devices. These networks, of course, cover a broad variety of distributed and battery-powered networked handheld computers for data collection, aggregation, and operator distribution, and have perfected skills in computation and processing. I'm going to. Nodes are small computers that shape a network by working together.

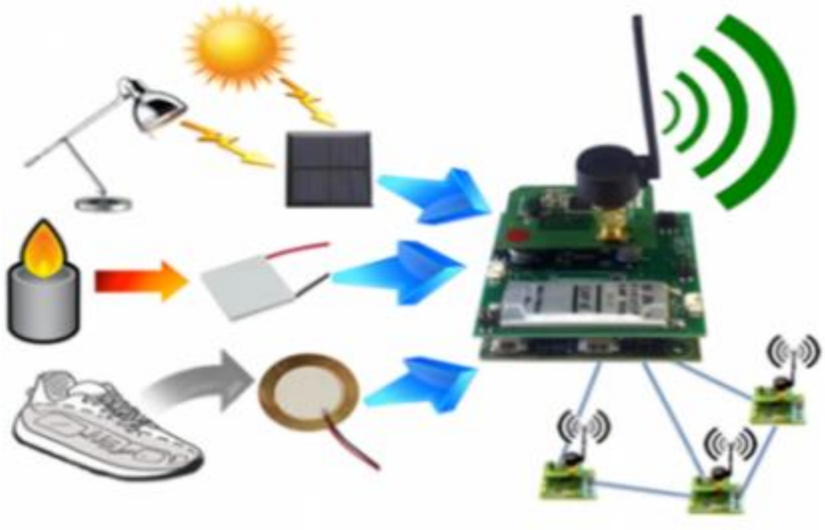


Figure 1. 5 wireless sensor network

The sensor node is a wireless system that is energy-efficient and multifunctional. Industrial food applications are common. To fulfil clear application aims, the sensor node assembly gathers data from the surrounding regions. The dying can use transmitters and receivers to communicate with one another. The death toll on a wireless sensor network could be in the hundreds or even thousands. Ad hoc networks have few nodes and no architecture, unlike network sensors.

1.4 Wireless Sensor Network Architecture

Previously, the most popular WSN architecture was the OSI architecture style. The architecture of the WSN comprises of 5 and 3 cross-layers. Five layers are primarily required for the network sensor: application, transmission, network, data link, and physical layer. Power management, mobile management, and mission management are the three intersecting layers. To achieve network, these WSN layers are used to make the sensors operate together to improve the network's overall performance. To find out: Wireless Sensor Network Forms and WSN Topology, follow the connection below.

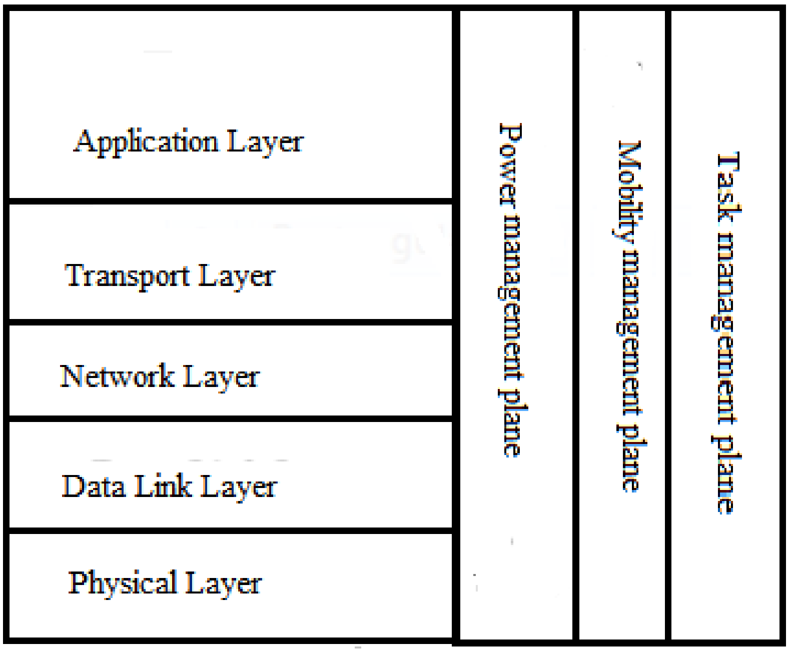


Figure 1. 6 wireless Sensor Network Architecture

1.4.1 Application Layer

The framework layer is responsible for handling the traffic and provides the programmer with clear application details that transform the outcomes skillfully. Sensor networks can be divided into several applications in various fields, such as agriculture, the military, climate and medicine.

1.4.2 Transport Layer

As certain protocols intended to provide this functionality are placed upstream, the task of the transport layer is to escape congestion and reliability. To detect and recover from losses, these protocols use many methods. When planning a device to link to other networks, the transport layer is completely needed.

It is rendered more energy effective by a reliable failure recovery. For WSNs, this is one of the main reasons why TCP is not suitable. The transportation layer can usually be separated into data packets under event guidance. There are many common protocols on the transport layer: STCP (Sensor Transmission Control Protocol), PORT (Protocol for Efficient Price Controlled Transmission), and PSFQ (Slow Forward Pumping).

1.4.3 Network Layer

Routing is the significant role performed by the network layer. It depends on the programmer, so it has a tone of characteristics, but in fact, the key tasks are power saving, some memory, buffers, sensors, there is no global ID and it has to be self-adjusting.

The basic idea of a routing protocol is to identify stable channels and redundant routes according to unclear metrics called numerous metrics for each protocol. In this network layer, there are many protocols that can be categorized into flat and hierarchical routing, which can also be divided into time, instances, and queries.

1.4.4 Data Link Layer

For the identification of data frames, data sources, MAC, error management, and point-to-point (or) point-multipoint reliability, the data link layer is responsible for data multiplexing.

1.4.5 Physical Layer

An edge that enables the bit stream to travel across the physical medium is given by the physical layer. Frequency spectrum, carrier frequency production, signal processing, modulation, and data coding are the explanations for this worksheet. As a representation of low-speed and wireless sensor network-specific regions, with low expense, power usage, density, and communication range, IEEE 802.15.4 has been proposed to improve battery life. To identify star and isotope topologies, CSMA / CA is used. There are several accessible IEEE 802.15.4.V versions.

1.5 The wireless sensor network characteristics

- Limits on power usage for nodes with batteries.
- The opportunity to cope with node crashes.
- Any modifications to contracts and uncertainty of contracts.
- Scalability across a wide delivery spectrum.
- The capacity to maintain stringent environmental conditions
- Simple to access
- Layered layout

1.6 Advantages in networks of wireless sensors

- It is necessary to incorporate network agreements without a defined infrastructure.
- Suitable for places that are remote, such as deserts, coasts, agricultural areas and dense woods.
- Flexible if there is an accidental scenario in which an extra workstation is required.
- The expense of deployment is not costly.
- Stop several of the wires.
- At any point, you will have adaptations with new gadgets.
- It can be opened by central tracking.

1.7 Wireless Sensor Network Applications

Wireless sensor networks, such as low sample rate, earthquake, magnetic, thermal, visual, infrared, radar, and sound, can consist of many various types of sensors and are smart to track a broad variety of surrounding circumstances. For continuous monitoring, event identification, event detection, and local control of actuators, sensor nodes are used. Network uses for wireless sensors specifically involve fitness, military, climate, home and other business areas.

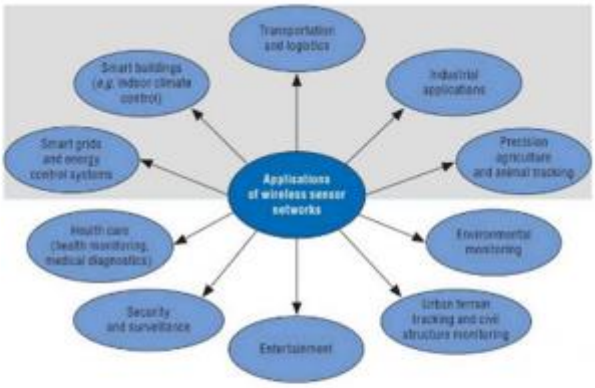

Applications of wireless sensor networks
Transportation and logistics
Industrial applications
Precision agriculture and animal tracking
Environmental monitoring
Urban terrain tracking and civil structure monitoring
Entertainment
Security and surveillance
Health care (health monitoring, medical diagnostics)
Smart grids and energy control systems
Smart buildings (e.g. indoor climate control)

Figure 1. 7 WSN Application

1.8 The following Wireless Sensor Network Applications

Applications in the military; applications in health; applications in the environment.

- Applications for the Home
- Applications in the Commercial Sector
- Monitoring of the surrounding area
- Environmental/Earth sensing technologies
- Air pollution monitoring and control
- Forest fire detection and prevention
- Landslide detection is important.
- Monitoring the water's quality
- Industrial monitoring and surveillance
- Health-care monitoring and evaluation

So, it comes down to networks for wireless sensors, architecture for WSN, functionality, and applications. We hope that you have a clearer grasp of this term. Also, please include your useful feedback by posting in the comment section below for any inquiries or for wireless sensor network project ideas.

1.9 WSN Network Topologies

The wireless network (WSN) topology requires a separate topology, including the one seen below, for radio transmission networks.

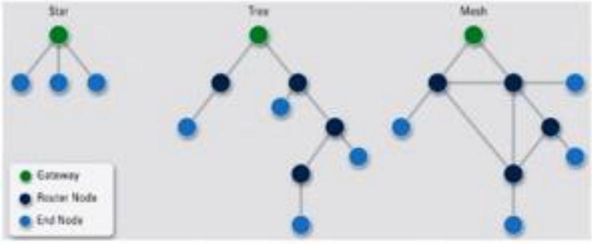


Figure 1. 8 wireless sensor topologies

1.9.1 Star Topologies

A star topology is a linked topology in which each node is connected to a gate directly. A single gateway can send messages to several remote nodes and accept them. Inside the installation topology, nodes do not transmit messages to each other. This decreases the communication latency between the remote node and the gateway (base station).

The gateway must be inside the radio propagation range of all specific nodes since it depends on a single node to control the network. The functionality to hold the power usage of remote nodes to a minimum and simply under control is included in the function. The network size depends on the amount of links that have been created to the hub.

1.9.2 Tree Topologies

The topology of a tree is sometimes called the topology of a cascading star. In the topology of the tree, each node is linked to the tree's highest node, then to the gate. The key benefit of the topology of the tree is that it is simple to extend the network and error detection is often easy. The drawback of this network is that it depends strongly on the carrier cable; the whole network would fail if it fails.

1.9.3 Mesh Topologies

A network topology enables data that is beyond the wireless communication spectrum to be transmitted from one node to another. When a node sends a message beyond the wireless range, an intermediary node is needed for the node to forward the message to the target node. The simplicity of separation and identification of faults in the network requires this benefit of the mesh layout. The disadvantage is that the network is big and needs a big investment.

1.10 Packet Loss Detection using Neural Networks

A neural network-based predictor is used to develop a method for identifying fraudulent sensor nodes and eliminating their influence from the system. This metric is compared to the actual sensor data in order to determine if the conviction rate has increased or decreased.

1.10.1 Packet Loss Detection in complex dynamic scenes

A particular neuron in the lobster brain that reacts intensely to photos of an approaching target like a predator is the Giant Lopula Motion Detector (LGMD). Without utilizing particular algorithms to identify artefacts, the computational model can tackle unpredictable situations. In this article, by integrating the excitement of Packet Loss Detection in a dynamic world, we suggest a neural network centered on LGMD. The network has a new mechanism for optimizing functionality and can optimize the extended edges of Packet Loss objects. The new mechanism filters out the isolated emotions produced by the context information. The advantages of the LGMD-based neural network presented in diverse environments were seen by offline research. Real-time robot experiments have shown that the usage of neural networks focused on LGMD as the only sensor mechanism enables the platform to perform successfully in a number of scenarios. Well-organized courtyards, especially those with complex histories, can be traversed by robots.

The Wireless Sensor Network is a geographically dispersed, autonomous wireless network of devices employing sensors that collaboratively monitor physical and environmental factors, such as the conditions at various places of temperature, sound, vibration, pressure, movements or pollution. The network nodes are linked using wireless channels. The electricity of each sensor node or of a battery is obtained. There are many sensor networks called sensor nodes, each with a tiny, lightweight and portable capacity. The transducer, micro-computer, transceiver and source of power are provided for each sensor node. The transducer creates electric impulses depending on physical and sensitive effects. A packet is a binary data unit that may be routed via a computer network. The dropping of packets is a compromised node that drops all or some of the packets to be sent. A tiny device called sensor node with the RADI, processor, memory, battery and the hardware of the sensor - is the Wi-Fi sensor network (WSN). The environment can be carefully monitored by extensive deployment of these sensors. Radio range, CPU speed, memory capacity and power are restricted in terms of resources to sensor nodes. The resource-free nature compels designers to create systems for specialized applications. This leads to certain patterns of communication on WSNs. Transportation is not as unpredictable as it is in ad hoc networks. WSN traffic is divided into one of three groups by Karlof and Wagner:

1. Many-to-one: A network's base station or aggregation point receives readings from many sensor nodes.

2. One-to-many: A single node (usually a base station or an aggregator) sends query or control information to numerous sensor nodes.

3. Local communication: To find and coordinate tasks, neighboring nodes transmit localized messages.

In addition, sensor nodes usually remain immobile, with a relatively low traffic rate in WSNs. There is also a regular flow of traffic. Long periods of inactivity may occur, during which sensor nodes switch off their radios and go to sleep in order to save energy used by idle listening. To take use of this WSN feature and conserve energy, MAC protocols such as S-MAC and TDMAMAC have been developed. Because sensor nodes rely on batteries, energy is a limited resource. Recharging or changing batteries is costly, and in certain cases, it may not be feasible. As a result, WSN applications must be particularly energy-conscious. The capacity to communicate in the real world through the wireless channel and sensor nodes to identify and manipulate a particular thing is one feature of WSN. Any of these nodes must work together to fulfil their objectives. On-line connections between the nodes o-one and a one via a Wireless Connection allows for a connectivity and a common functioning of the underpowered Wireless Sensor Network (WSN). They may work in extremely dynamic conditions, such as fighting and monitoring. Since WSNs work on their own, many unique assaults are rarely ignored. WSNs have recently acquired a great deal of press because of their broad adoption in the military and civic environments. WSN is commonly utilised in clandestine and often adverse places, for example military and domestic intelligence. The maintenance of netbook integrity thus requires authentications that achieve the overall objectives of comfort, data privacy, and trustworthiness. Today, artificial intelligence technology in the world has been employed, multiple artificial intelligence devices and protocols are utilized for different objectives. Artificial information agents and protocols play an important role in wireless sensor nodes.

A. Sensor nodes

The sensor nodes are used to manage the jobs in the network. Although measurements and queries may occur in the Task Manager, data may be sent via sensor nodes depending on these methods. Depending on device requirements computations may be done with a node If the model is constructed, it may either transmit data to the other nodes or it may be sent on to the task manager as it is. Therefore, the globe is the source. In the meanwhile, a device that receives data from a sensor is a sink or an actuator.

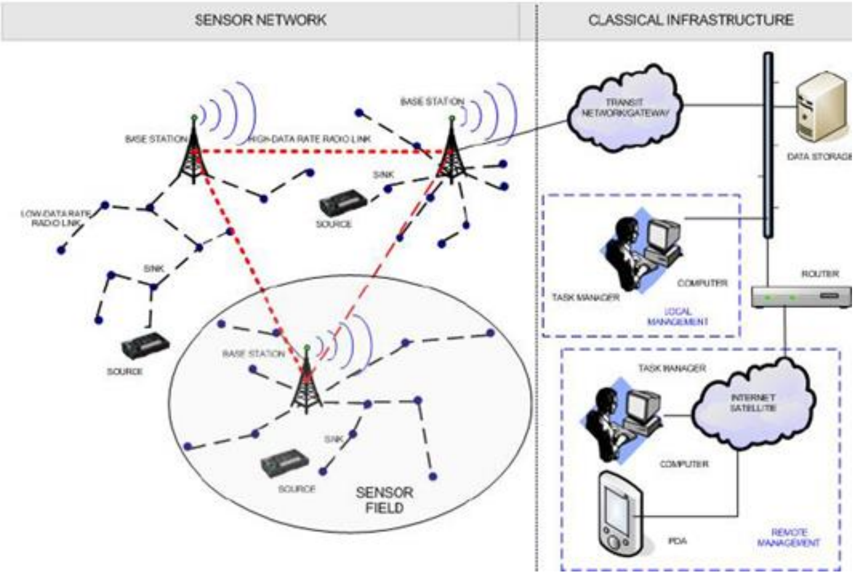


Figure 1. 9 Illustration of sensor network and peripherals

B. System Workings and Processes in a WSN

1.11 Communication Architecture

The sensor infrastructure is focused on this part. The node and sub-world sensors are tested. The sensors are tested. Before we proceed to protocols and Systems used to establish a network of sensors. It is essential to examine the entire savings in electricity and hardware/software One of the purposes of this survey is to gather and propose hardware for use on sensor nodes. A detailed description of the equipment may be acquired.

1.12 Sensor Node in communication architecture

This list includes the conventional sensor node controller, memory, sensors, communication system and power (see Figure 2). The job of a controller is that all the relevant data can be processed and arbitrary algorithms implemented. The memory functions are data and memory of the program. The communication techniques with the environment are input sensors and output actuators. These devices allow one or more environmental iterating to be monitories or regulated. The device interacts with radio waves. Finally, electronic components need to be supplied with electricity. Electricity efficiency is one of the major architectural considerations in WSN Therefore, these interconnected pieces must leverage the minimal number of resources to operate.

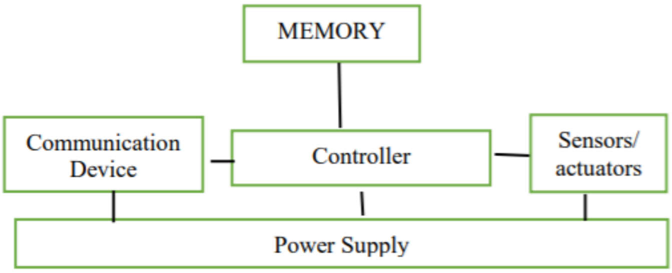


Figure 1. 10 Overview of sensor node hardware component.

1.13 Wireless Sensor Network Applications

These sensor networks use many sensors including low sampling rate, seismic, magnetic, thermal, visual, infrared, radar, and acoustic, and all these sensors have something in common: They all allow for monitoring of several aspects of the environment. Sensor nodes are often used for continual sensing, for events like the identification of an event or a change in state, as well as for event detection and local control of actuators. Wireless sensor networks are widely used to commercial, military, environmental, domestic, and other health and welfare applications.

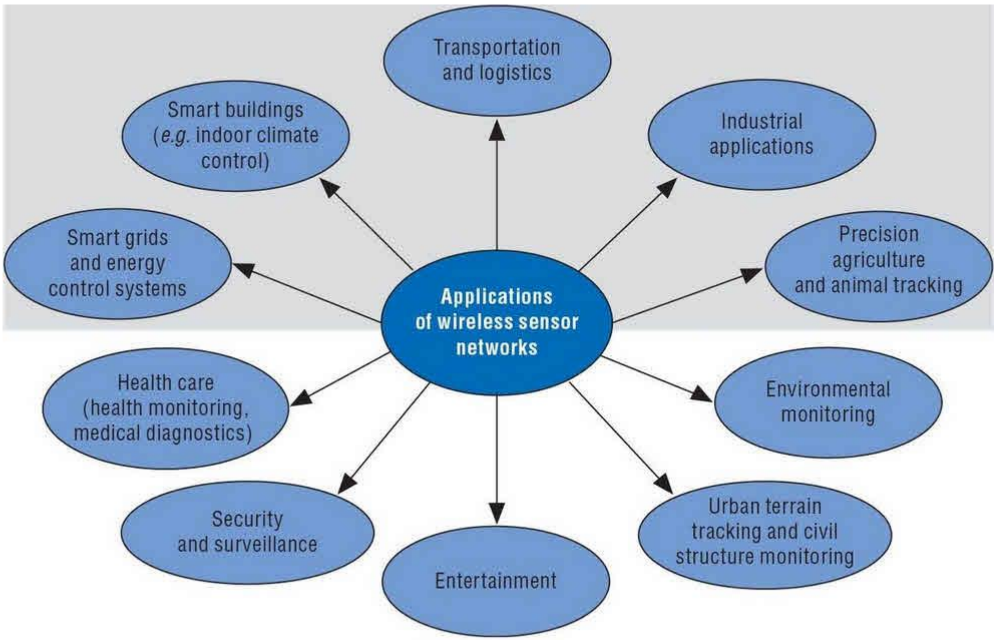

Applications of wireless sensor networks
Transportation and logistics
Industrial applications
Precision agriculture and animal tracking
Environmental monitoring
Urban terrain tracking and civil structure monitoring
Entertainment
Security and surveillance
Health care (health monitoring, medical diagnostics)
Smart grids and energy control systems
Smart buildings (e.g. indoor climate control)

Figure 1. 11 Wireless Sensor Network Applications

1.14 Design Issues of Wireless Sensor Network Architecture

The design issues of wireless sensor network architecture mainly include the following.

- Coverage
- Clocks
- Computation
- Cost of Production
- Design of Hardware
- Quality of Service

Coverage

A coverage algorithm is used for detection and transmission of sensors in the network of wireless sensors via the routing algorithm. The sensor nodes should be selected for the whole network. Efficient approaches are proposed such as lowest and maximum exposure route algorithms and a coverage design technique.

Clocks

WSN is a significant service for clock synchronization. This synchronization mainly involves providing the nodes of local clocks in the sensor's networks with an ordinary time scale. In some applications, such Clocks must be synchronized, such as monitoring and tracking.

Computation

The aggregate of data that passes through each node may be defined as the computation. The major problem with computing is that it must decrease resource use. If the base station's life expectancy is at risk, data processing will be completed at each node before data is sent to the base station. If we have resources at each node, the whole calculation should be done at the sink.

Production Cost

A huge number of sensor nodes are grouped in a WSN. As a result, if the price of a single node is extremely high, the whole network price will be quite high as well.

Ultimately, each sensor node's price must be maintained low. As a result, determining the cost of each sensor node in a wireless sensor network is a difficult task.

Hardware Design

Any sensor network's hardware, such as the power control, microcontroller, and communication unit, must be energy-efficient when designed. It may be designed in such a manner that it consumes less energy.

Quality of Service

Service quality or QoS is only that the data has to be shared in time. Because some sensor-based applications rely mostly on time in real time. Therefore, the data will be meaningless if the data is not transmitted to the recipient in time. In WSNs, many sorts of QoS problems are identified, including network topology that may often change and the available information state utilized for routing may not be accurate. Mainly QoS cover PDR, E2Edelay and Throughput in this investigation.

This permits to maintenance least power utilization.

But other network nodes are authorized to transfer messages from one node to the next in the network, enabling the multi-hop capability. In general, the multi-hop nodes have high power and are often connected to the main line. This is the topology adopted by the forthcoming ZigBee standard network.

1.15 Structure of a Wireless Sensor Node

Different units such as sensing, processing, transceiver & power are the components for making wireless sensor nodes. It has other components which rely on an application, such as a power generator, a searching system and mobilizer. Two parts, namely ADCs and sensors, often incorporate sensing units. In this respect, sensors create analogue signals which may then be sent to the processing unit by means of ADC into digital signals. In general, the sensor node may be combined to do the activities with the other nodes in order to do the assigned sensing activities through a small storage unit. With the assistance of a transceiver unit the sensor node may be linked to the network. One of the most important components of the sensor node is a sensor node. The power units are supported by solar cell-like power scavenging units, while others rely on the application. A functional block diagram with wireless sensor nodes is seen above. These modules are designed to meet the needs of large applications on a flexible platform. For example, the substitution of a signal conditioning block may be done depending on the sensors to be placed. This allows the usage of the wireless sensing node of various sensors. Similarly, for a given application the radio link may be switched.

1.16 Sensor Network Model

We assume the following presumptions with respect to the sensor network:

(a) It is static in that the sensor nodes are not movable; thus, each sensor node knows its own location, regardless of whether it is deployed via antenna spread or physical fixing. If this is not the case, the nodes will be assigned their own location through the placement process.

(b) Sensor nodes in computation, networking and power tool capacities are similar to existing generation sensor nodes, such as MICA Berkeley. We presume that every node has space to store up to hundreds of bytes of core content in order to safeguard information transmission using symmetric encryption.

(c) The base station, also known as the entry point, which functions as the master controller and server, is a laptop and is provided with energy for a long period of time.

(d) The architecture of wireless cellular networks is our focus (WCN). A number of base stations in this architecture have already been built in the sector. A cell that covers a portion of each base station's region is created around it.

1.17 Objectives of the work

- To detect the malicious activities in WSN
- To estimate the packet loss and delay of transmission.

- Perform the test and established the relation of attack of WSN and loss of network quality.

CHAPTER 2

REVIEWOF LITERATURE

Sharma & Lobiyal (2015), Each responsive node in a densely dispersed sensor network detects an event and broadcasts it to a specific party through a multi-hop connection established between the nodes. Sensor nodes located near the basin node need more data transmission and control packets, and as a result, they are subjected to considerably greater rates of energy depletion and, as a result, are anticipated to have a substantially shorter network life than other sensor nodes. In order to minimize this issue, the efficacy of some of the most often used methods was tested, and the results of the simulation were used to verify the research. In terms of transmitting speed and packet distribution speed, the AODV and DSR protocol are superior to TORA, though AODV is superior to DSR and TORA in the operating efficiency state. AODV is similar to DSR and TORA protocols with fewer end-to - end latency and average power usage, although the packet drop rate in the TORA protocol is larger. Compared to AODV and TORA, the routing load on the DSR protocol is smaller.

Roy et, al. (2020), Since wireless sensor networks must send data to sensors placed near the basin, they now confront the most severe energy challenge. The current existing methods to the energy problem believe that the best option is the Mobile Sink (MS) technique. Though allowing MS to traverse each of the nodes in order to gather data increases the latency. A block-based routing protocol that seeks to retain the strength of the sensor nodes to boost the existence of the network achieves the data transmitted to the site of residence. In addition, in many WSN-sensitive coverage implementations, expanding the existence of the coverage is equally essential, as is network life. To maintain network coverage, even if some nodes are down, the recommended parameter range is utilized in this article.

Rai et al. (2017), Quality of service is of vital importance to wireless sensor applications, especially since the needs for various aspects of the use of wireless sensors are rising. Many technologies used in wireless sensor networks (WSN) have many restrictions when it comes to design and standards, thus maintaining the operational standard in these networks is a tough task. While traditionally, QoS has focused on the level of the network, such as latency, efficiency, and volatility, it must now include use cases like mobility, data analytics, and IoT. They provide in this document all of the necessary WSN criteria, including facilities, roles, and capacity, and they also promote the archiving of qualified services. When it comes to raising the quality of WSN services, there are three important quality factors to keep in mind: cost, efficiency, and customer retention. Several important requirements for wireless sensor networks' decentralized and complicated architecture include lowering power consumption and increasing the network's life span, among other things.

Fotohi & Bari (2020), In Wireless Sensor Networks (WSN), there are many nodes whose main tasks are to monitor and control ecosystems. Additionally, the sensor nodes are dispersed according to how the network is being used. One of the most challenging aspects of this kind of network is the use of power by the sensor nodes. This rapidly decreases the sensors' power usage. The useful life of the network, however, reduces. Sensor nodes are susceptible to several attacks due to their weaknesses, one of which is Sleep Attack Denial (DoSA), which threatens WSN. Therefore, by preventing the nodes from accessing sleep and power saving mode, the DoSA assault implies the lack of power on these nodes. A travelling gutter is thus used to maximize the use of electricity and to enhance the service life of the network. To block DoSA, the Firefly algorithm for node pooling and two-level authentication was suggested. In addition, the Hopfield neural network detects the pelvic motion orientation route for the transmission of CH data, which is used to guide the transmission of CH data.

Liu (2017), a problem for power-constrained WMSNs is how to reconcile service quality and energy efficiency criteria. The theoretical review of the MAC layer and PHY layer design focused on the IEEE 802.15.4 standard intends to analyses the layer-to-layer analytical model to provide a more comprehensive view of the relationship between sensor network parameters and efficiency, and pave the way for more developments in active studies on multichannel optimization. Find an efficient performance measure and create an effective performance selection or scoring technique that is focused on the necessary parameters and that can be utilized as parameter inputs for the multichannel allocation process in order to maximize efficiency. Based on lightweight and highly effective computational intelligence technology, a robust dynamic control scheme for multi-channel assignment tasks is planned. Introducing the multi-channel mapping mechanism of MCDB FLS. As parameters to monitor the adoption of the multichannel implementation, the proactive bandwidth usable in the layers is calculated. In addition, for device acceptability control, the fuzzy logic-based bandwidth threshold model offers complex optimization. Simulations demonstrate that in QoS and Energy Quality measurements, MCDB FLS does higher than benchmarks, and allows a trade-off between energy efficiency and increased QoS. Additionally, all action weight settings are applied on the basis of a controlled multilayer learning workbook with a community grouping policy that is implemented. The major weight fusion system aids in the reduction of energy consumption since it was discovered in the first stage of the learning process that the main atmosphere exists.

Zhu et al. (2019), There is great potential for wireless sensor networks (WSNs) to be used in a wide range of applications such as military and intelligent transportation, the health and medical sectors, environmental monitoring, and so on. It is essential for accurate and fast diagnosis of wireless sensor network problems, not only as a guarantee of dependability, but also for other reasons. This article described and analyzed the root cause and description of wireless sensor network failures, with a particular emphasis on the current state of research in fault diagnosis technologies at the national and international levels.

Anastasi et al. (2010), Wireless Sensor Networks (WSNs) are a highly promising wireless technology solution for industrial applications that is currently under development (WSN). However, for the reliable deployment of WSN networks in an industrial environment, four important criteria must be fulfilled, namely, energy consumption, scalability, flexibility, and timeliness. These authors focus their attention in this paper on WSNs based on the IEEE 802.15.4 standard, and they indicate that they may have a major reliability problem. This issue occurs when energy conservation is allowed by the power management mechanism, and this results in a very low delivery rate of packets, and also when the number of sensor nodes in the network is very low (for example, 5). To explore the root causes of this problem, based on simulations and tests on a real WSN, and find that it is triggered by the conflict-based Media Access Control (MAC) protocol used to access channel and default parameter values. They have also noticed that it is possible to minimize the issue and reach a delivery rate of up to 100 percent, at least in the situations covered in this paper, by setting more acceptable MAC parameters.

Khan et al. (2013), Their aim in this article is to examine how PDR and absolute latency in wireless sensor networks are influenced by distinct topological configurations. This paper also focuses on analyzing the output for mission critical applications of three distinct network topological configurations.

Sunitha, & Chandrika (2016), Several risks are created to preserve the reliability and protection of the network because of the mobility of the sensor motes. In the field of data production, data mining is also a burgeoning technology; it advances various data pre-processing, data interpretation, and data mining strategies and methods, such as data aggregation, correlation, grouping, and prediction. Today, several researchers face major problems in the wireless sensor network, such as limited capacity, processing limitations, node storage limitations, each sensor's power usage, wide area coverage, and protection. Many studies have identified many algorithms, methods, methodologies for defense of privacy, but they are not 100 percent optimized solutions yet.

Sunitha & Chandrika, (2016), 1. The Industrial Internet of Things (IIoT) has attracted great attention from academia and industry with the growth of information technologies and smart manufacturing. With diverse implementations in many areas, including environmental tracking, Wireless Sensor Networks (WSN) have many benefits, making them a very significant part of the Internet of Things. Power exhaustion and hardware failures, however, in WSNs will cause node failure. Wireless channel transmission may even be influenced by the manufacturing climate, contributing to network stability challenges, even with closely integrated data and control levels in conventional networks, which also raises the expense and difficulty of network management. Uh.

Com. They are adding a new Software Information Network (SDN) in this document and changing this network to propose a system named the Wireless Sensor Network (SD-WSN) Improved Software Specified. The following issues may be solved through this new structure.

1) Address the issue of network optimization and smooth convergence of WSN into IoT for large-scale heterogeneous networks.

2) The issue of network coverage is overcome, which increases the network's stability.

3) Due to different issues, particularly related to power consumption, the system handles node failure. The stability of wireless sensor networks must also be enhanced by designing complex schemes to minimize power consumption and latency time for network nodes under IoT conditions. Experiments have shown that node power usage and delay time are greatly decreased by the enhanced solution, thereby improving WSN efficiency.

Barki et al. (2018), In MANET networks, the complex behavior of the nodes renders administration and management challenging. Researchers also worked to develop the routing protocol used in order to address these issues. In this paper, from a compilation of methods and techniques suggested by researchers in this area, they investigate the impact of ANN in the assessment of quality and efficiency in MANET networks and try to use this analysis in a summary table to conclude conclusions and potential improvements to these methods.

Singh & Dhaka (2016), Dynamic conditions that shift fast over time are tracked by wireless sensor networks. This complex behavior is triggered by external variables or is initiated by the programmers of the device themselves. Sensor networks also implement deep learning approaches to remove the need for excessive overhaul in order to respond to those conditions. Machine learning often inspires several realistic ideas that optimize the usage of energy and prolong the network's existence. In this paper, they offer a systematic overview of the 2002-2014 literature of machine learning approaches used in Wireless Sensor Networks (WSN) to solve popular problems. The benefits and drawbacks of each suggested algorithm are measured against the corresponding problem. In order to help WSN programmers build machine learning strategies tailored to their application problems, they also have a comparative reference. They give an outline of applications for embedded networks and address the criteria that arise from this discussion. In addition, inside the network, they speak about selected processing strategies and mention the similarity between neural and posterior Hopfield propagation networks. It is described within the sense of the sensor network in the following neural networks. In the framework of sensor networks, they define the motivation and operational condition of neural networks and they analyses the first findings obtained from their implementation of the test. With these models, they claim, there is a high potential that promises a strong influence on future study, especially when implemented as hybrid technology. In order to locate a Packet Loss in the sensor network, they are doing this for WNS and also to try to find out the throughput importance of data sent via the sensor network.

Gupta & Pal (2016), Wireless ad hoc networks map complex conditions that shift quickly over time. This complex behavior is triggered by external variables or is initiated by the programmers of the device themselves. Ad hoc networks also implement machine learning methods in order to respond to certain situations to eliminate the need for needless overhaul. Machine learning often inspires several realistic ideas that optimize the usage of energy and prolong the network's existence. In this paper, they present a detailed literature analysis of machine learning approaches that have been used to resolve popular issues in ad hoc wireless networks (WSN) between 2002-2014. The benefits and drawbacks of each suggested algorithm are calculated against the corresponding problem. In order to help WSN programmers build machine learning strategies tailored to their application problems, they also have a comparative reference. They give an outline of applications for embedded networks and address the criteria that arise from this discussion. In addition, inside the network, they speak about selected processing strategies and mention the similarity between neural and posterior Hopfield propagation networks. It is discussed within the context of the ad hoc network in the following neural networks. In the framework of ad hoc networks, they define the motivation and operational condition of neural networks and analyses the first findings obtained from the application of experiments. With these models, they claim, there is a high potential that promises a strong influence on future study, especially when implemented as hybrid technology. They enforce this such that in an ad hoc network, WNS detects a Packet Loss and they often aim to figure out the throughput benefit of data sent through the ad hoc network. On ad hoc wireless networks, they simulate a Trojan attack and determine the network impact. Using MATLAB-10 simulation programmer, they conduct their simulations consisting of a list of all network protocols to model different current network architectures. MATLAB-10 does not include any malicious protocol emulation units, but it includes dedicated wireless routing protocols. Therefore, they first apply a new Trojan protocol to MATLAB-10, to simulate Trojan assaults. In order to simulate a Trojan threat, they began their research by writing a new AODV protocol using MAT files. They conducted experiments on multiple topologies to assess network output with and without Trojans on the network after adding a new routing protocol that simulates a Trojan horse. Unsurprisingly, network efficiency has dramatically degraded due to the existence of Trojans. Next, to remove the impact of the Trojan horse on the AODV network, they suggested an IDS approach. In MATLAB-10, they apply the solution. And they test the conclusions as they did with the Trojan. As a consequence, their approach, with a 24-38 percent success rate, removed the Trojan influence.

Vij & Joon (2017), Wireless sensor networks consist of individual nodes that, by the identification or regulation of physical parameters, may communicate with the world. For the success of their assignments, these nodes shall collaborate. The nodes are interconnected and each Wireless Sensor Network (WSN) is a community of sensors with limited resources capable of interacting and collaborating with each other to accomplish a shared objective by wireless connexons. In rugged conditions, such as battlefields and observation zones, sensor nodes run. They give an outline of applications for embedded networks and address the criteria that arise from this discussion. In addition, inside the network, they speak about selected processing strategies and mention the similarity between neural and posterior Hopfield propagation networks. It is described within the sense of the sensor network in the following neural networks. In the framework of sensor networks, they define the motivation and operational condition of neural networks and they analyse the first findings obtained from their implementation of the test. With these models, they claim, there is a high potential that promises a strong influence on future study, especially when implemented as hybrid technology. In order to locate a Packet Loss in the sensor network, they are doing this for WNS and also to try to find out the throughput importance of data sent via the sensor network. On the MATLAB command prompt and the Interface produced during the quest, another complete simulation was performed. Find great value for all words for parcel delivery, such as efficiency, E2Edaly, and PDR. The propagation of the neural network with a large PARAM value will then offer a safer option for spontaneous WSN Packet Loss Detection tests and prevent more packet drops. They discovered it by checking the GUI seven times before and seven times for recommendation, based on recommended studies. It is obvious that only 51 packets were missing when the 1280 packet delivery was sent and 105 packets were lost earlier when sending the same data packet. So, they have a rather noticeable outcome of the suggested work in digital records. Compared to before, almost twice. So, it is very obvious that when a neural network with high PARAM value is implemented, thanks to highly active pattern recognition technologies, it has a great improvement in reducing packet loss to a minimal, which would also correct the loss concern. From packets. Therefore, both the final delay and output changed marginally. The suggested systems therefore do a better job of identifying accidents during transmission and stopping them.

Zhao et al. (2018), The target tracking problem has always been the wireless sensor network access point, and with the introduction of a modern streaming and multimedia streaming application, new streaming efficiency criteria have been proposed to drive target tracking; Thus, in this paper , they propose a network-based software-defined adaptive hierarchical routing algorithm for a wireless sensor The algorithm takes both network strength and efficiency into account, uses the Hopfield Neural Network algorithm to determine the optimal path as local routing (LR) between neighboring clusters, and adopts a local route-based multiple-choice backpack problem model. For the end to be reached. -- Worldwide final instructions, under various objective scenarios, to obtain target monitoring knowledge routing. Physical trials and simulated studies are used in the test bed. The experimental findings indicate that, in various test conditions, the suggested algorithm is superior to the Low Energy Adaptive Cluster Hierarchy (LEACH) and the Sequential Mapping Directive.

Alhashemi & Almomani (2019), Current advances in the field of communication are contributing to ongoing and immediate demands for innovative technology in the field of data transmission that can render the communication process more efficient and stable. Recently, WSN has arisen as a common and significant form of network that can be utilized in a setting that a human being cannot continuously handle. In order to drive the efficiency of WSN in terms of different parameters, including age and capacity, it is possible to use different behavior, such as meeting. As a common grouping strategy in WSN, KSOM appeared. The purpose of this article is to determine WSN’s efficiency in terms of average life and energy consumed after introducing Kohen to the role of the neural network. Results revealed that compared to the LEACH procedure, lifetime efficiency improved by 9.1 percent, while energy usage decreased by 3.03 percent.

Ahad et al. (2016), Due to the highly complex and frequently uncertain environmental factors that define wireless networks, modern wireless network architecture, including decision making and parameter optimization, is incredibly challenging. In order to cope with this dynamic architecture, there is a common trend in digital networks to integrate artificial intelligence (AI) technologies. The well-established Artificial Intelligence Architecture for Neural Networks (NN), which is well recognized for its extraordinary generality and flexibility, has been adopted, although a range of AI innovations have been profitably utilized in the wireless networking community. For cellular networks in a number of settings. In particular, for tasks that require sorting, learning, or development, NNs are particularly common. They include a presentation of common NN models in this paper, as well as a detailed analysis of NN applications in wireless networks. In specific, as they evaluate alternate AI frameworks and technologies, they also discuss the drawbacks and complexities of NN implementation. While there are several NN surveys in the literature, to their knowledge, their paper is the first in red based on NN applications in wireless networks.

Alarifi & Tolba (2019), The wireless sensor network (WSN) architecture is enabled by the Cloud Aided Internet of Things (C-IoT). The sensor network for Internet of Things (IoT) sensor nodes is a self-contained collection of independent resource constraints. In a dedicated way, the nodes connect to transfer knowledge across the simulated world from the server. WSN clustering aims to increase the efficiency of the network by regulating the use of resources and improving the precision of data processing. The C-IoT service prices are increased through this. It needs complicated clustering algorithms to optimize IoT sensor networks via power and overhead control. The required output enhancement during streaming in a virtualized setting may not be accomplished by a simple stacking scheme. This document aims to suggest, with the assistance of the sensor network, an augmentation-based learning system, Adaptive Q-Learning (AQL), to enhance network efficiency with minimal power-offset in CIoT. AQL functions in two separate phases: selecting the party chief and choosing the carrier. In order to rate a contract based on its previous actions through the show, a decision-making mechanism is used. Using the conditions of adaptive redirection and head placement, AQL optimizes coordination with and within classes. The simulation results show the accuracy of the proposed AQL by retaining, considering the decreased overhead on the sensor network, the number of active nodes in the network and its constant power. The efficiency of CIoT is significantly enhanced with the realization of constructive characteristics in sensor networks. Experimental findings indicate that the proposed learning technology is successful in enhancing network existence with a strong demand response rate and reducing waits, higher prices, and request failures.

Madhav (2017), In the analysis, a data compression method using Huffman code, LEACH and Dijkstra algorithms showing effective nodes of data transmission maximized the useful life of the network. A major security concern arises during transmission, primarily in military areas or other high security areas where several attackers attempt to break records. The research performed on network protection is therefore aimed at establishing a security pattern to secure the data transmitted over the network. Noise, redundancy, and missing values are some of the other typical problems arising on the network during packet transmission. The completed work given an adaptive preprocessing approach that uses Principal Component Analysis (PCA) and the Hopfield Hyperbolic Neural Network (HHNN) to streamline data flow in order to solve these problems. By increasing the precision of the forecast, this method gives greater performance. Collecting and scheduling data in various aquarium settings is the other major issue with WSN. The study used TDMA scheduling to predict delays in data collection and reduce high power usage in order to solve the issue, whereas the pocket route algorithm (PDT) decreases redundancy. The findings indicate that in the simulation, the quest was successful. The results of the simulation show high performance in terms of reduced delays, increased network existence, increased security, decreased power usage, and decreased data loss during wireless sensor network data transmission. The suggested study has now been effectively conducted, producing stronger performance than other existing approaches used to address some of the issues handled by wireless sensor networks.

Dang et al. (2020), The internal fingerprint position technique based on channel status information (CSI) has received widespread interest. However, due to low fingerprint resolution, unsatisfactory classification and matching effect, and sensitivity to environmental effects, this approach struggled to have a stronger locating effect and a higher locating accuracy. This article proposes a CSI-driven internal fingerprint position mechanism based on the Hopfield Discrete Neural Network (DHNN) to solve the problem. The strategy generally consists of offline and online steps. A low-pass filter is used to preprocess the fingerprint information for each reference point in the offline stage, after which the step difference is followed to correct the fingerprint details of all the reference points. This increases the accuracy of fingerprint data, while eliminating issues such as internal environmental shifts, the impact of multi-path signals, etc. impacting fingerprint data. Finally, after collecting reasonably detailed fingerprint details, a premium fingerprint database was developed. Data from each landmark in the fingerprint database is allocated as attractors in the online process, to ensure data accuracy. Meanwhile, for affinity decision through DHNN, the position information of the test point is processed. Ultimately, they find the results of the translation. The experimental findings have shown that localization accuracy with an average error of 1.6 m can be accomplished in the experimental setting using the proposed procedure. It has better stability compared with alternative approaches, and can significantly minimize labor costs and time.

Dang et al. (2020), The internal fingerprint position technique based on channel status information (CSI) has received widespread interest. However, due to low fingerprint resolution, unsatisfactory classification and matching effect, and sensitivity to environmental effects, this approach struggled to have a stronger locating effect and a higher locating accuracy. This article proposes a CSI-driven internal fingerprint position mechanism based on the Hopfield Discrete Neural Network (DHNN) to solve the problem. The strategy generally consists of offline and online steps. A low-pass filter is used to preprocess the fingerprint information for each reference point in the offline stage, after which the step difference is followed to correct the fingerprint details of all the reference points. This increases the accuracy of fingerprint data, while eliminating issues such as internal environmental shifts, the impact of multi-path signals, etc. impacting fingerprint data. Finally, after collecting reasonably detailed fingerprint details, a premium fingerprint database was developed. Data from each landmark in the fingerprint database is allocated as attractors in the online process, to ensure data accuracy. Meanwhile, for affinity decision through DHNN, the position information of the test point is processed. Ultimately, they get the results of the translation. The experimental findings have shown that localization accuracy with an average error of 1.6 m can be accomplished in the experimental setting using the proposed procedure. It has better stability compared with alternative approaches, and can significantly minimize labor costs and time.

Jyoti, (2016), A Wireless Sensor Network (WSN) is made up of a large number of sensor nodes that are constrained in the spectrum of battery power and connectivity and have different models of sensor capability. Environmental tracking is one of the most significant features of a wireless sensor network. A Wireless Sensor Network (WSN) incorporates autonomous, spatially dispersed sensors to monitor physical or maintenance requirements such as noise, sound, vibration, temperature, motion, or pollutants and to collaboratively transmit their data across the network to a key location (base station or basin). Only multi-directional antennas are fitted with wireless sensor networks, which may cause heavy Packet Loss. In these networks, the output per node tends to decline as the number of nodes grows. To minimize interruption, it is also recommended to transmit with several short-range hops. The clash of packets allows wireless networks to destroy packets and consume energy. Thanks to explosive flow and pollution across the ports, it gets worst in thick WSNs. To retrieve the found beams, they suggest a neural network diagram in this paper. The proposed study prevents Packet Loss with a neural network in Hopfield and improves the pace of packet transmission and network latency, thus reducing the delay of end2.

Din et al. (2020), The usage of sensors has been in high demand in all systems, as well as in today's lives. The public domain has also begun to shift towards smartphone apps that are more available. For eg, school child monitoring, fitness tracking, tracking device, fire detection, etc. Therefore, the preferred alternative for satisfying these needs is a Wireless Sensor Network (WSN). However, WSN itself remains hindered by restricted battery use notwithstanding the excitement for developing different applications with the sensors. Various forms of studies have been undertaken to resolve this concern owing to certain applications that need a long battery life. The role of artificial intelligence (AI) to improve the sensor's battery life is one of those reasons. Fuzzy Reasoning (FL) is one of the favored AI structures that researchers have opted to incorporate for WSN to improve WSN's lifetime in particular. There are three organic functions of Fuzzy Logic that must be tested for potential in WSN applications. To achieve the best results for studying the usage of sensor batteries, the recommended solution is to mix various forms of fuzzy logic organic functions that are triangle with Gaussian and Gaussian with trapezoid and trapezoid with triangle. Touch cost, core strength, and residual power as mist input are criteria used for community head selection. This solution would use an established multilevel algorithm (Plot) algorithm and this is part of the development of the MAP towards WSN's lifetime. During data transmission, the findings can compare, examine and analyses the dead node count and power use of the sensor node. In conclusion, the lifetime of the sensor network will be increased with this approach since the technology introduced can reduce the energy consumption of sensor nodes.

Li & Serpen (2016), This article suggests that an artificial neural network be used in a completely distributed parallel computing mode in a wireless sensor network. The aim is to provide cognitive knowledge and adaptability for the wireless sensor network for better autonomous activity. A case study in which a Hopfield neural network designed as a static optimizer for a poorly linked dominant group problem is used in a wireless sensor network to enable it to tailor the network architecture to future improvements immediately and after deployment in the field illustrates the applicability and usefulness of the proposed model. In order to reflect the network infrastructure, the loosely related minimum dominance range established for the wireless sensor network topology diagram model is used and can be recalculated any time the topology of the sensor network shifts. A simulation analysis was performed with up to 1000 TOSSIM emulators utilizing the TinyOS-Mica sensor network platform. The time complexity, message complexity, and consistency indicators of the approach to the case study were measured and assessed. The simulation results showed that, as a static optimizer, the WSN integrated with the Hopfield neural network was competing with other local or distributed algorithms to demonstrate its viability for the poorly related dominant group query.

Karthikeyan et al. (2017), In order to find the shortest stuck path, numerous intellectual enhancement demonstrations, such as artificial neural networks (ANN), genetic algorithms (GA), etc., have been scheduled. As the two major fields are dedicated cell networks (MANET) and wireless sensor networks (WSN), rapid expansions of wireless connectivity have been accomplished largely in the sector of mobile phone networks. In the mobile wireless network, fabric avoidance is the greatest obstacle, i.e., the topology of the network varies with time owing to energy conservation or node versatility. The dilemma of dynamic optimization is related to the versatility of the nodes in order to find the shortest path (SP) in this network. The nodes normally die or may switch due to power reduction, and this situation makes it more challenging for the network to find the shortest path. In this paper, they propose a new approach for the identification and orientation of shorter dynamic paths in MANET using genetic algorithms (GA). One of the fastest rising wireless networks of the next decade is MANETs. Initial findings show that after each update, the GA-based algorithm will respond rapidly to environmental change (i.e. change in network topology) and generate high-quality solutions.

Polastre et al. (2004), They include an in-depth analysis of the use of wireless sensor (WSN) networks to track real-world ecosystems. To meet the requirements of biologists, a series of system design requirements covering node hardware design, sensor network software, protective enclosures, and system layout have been created. 43 nodes were installed on a tiny island off the coast of Maine in the summer of 2002 to relay valuable data live on the site. While researchers expect that certain difficulties would emerge in the application of WSN in the modern world, several challenges can only be found by practice. They offer a portfolio of four months of deployment experience on a remote island. To test device performance, they analyses environmental data and node health. The WSN's close integration with its climate offers environmental evidence at historically unimaginable densities. They illustrate that sensor knowledge is often helpful in forecasting device efficiency and network faults. They evaluate node and network architecture on the basis of more than 1 million data readings and build network reliability profiles and models of failure.

Robinson et al. (2019), In this article, they suggest a new Wireless Sensor Network (WSN) energy-conscious routing protocol focused on threshold rate and fuzzy logic to increase energy performance. The heads of the groups are picked on the basis of the WSN likelihood values for each node, which are derived from each node's residual energy. To measure the average strength of the whole network at the current level, the cumulative residual energy of the node is used. The nodes are more likely to have a greater probability of being chosen as the block head, which receives packets over a single hop link from the block member. Using blurry power of multi-hop coordination, the head of the block forwards the gathered data to the drain. Three parameters are used for fuzzy control: the duration of the tail of the node, the size of the node from the base station, and the residual power of the node. Data from tests suggests that by complementing certain methods, the proposed energy effective cluster routing protocol system (called MLSEEP) achieves stronger results than current protocols.

Venu & Rahman (2019), Without any center or administrative nodes, an ad hoc cell network briefly sets up the network. Generally speaking, to relay data or messages, AODV can find the fastest path from the foundation to the end point. An on-demand custom vector protocol (RPFAODV) focused on restricted flood prediction is included in their proposed solution. The objective of RPFAODV is on defining the endpoint node, predicting the path based on the power level of each node, the position of the end node through the route request packet, and the route answer packet messages. Once a path answer packet has been sent from an end node to a source node, it is now configured to transfer the data packet to the destination as a party. The unnecessary node crossing in this suggested protocol is constrained by the prediction of the network route. In the other transmitting field of the network, they forward the data or notification from the destination to the local coverage nodes. Better output outcomes compared to other traditional routing protocols. In this paper, in addition to the interactive AODV protocols, the RPFAODV protocol was analyzed and its individuality was measured with appreciation for the numerous movements centered on the speed of message transmission, the end-to - end latency, amount of dropped packets, and Network Simulator (NS2) throughput.

Narayana & Midhunchakkaravarthy (2020), The term "Mobile Ad Hoc Networks" refers to networks that do not need any kind of infrastructure and are mostly used to establish communication when a wired network fails. It is suggested in this article to use a Time Interval Based Blockchain Model (TIBBM) for security-related information collection, which may be used to identify rogue nodes in a mesh network. The suggested approach creates the Blockchain information structure, which is then used to identify rogue nodes at predetermined time intervals, as described above. A Network Block Monitoring Node (NBMN) is chosen following route selection in order to conduct a malicious node detection procedure. This node will monitor the blocks produced by the nodes in the routing table in order to identify malicious nodes. Finally, the NBMN node is able to determine the position of malicious nodes by using the Blocks that have been generated. The suggested model is compared to the conventional malicious node identification model, and the findings demonstrate that the new model outperforms the old model in terms of harmful node detection.

Gao et al. (2020), This paper presents an unsupervised learning-based method for detecting energy depriving malicious nodes in an energy harvesting cooperative wireless sensor network (EHC-WSN). A malicious energy depriving mode may falsibly show that it has little energy and, in this way, obtains energy from neighboring nodes, thus depriving them of energy. To detect these malicious nodes, we utilize a clustering method. In our method, each node first observes the energy of its neighboring nodes, then it utilizes this information to obtain data points for the clustering. After clusters are formed, each node judges on a cluster of data points from malicious nodes and makes a malicious node determination.

Jaint et al. (2019), Essentially, Wireless Sensor Networks (WSN) are collections of sensor nodes that are dispersed over a wide region in order to gather the information that is required. However, sensor nodes are also susceptible to assaults like as malware, hackers, defective hardware, and natural disasters, among other things. As a result, it is essential to defend a sensor node from an assault because if it is attacked, the information provided by the sensor may be inaccurate, resulting in incorrect data processing, which could result in unintended consequences. In this article, we present a machine learning-based method for detecting rogue nodes in a sensor network that has been randomly distributed. An application of the Support Vector Machine for time series prediction has been used to identify the malicious nodes based on the previous data that were collected by those particular nodes.

Zhang et al. (2018), With the advancement of Internet technology, social networking sites have risen to become significant applications in today's networked society. However, as a result of the fast rise in the number of users, the inflow of a range of false information, as well as the presence of malevolent users, has been brought to the forefront. As a result, it is necessary to develop a proper management system for user authentication in order to guarantee that social networks continue to operate normally. In wireless sensor networks, node trust assessment is an efficient way of dealing with common network assaults that may occur. It is suggested in this article that a new trust management system based on Dempster–Shafer evidence theory for malicious node identification be used to address the problems of quantification and uncertainty of trust. First and foremost, the trust degree may be calculated by taking into consideration the spatiotemporal correlation of the data gathered by sensor nodes in the surrounding region. Second, in accordance with the D–S theory, the trust model is created in order to count the number of interactions between trust, mistrust, and uncertainty, and to assess the direct trust value and indirect trust value as a result. Then, to compute the total trust in order to detect the malicious nodes, a flexible synthesis technique is used to do this. The simulation findings demonstrate that the suggested system has significant benefits over conventional approaches in terms of accuracy in the detection of malicious nodes and data fusion accuracy, as well as the potential to achieve high scalability.

Jamshidi et al. (2018), A Sybil attack, where a malicious node creates multiple fake or captured identities, is one of the most well-known attacks against wireless sensor networks (WSNs). This attack can leave devastating effects on operational and routing protocols, such as voting, data aggregation, resource allocation, and misbehavior detection. In this paper, a simple and precise algorithm for detecting Sybil attacks in mobile WSNs is proposed. Considering the rapid growth of Internet of Things (IoTs) devices and WSNs' popularity, the threat from this attack is serious.

Shakeel et al. (2021), presented a WSNs are often employed in a wide range of monitoring applications. Reducing network resource utilization is critical for programs that are often put in places that are difficult for people to access. Most WSN protocols have been developed to help expand the network's presence. The results from this research, which utilized a Hopfield neural network, are organized next to one other so as to facilitate comparison. This study also describes how to manage WSN collisions quickly and correctly. Future studies that include neural networks and a significant amount of fuzzy logic will help to avoid these problems in the future.

Kaur & Sharma (2020), presented a WSN technologies are highly approached, since they previously had to communicate with at least a few sensor nodes from several applications. Sensor node power consumption affects the WSN, since the application monitoring node depends on collected data from the sensor node. The amount of energy used to transfer packets throughout the whole network, the percentage of packets that get dropped along the way, the number of packets that get sent to the base station and cluster head are all considered factors. Dead nodes (which have a one-in-a-few (or more) chances of surviving each round) are also obtained via the simulation.

Rao et al. (2020), presented the intrusion detection technique that is presented in this study is an entirely new approach that takes into consideration network trust and sensor packet loss rate. The suggested approach finds rogue nodes by digging deep into packet loss. For packet loss rate assessment, two independent metrics such as buffer capacity metric and residual energy meter are used. Another thing the trust assessment takes into consideration is fundamental sensor-node communication. An experiment is performed using the suggested methodology and its effectiveness is gauged by FPR and MDR (MDR). The findings suggest that the recommended strategy has superior outcomes.

Lodhi & Sattar (2019), presented a WSNs, also known as wireless sensor networks (WSNs), consist of autonomous nodes located in discrete locations (often outdoors) and connected to sensors to sense and maintain physical and environmental conditions. In practice, however, these protocols slow down the cluster head and hence reduce the rate at which packets are processed. By using this statistic, they show how to identify the "optimal ability to control packet loss" and how to prolong the network lifespan. This measure gives an indication of the energy and memory state of nodes. The knapsack method is used to calculate the residual status of an intermediate node. NS2 conducts an evaluation of our suggested work, and the findings reveal that our protocol works better than previous protocols.

Jaradat et al (2019), presented an application for real-world deployment of the LEACH protocol is given in this research study, in which a simulation model is presented for use in evaluating the protocol's performance in a noisy WSN (wireless sensor network) environment. This model represents the noise level as the probability of packet receipt (pr). When the number of peers on the network is less than one, the network is regarded to be noise-free and all packets transmitted are received. The suggested simulation model was constructed using Python, a computer language that offers more support for simulation development. The homogeneous LEACH algorithm's performance was evaluated for multiple network metrics in the presence of varied noise levels. A noise-free, analytically determined energy model was developed.

Rahmadhani et al. (2018), presented a LEACH (Low Energy Adaptive Clustering Hierarchy) which is a wireless sensor network clustering routing system (WSN). The setup and steady state phases of the LEACH algorithm are separated. LEACH Routing has a significant packet loss on a busy network. They need a Delay Tolerant Network to tackle the issue (DTN). DTN is a sophisticated design that enables communication under difficult situations, such as a congested network. LEACH-WSN and LEACH-WSN over DTN show no significant differences in terms of energy consumption in two scenarios, but when they look at the lifespan of nodes, which is dependent on energy consumption, LEACH-WSN over DTN has an early death node. When the number of nodes grows or the network becomes congested, LEACH-WSN has a major advantage over DTN.

Mugheri et al. (2018), presented a WSN, security has always been a primary issue. WSN currently lacks a robust security solution for its operations because to limited resources and node size constraints. Some of the purposed security approaches for WSN are evaluated in this study for concerns that still remain in the purposed security techniques. Some of the documented or implemented security algorithms by researchers are being researched to do the analysis on security approaches, and the flaws with such algorithms are being identified. Following the study, it is evident that the majority of the algorithms being developed by academics for WSN must be constructed with WSN's resource constraints in mind.

Vhatkar et al. (2017), presented the wireless sensor network (WSN) has emerged as a popular kind of network, particularly in environments where human interaction is an issue. In a WSN, a group of sensors in a sensing environment work together to monitor and regulate the physical properties of an environment. WSN needs an energy efficient routing protocol to effectively complete the specified job while maintaining a longer network lifespan.

Tedeschi et al. (2017), presented a Node's misbehaving may cause packet losses. Malicious nodes and network assaults may both lead to packet losses. It is vital that a clear understanding of the reason be included into effective response methods in order to get the network up and running again. They validated their model using sensor data and discovered that our model accurately represents the packet loss causes. As a result, they were able to find the most precise and granular factors for packet loss.

Thrimoorthy et al. (2017), They must have a network connection in order to exchange data across several devices. The devices may be any electronic equipment that works with data transfer protocols, such as computers, laptops, smartphones, or sensors that are connected to a router through wireless or cable connections. Wired and wireless networks are both examples of network-networks. They study sensors as network devices in the article which has been provided. Whenever there is congestion, there are a host of unintended effects, such delayed decisions, packet loss, higher network overhead when retransmitting lost packets, and lower sensor life spans. In this research, a virtual model is offered that may aid in comprehending how data are exchanged through a network of sink nodes and sensors, as well as a mechanism for detecting and controlling congestion.

Khan et al. (2013), introduced the Low latency and consistent message transmission is a benefit of wireless sensor networks (WSNs) in mission-critical and delay-sensitive industrial applications. Reliable communication between the sink and the sensing nodes is vital in applications like gas leakage detection, monitoring of pressure, and control of industrial processes. Nodes are deployed densely in varied contexts with no specified network architecture in wireless sensor networks. Also, this article discusses three potential network topological configurations that might support mission-critical applications. They used three distinct topological designs known as Linear, Tier-1, and Split Tier-1 to analyses the performance of a wireless sensor network (WSN).

Liu et al. (2014), examined the delay performance in a wireless sensor network (WSN) using a cluster-tree topology in this research. Due to the close relationship between sensors and sinks, as well as the resource allocations of cluster heads, end-to-end latency might be greatly reliant on how widely distributed the sensors are in relation to the sinks (CHs). The results of this experiment help to establish the packet loss rate. After proposing a heuristic to jointly discover the timeline allocations of all the CHs in a WSN in order to achieve the minimal and balanced packet drop rate for traffic originating from different levels of the cluster tree, a proposed heuristic for a balance between latency and packet drop rate is then introduced. Simulation results are used to illustrate that the suggested CH timeframe allocation strategy is effective and also to validate the study. Accordingly, the system life sensor hub relies upon the battery life. For this situation, viable information driven WSN is a standard test as a unique test. Therefore, any improvement in these networks should focus on improving the energy consumption of the network. Unfortunately, malicious node can cause rapid eradication of energy during the attacker node. This is why the most important investigation work is to look for the fall energy analysis due to the worst node.

2.1 Research Gap

The review study of this WSN found that the detection of suspicious activities research has less for WSN infrastructure through some intelligent mechanism. The prior studies like flexible synthesis, Support Vector Machine usually use to detect the malicious nodes and attacks. The most of the venerable to attack situation supposed to be in the MANET as par the general findings of the reviews.

2.2 Problem Declaration

As considering the hues node implanted in the area, the detection of suspicious activities in WSN also going to very difficult.

CHAPTER 3

PROBLEM FORMULATION AND METHODOLOGY

3.1 How Packet Loss Occur In WNS

Packet Loss occurs if a packet is transmitted simultaneously by two or more nodes across a network. The packets transmitted must be rejected and then retransmitted, which increases the energy consumption and latency by retransmitting those packets. Attack Packet Loss is a type of DOS attachment that takes place in the Data Link Layer. Packet Loss occurs when a packet is transmitted simultaneously by two or more close stations. This can lead to the loss of the packet and to a network loss. These protocols may efficiently reduce Packet loss. However, due to hidden terminal problems and Packet Loss, all Packet loss intrinsically cannot be eliminated when several nodes at the same time sense medium free. Moreover, WSNs are severely affected by packet Loss. The loss of critical control data from base stations can result in Packet loss and applications may fail.

3.2 Role of Neural Network in WSN

A one-to-many communication, namely broadcasting, is the most fundamental way of exchanging information in both types of networks. A firing neuron in a biological neural network sends a potential for action for all neurons connected to it through synapses, each of which could impose different delays and amplifications on the signal transmitted. Likewise, a communications node in the sensor network transmits its signal throughout its transmission range to all nodes. The computation of action capabilities suggested by Hopfield et al., who discovered that analogue data can be encoded into action potential firing durations, and that the timing of action capabilities may be utilized to conduct a support vector algorithm, is another example of such a paradigm. There was no specific requirement for the ability to perform broadcast-based communication. Therefore, the earliest neuron firing naturally occurs when the property variable of the neuron is compared to the minimum value. Instead of overlapping Hopfield's approach, it is thus essential to choose a winner with the desired optimality.

3.3 Feed Forward Back Propagation

In order to simulate how human brain information processes, ANNs are biologically based computer program. It is an extremely potent approach to build a complex, nonlinear link between a set of data inputs and outputs. The computing power is derived from a network connection. The inputs, simulation functions, transfer functions and output are weighted in every neuron. The weighted sum of the inputs represents the neuronal activation function. A transmission function that introduces non-linearity and produces output transmits the activation signal. The interunit connections are optimized during the training process. Once the network is trained, the test output will be calculated with new unseen input information. In the neural network there are many back propagation algorithms used, but mostly the back propagation feedback neural network (FBNN).

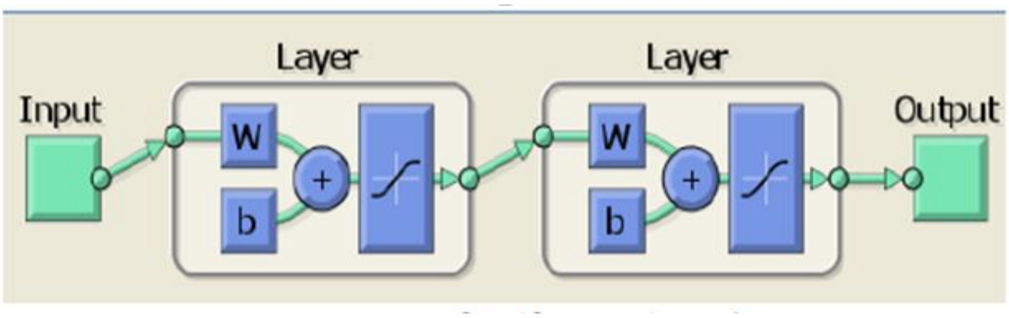


Figure 3. 1 Simple two-layer feed forward back propagation neural network

In general, there are three layers of a two-layer simple feed-forward-back nets: an input layer, a covered layer and the output layer.

3.4 Hopfield Neural Network

The neural network is a kind of computer network. In computing, Hopfield is a basic artificial network that may be used to store memories or patterns. The Hopfield neural network model is a binary unit network with symmetrical unit weights that is completely linked with the rest of the network. Based on that function, the neural state, weight, and bias value derived from the problem data are calculated. The neuron update rule is based on the function of energy and is defined as follows:

3.4.1 Hopfield network applied to the single sensor node

Poor channel conditions are a frequent source of problems for wireless communication. Algorithms or other methods, such as retransmission, must be used to deal with incorrect or even missing data packets. It is in this environment that HN demonstrates promising characteristics like as associative memory, resilience, and the capacity to rectify mistakes. In the situation of missing data, the HN executes pattern rectification. The HN is a single layer feedback network that is completely interconnected and does not have any direct feedback connections, which implies that each neuron is not directly connected to itself, as is the case with other feedback networks. It also has symmetrical weights (bidirectional), which means that the weights between all single neurons are the same in both directions. In the example of Figure 3.4, the HN shows the sensor input pattern that is read by three sensors and shown by the HN.

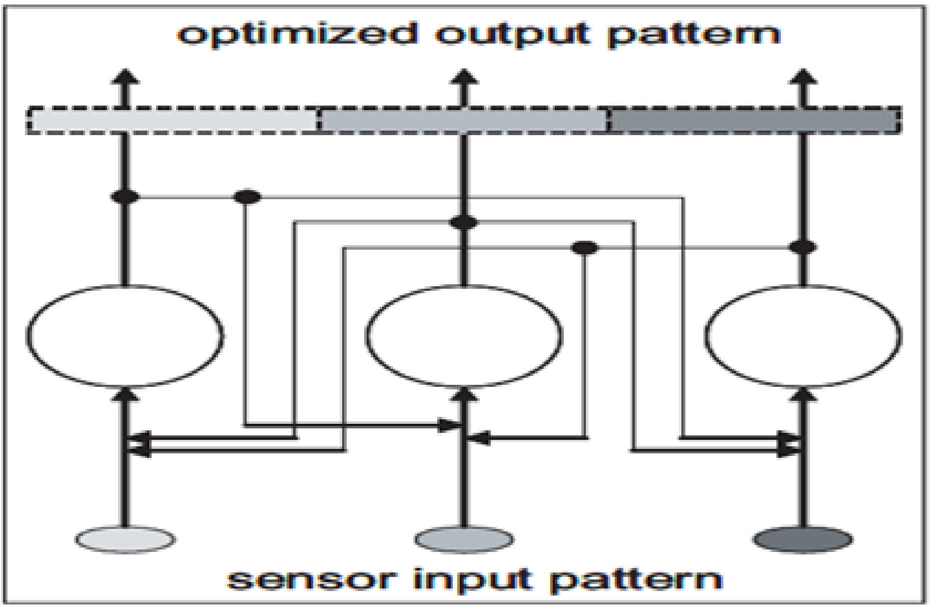


Figure 3. 2 The Hopfield System & network

3.5 Packet Loss Avoidance Using HNN

Poor channel conditions are a frequent source of problems for wireless communication. Algorithms or other methods, such as retransmission, must be used to deal with incorrect or even missing data packets. Associative memory, resilience, and the capacity to rectify mistakes are all promising characteristics of the HNN in this context. HNN makes use of principles such as associative memory, design completeness, and error correction. Here, associative memory refers to the fact that a pattern is preserved across the whole network rather than being kept in a single neuron. When an incomplete or corrupted pattern is used to reconstruct the full pattern/network, the correlations may be used to finish the pattern/network throughout the entire network. The HN is a single layer feedback network that is completely interconnected and does not have any direct feedback connections, which implies that each neuron is not directly connected to itself, as is the case with other feedback networks.

3.6 Procedure

Create a network of 20 nodes that are organized in a circular pattern.
Choose the source and destination nodes, as well as the sensor node, from the list of nodes.

Despite the fact that (data is not received by destination)

repeat

In the event that (sensor node detect packet loss)

Then

Use a pattern recognition neural network to move the node at which packet loss is observed to a different location on the network.

And then restart the transmission from the source node.

Else

Transmit data from one node to another via a network protocol.

Estimate the PDR, E2Edelay and Throughput
Then
Repeat Test

```
Draw the Test Results in Excel
Construct the Trend Line
End if
End while
Exit
```

3.6.1 Execution Process

Present Investigation is to find the Packet Drop During Transmission of packets in WSN as the PDR, E2Edelay and Throughput. We try to enhance the Packet Drop During Transmission through proposed machine learning (Neural network) for this investigation. Because it used a used a memory frame to record each communication which gives better accuracy to detect the any malicious activities of WSN. The overall execution step to perform the proposed work as illustrated in below as flow diagram.

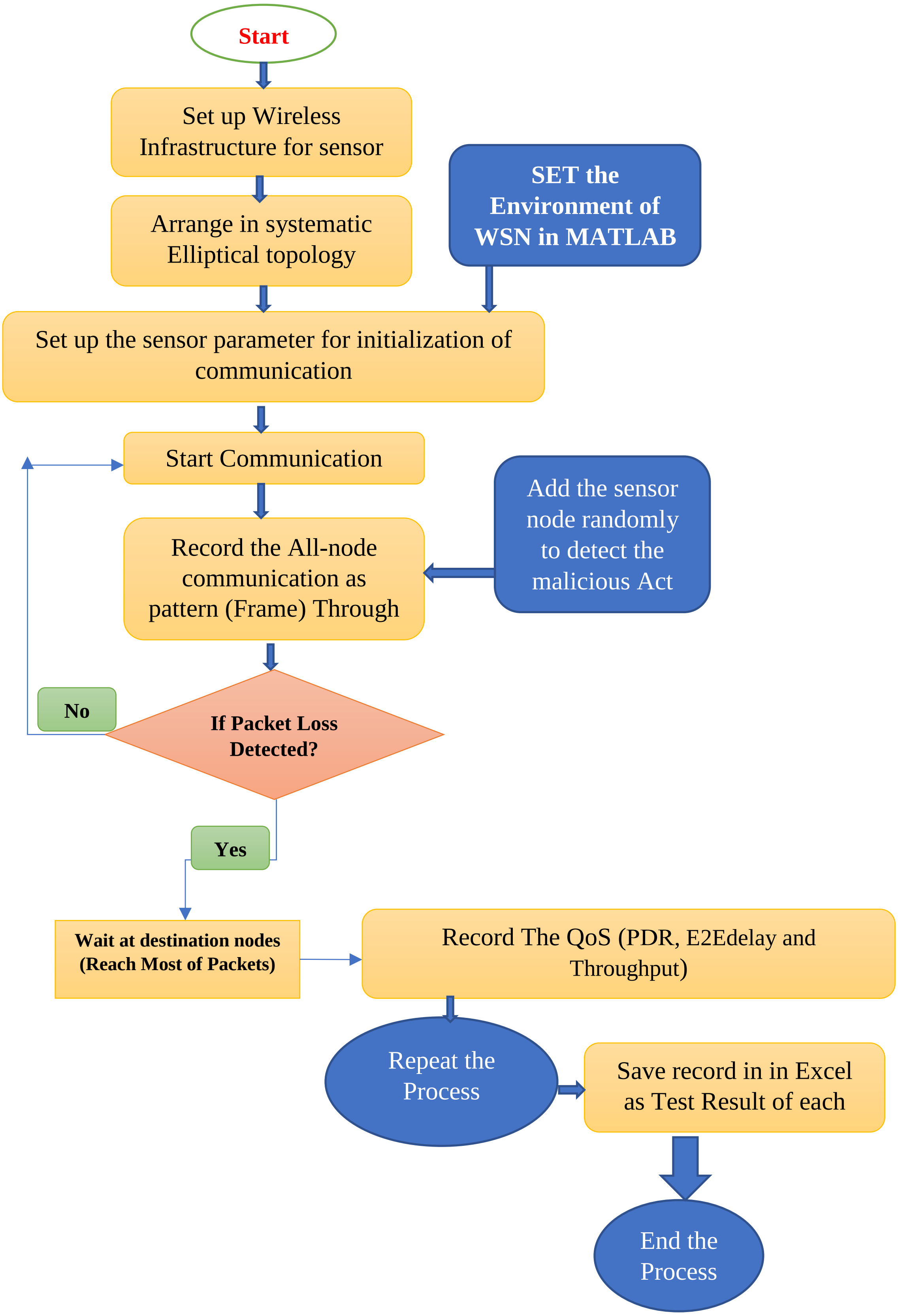

Start
Set up Wireless Infrastructure for sensor
SET the Environment of WSN in MATLAB
Arrange in systematic Elliptical topology
Set up the sensor parameter for initialization of communication
Start Communication
Add the sensor node randomly to detect the malicious Act
Record the All-node communication as pattern (Frame) Through
No
If Packet Loss Detected?
Yes
Wait at destination nodes (Reach Most of Packets)
Record The QoS (PDR, E2Edelay and Throughput)
Repeat the Process
Save record in in Excel as Test Result of each
End the Process

Figure 3. 3 Execution Process

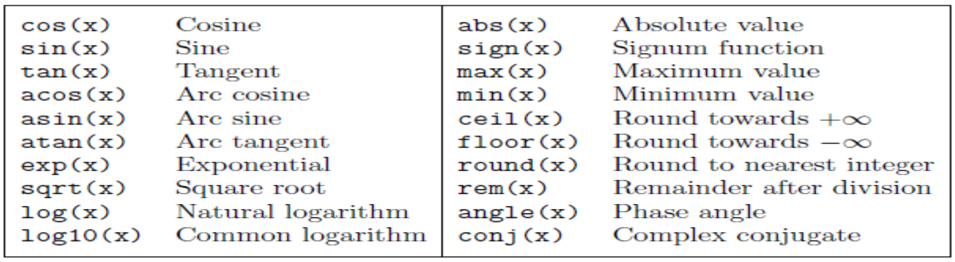
CHAPTER 4

SIMULATION & RESULT

These practical solutions may use machine learning to make more efficient use of network resources and increase the lifetime of your network. To summarize, this research presents a comprehensive literature assessment of machine learning approaches from 2002 to 2018, which are utilized to deal with commonplace challenges in wireless sensor networks (WSNs). The pros and cons of each algorithm are examined to decide which would be most suitable for the task at hand. This serves as a resource for WSN designers, who may use it to assist create the ideal machine learning solution for their application's unique issues. It is clear that in the early stages of packet sending, a certain number of packets were transmitted due to the fact that only a small percentage of packets were lost. Based on these findings, in the digital data, it is evident that the suggested task would be successful. Compared to the same time period a year before, it has almost doubled. Since it is now known that when neural networks employ high iterating values, they perform significantly, it follows that when neural networks use high iterating values, they minimize packet loss owing to highly active pattern recognition algorithms, which also corrects packet loss issues. The improvements in end-to-end latency and throughput are secondary to this change. Since the suggested system performs a good job of collision detection during transmission and avoidance, then the suggested system performs an excellent job of collision detection during transmission.

For technical calculations, MATLAB offers several predefined mathematical functions, including a huge number of mathematical functions.

Table 4. 1 lists some commonly used functions, where variables x and y can be numbers, vectors, or matrices. Elementary Functions used in MATLAB



`cos(x)`	Cosine	`abs(x)`	Absolute value
`sin(x)`	Sine	`sign(x)`	Signum function
`tan(x)`	Tangent	`max(x)`	Maximum value
`acos(x)`	Arc cosine	`min(x)`	Minimum value
`asin(x)`	Arc sine	`ceil(x)`	Round towards $+\infty$
`atan(x)`	Arc tangent	`floor(x)`	Round towards $-\infty$
`exp(x)`	Exponential	`round(x)`	Round to nearest integer
`sqrt(x)`	Square root	`rem(x)`	Remainder after division
`log(x)`	Natural logarithm	`angle(x)`	Phase angle
`log10(x)`	Common logarithm	`conj(x)`	Complex conjugate

The performance of each classifier in terms of packet delivery ratio, end2end delay, and throughput was compared. For better understanding of results comparison, we introduce these criteria.

a) **Packet delivery ratio**- It reflects the ratio of the total number of published messages that each subscriber node collects to the total number of published messages that all publisher nodes produce for the subscriber node events.

It can be calculated by the following formula:

PDR= ((total packets-loss)/total packets)

b) **End2End Delay**- The delay of a packet in a network is the time it takes the packet to reach the destination after it leaves the source.

c) **Throughput** – The throughput of a channel is defined as the number of packets that travel through it in a given amount of time. With growing node density, this performance measure displays the total number of packets that have been successfully transported from the source node to the destination node, and it is expected to increase over time.

According to the formula, the number of samples produced by the network in response to an arbitrary query is equal to the number of sensors (k) that are present and active at the time the query is received.

It can be calculated by the following formula:

Throughput=total packets/End2EndDelay

4.1 Proposed Methodology

The machine learning like Neural network must has very good tools to monitoring the WSN. The sudden various of change of activities in pattern of the network could be monitored through the proposed neural network. The delay and the loss of communication packet in the proposed network is the key findings of this research.

This thesis has been integrated with modified version of neural network that has param value of 5000 round of calculation that earlier has only capability of 1000 round of test value. The parameter has been earlier and the shaper has been changed to elliptical that earlier was circular.
The various initial parameters have been as below.

- nr_fr=13; Frame that has been assign for catching memory allocation.
- Total packets=0; Initialize the value of packets.
- Packet Trans=15; Initialize the value of packets transmitted.
- Inienr=100; Initialize the value of initial energy provided to each node.
- Ec=0.55; Energy count for each utilization of communication.
- drop=0.20; Probability of drop of node to dead node.
- loss=0; Initialize the value of lass at initial stage.
- Delay=0; Initialize the value of delay.
- trainParam.epochs = 5000; main code for neural network that has been.
  increased to the 2000 which is quite good for testing the proposed scenario.

The parameter has been framed in MATLAB code and run the simulation several times and estimation of the PDF, E2E delay and throughput has been generated on the command prompt of the MATLAB. This could also be calculated with the MATLAB Code. But this needs huge time calculation and self-insertion of the test condition. The outcome might vary but the essence of the result will remain same. The simulation by the constructed GUI as follows.

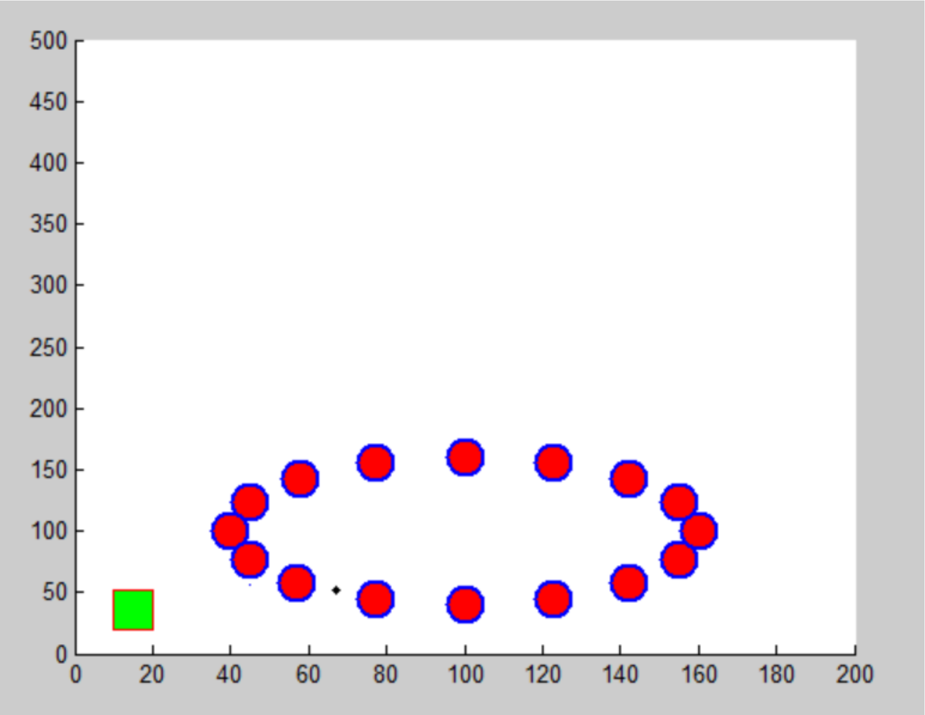
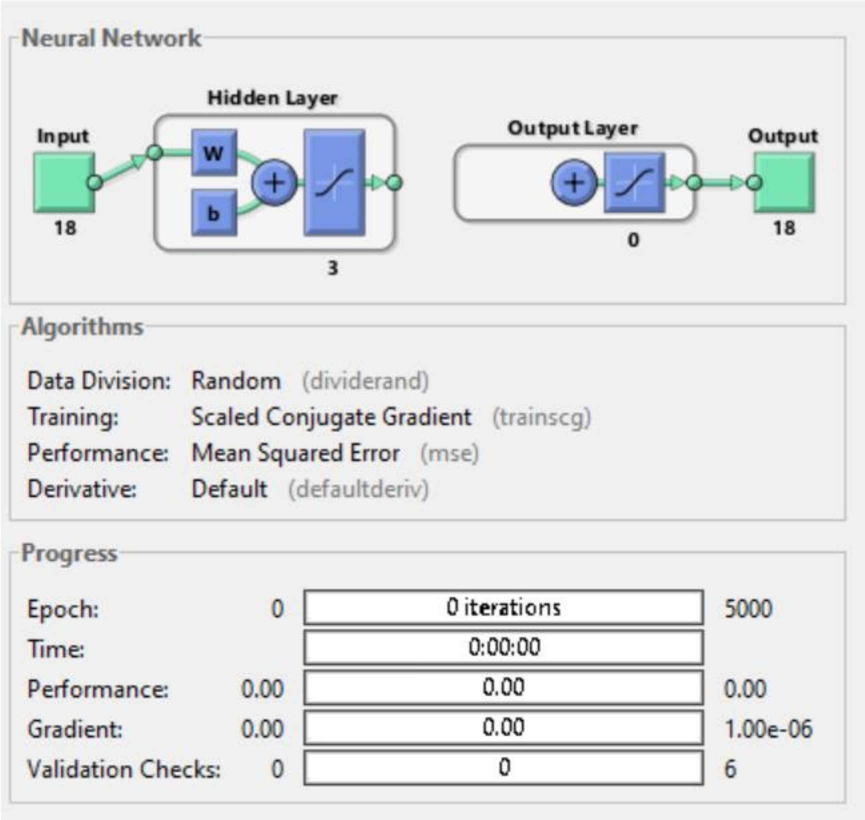


Figure 4. 1 Layout for WSN – Hopfield

This is the GUI constructed in MTALAB-2013. As we have a elliptical topology set up of nodes along with two sink node which acts as base station.



Algorithms

```
Data Division:  Random  (dividerand)
Training:       Scaled Conjugate Gradient  (trainscg)
Performance:    Mean Squared Error  (mse)
Derivative:     Default  (defaultderiv)
```

Progress

```
Epoch:              0     0 iterations     5000
Time:                     0:00:00
Performance:     0.00     0.00             0.00
Gradient:        0.00     0.00             1.00e-06
Validation Checks:  0     0                6
```

Figure 4. 2 Status of neural network (Hopfield Neural Network)

The above is the neural network which apply over the WSN nodes and network parameters. Through which the packet status could be evaluated.

4.2 Result -FFBP

Table 4. 2 FFBP

S. No.	Packet transmitted	Packet drop	PDR	e2edelay	Throughput
1.	170	9.0000	0.9471	2.1262	79.9535
2.	170	13.5000	0.9206	2.0819	81.6566
3.	210	13.5000	0.9357	2.0811	100.9061
4.	190	22.5000	0.8816	2.1306	89.1758
5.	170	15.7500	0.9074	2.0603	82.5139
6.	200	11.2500	0.9437	2.0513	97.5009
7.	210	13.5000	0.9357	2.0449	102.6938
8.	190	18.0000	0.9053	2.0616	92.1624
9.	200	11.2500	0.9437	2.0422	97.9358
10.	180	6.7500	0.9625	2.0621	87.2907
11	170	9.0000	0.9471	2.0491	82.9641
12	210	13.5000	0.9357	2.0811	92.1624
13	210	13.5000	0.9357	2.0489	100.6938
14	190	9.0000	0.9040	2.0626	91.1624
15	170	9.0000	0.9471	2.1262	79.9535
16	170	13.5000	0.9206	2.0812	81.6576
17	210	13.5000	0.9367	2.0811	100.9261
18	200	11.2500	0.9357	2.0449	102.6938
19	190	18.0000	0.9053	2.0616	92.1624
20	200	11.2500	1	2.0422	97.9358

4.3 Result – HOPFIELD

Table 4. 3 HOPFIELD

S. No.	Packet Transmitted	Packet Drop	PDR	e2edelay	throughput
1	180	4.5	0.975	1.0414	168.523142
2	170	3	0.9824	1.0414	160.361052
3	210	16.5	0.9214	1.0618	182.23771
4	200	12	0.94	1.1042	170.259011
5	190	12	0.9368	1.1906	149.504452
6	190	12	0.9368	1.1871	149.945245
7	190	6	0.9684	1.0417	176.634348
8	180	10.5	0.9417	1.0625	159.529412
9	180	4.5	0.975	1.0411	168.571703
10	190	12	0.9368	1.1421	155.853253
11	190	6.75	0.9625	1.1806	155.217686
12	210	10	0.9471	1.1071	180.652154
13	210	13.5	0.9357	1.0317	190.462344
14	220	13.5	0.9357	1.0125	203.950617
15	190	11	0.904	1.0311	173.601009
16	170	11	0.9471	1.1221	141.698601
17	180	11.5	0.9206	1.1071	152.19944
18	210	15.5	0.9367	1.0317	188.523796
19	170	6	0.9647	1.224	133.986928
20	170	6	0.9647	1.0311	159.053438

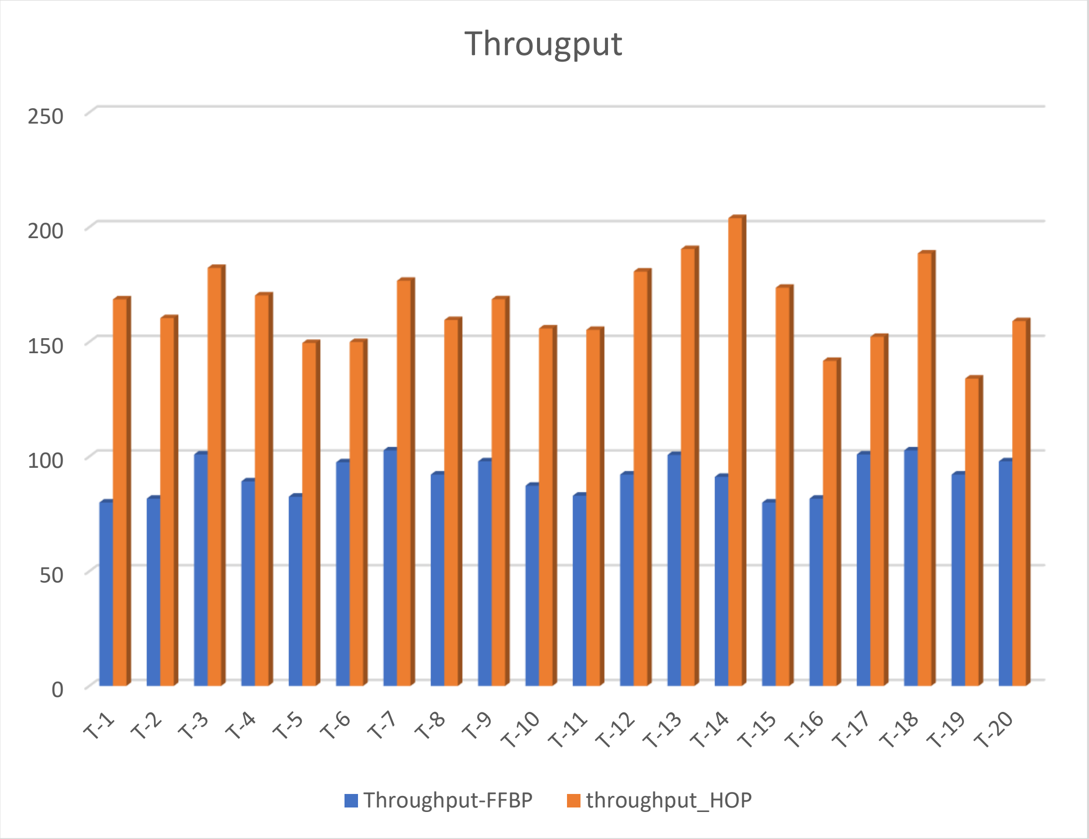


Figure 4. 3 comparison between throughput of FFBP and HOP

Table 4. 4 Throughput of FFBP and HOP

S. No.	Throughput-FFBP	Throughput-HOP
T-1	79.9535	168.523
T-2	81.6566	160.361
T-3	100.906	182.238
T-4	89.1758	170.259
T-5	82.5139	149.504
T-6	97.5009	149.945
T-7	102.694	176.634
T-8	92.1624	159.529
T-9	97.9358	168.572
T-10	87.2907	155.853
T-11	82.9641	155.218

T-12	92.1624	180.652
T-13	100.694	190.462
T-14	91.1624	203.951
T-15	79.9535	173.601
T-16	81.6576	141.699
T-17	100.926	152.199
T-18	102.694	188.524
T-19	92.1624	133.987
T-20	97.9358	159.053
Avg.	**91.70507**	**166.0383**

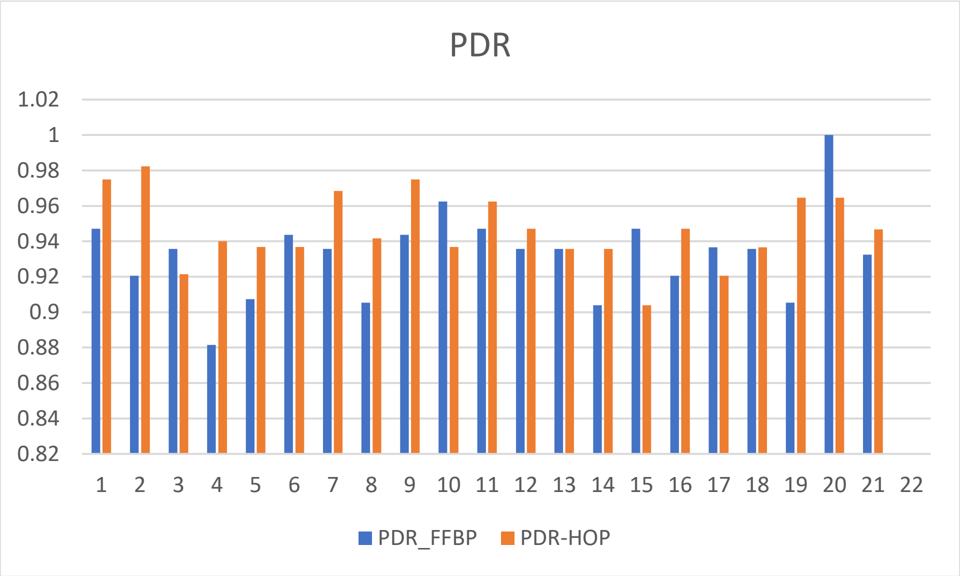


Figure 4. 4 comparison between PDR of FFBP and HOP

Table 4. 5 comparison between PDR of FFBP and HOP

S. No.	**PDR_FFBP**	**PDR-HOP**
T-1	0.9471	0.975
T-2	0.9206	0.9824
T-3	0.9357	0.9214

T-4	0.8816	0.94
T-5	0.9074	0.9368
T-6	0.9437	0.9368
T-7	0.9357	0.9684
T-8	0.9053	0.9417
T-9	0.9437	0.975
T-10	0.9625	0.9368
T-11	0.9471	0.9625
T-12	0.9357	0.9471
T-13	0.9357	0.9357
T-14	0.904	0.9357
T-15	0.9471	0.904
T-16	0.9206	0.9471
T-17	0.9367	0.9206
T-18	0.9357	0.9367
T-19	0.9053	0.9647
T-20	1	0.9647
Avg.	0.93256	0.946655

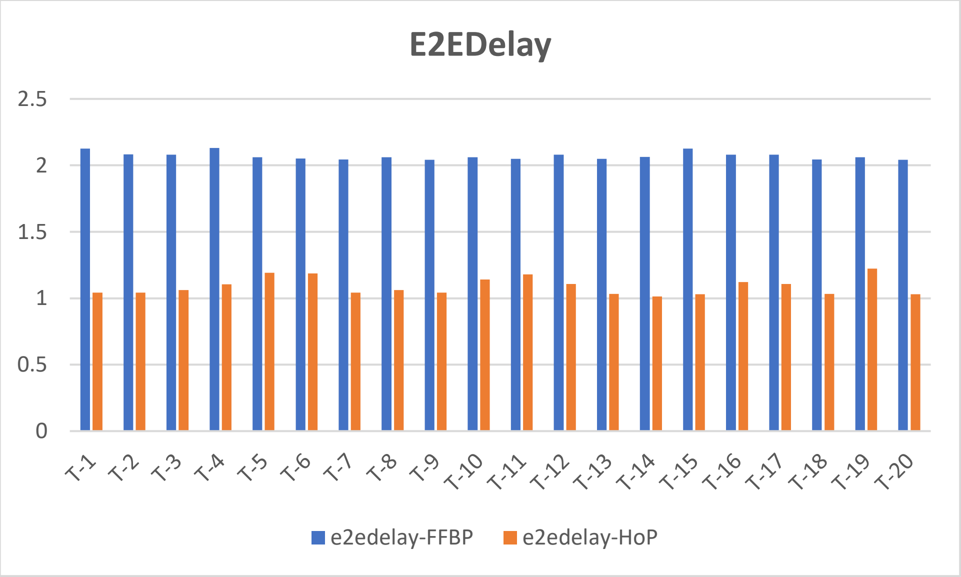


Figure 4. 5 comparison between e2e delay of FFBP and HOP

Table 4. 6 comparison between e2e delay of FFBP and HOP

S. No.	**e2edelay-FFBP**	**e2edelay-HoP**
T-1	2.1262	1.0414
T-2	2.0819	1.0414
T-3	2.0811	1.0618
T-4	2.1306	1.1042
T-5	2.0603	1.1906
T-6	2.0513	1.1871
T-7	2.0449	1.0417
T-8	2.0616	1.0625
T-9	2.0422	1.0411
T-10	2.0621	1.1421
T-11	2.0491	1.1806
T-12	2.0811	1.1071
T-13	2.0489	1.0317
T-14	2.0626	1.0125
T-15	2.1262	1.0311
T-16	2.0812	1.1221
T-17	2.0811	1.1071
T-18	2.0449	1.0317
T-19	2.0616	1.224
T-20	2.0422	1.0311
Avg.	2.071055	1.089645

4.3 Compare Results

Table 4. 7 Compare Results

	Existing Model (FFBP)	**Proposed Model (NN)**
Platform	MATLAB	MATLAB + Trend Analysis
Base Research	WSN	WSN
Research Area	Conventional	HNN (Part of ML)
Technique	Feed Forward Back Propagation	Neural Network
Throughput	42.93	75.911
PDR	27	25
Model	WSN Node	WSN Node
Real Time	Yes	Yes

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

The primary characteristics of WSNs are that they are one-of-a-kind in terms of network form flexibility and sensor mobility. The throughput, latency, and packet transmission rate of a network are all discussed in this article. A jump field neural network is used to transmit packets during the packet transmission process. Packet transfer rates and throughput improve, but end-to-end delays decrease in this environment. Also included are descriptions of approaches that may be used to successfully recover from wireless sensor network congestion. Machine learning applications will be able to be used in the future to prevent packet loss by iterating on the iterating began. Embedded network applications are discussed in general terms in this article, which then goes on to analyses the requirements found by the study. In addition, we discussed the in-network processing methods that were selected and compared the Hopfield neural network to the back propagation network, emphasizing the similarities in their physical appearance. It is possible to expand the sensor network. In the neural network that follows, a new context is introduced. The description of the feasibility of neural networks in a sensor network setting, as well as an assessment of the early findings obtained by our test implementation, are both very important in this context.

5.1 Future Scope

It is possible to test various topologies with a greater number of sensor nodes for the purposes of experimentation and simulation. The future of this experiment will also benefit the VANET scenario, which is being intentionally enhanced via the use of 5G technology. When using 5G communication, you get a platform for the WSN sensor and its extremely reliant usage in different data collecting platforms, thanks to the 5G communication platform.

Reference

1. Narayana, V. L., & Midhunchakkaravarthy, D. (2020, July). A Time Interval based Blockchain Model for Detection of Malicious Nodes in MANET Using Network Block Monitoring Node. In *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 852-857). IEEE.
2. Gao, B., Amagata, D., Maekawa, T., & Hara, T. (2020). Detecting Energy Depriving Malicious Nodes by Unsupervised Learning in Energy Harvesting Cooperative Wireless Sensor Networks. *Journal of Information Processing*, *28*, 689-698.
3. Jaint, B., Indu, S., Pandey, N., & Pahwa, K. (2019, October). Malicious Node Detection in Wireless Sensor Networks Using Support Vector Machine. In *2019 3rd International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE)* (pp. 247-252). IEEE.
4. Zhang, W., Zhu, S., Tang, J., & Xiong, N. (2018). A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks. *The Journal of Supercomputing*, *74*(4), 1779-1801.
5. Jamshidi, M., Darwesh, A. M., Lorenc, A., Ranjbari, M., & Meybodi, M. R. (2018). A precise algorithm for detecting malicious sybil nodes in mobile wireless sensor networks. *IEIE Transactions on Smart Processing & Computing*, *7*(6), 457-466.
6. Shakeel, N., Haroon, M., & Ahmad, F. (2021). A Study of WSN and Analysis of Packet Drop During Transmission. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST).*
7. Kaur, K., & Sharma, E. S. (2020). Analysis Grid Based DEEC Protocol with Priority Queue for Increasing Lifetime Of WSN. *IJRAR-International Journal of Research and Analytical Reviews (IJRAR)*, *7*(2), 699-703.
8. Rao, A. N., Naik, B. R., Devi, L. N., & Subbareddy, K. V. (2020, September). Trust and Packet Loss Aware Routing (TPLAR) for Intrusion Detection in WSNs. In *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 386-391). IEEE.

9. Lodhi, A. K., & Sattar, S. A. (2019). Cluster Head Selection by Optimized Ability to Restrict Packet Drop in Wireless Sensor Networks. In *Soft Computing in Data Analytics* (pp. 453-461). Springer, Singapore.
10. Jaradat, Y., Masoud, M., Jannoud, I., Abu-Sharar, T., & Zerek, A. (2019, March). Performance analysis of homogeneous LEACH protocol in realistic noisy WSN. In *2019 19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)* (pp. 590-594). IEEE.
11. Rahmadhani, M. A., Yovita, L. V., & Mayasari, R. (2018, July). Energy consumption and packet loss analysis of LEACH routing protocol on WSN over DTN. In *2018 4th International Conference on Wireless and Telematics (ICWT)* (pp. 1-5). IEEE.
12. Mugheri, A. A., Siddiqui, M. A., & Khoso, M. (2018). Analysis on Security Methods of Wireless Sensor Network (WSN). *Sukkur IBA Journal of Computing and Mathematical Sciences*, *2*(1), 52-60.
13. Vhatkar, S., Shaikh, S., & Atique, M. (2017, February). Performance analysis of equalized and double cluster head selection method in wireless sensor network. In *2017 Fourteenth International Conference on Wireless and Optical Communications Networks (WOCN)* (pp. 1-5). IEEE.
14. Tedeschi, A., Midi, D., Benedetto, F., & Bertino, E. (2017). Statistically-enhancing the diagnosis of packet losses in WSNs. *International Journal of Mobile Network Design and Innovation*, *7*(1), 3-14.
15. Thrimoorthy, N., Anuradha, T., & Kumar, A. (2017, September). A virtual model to analyze congestion in a wireless sensor network (WSN). In *2017 International Conference on Advances in Electrical Technology for Green Energy (ICAETGT)* (pp. 28-32). IEEE.
16. Khan, M. F., Felemban, E. A., Qaisar, S., & Ali, S. (2013, December). Performance analysis on packet delivery ratio and end-to-end delay of different network topologies in wireless sensor networks (WSNs). In *2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks* (pp. 324-329). IEEE.
17. Liu, W., Zhao, D., & Zhu, G. (2014). End-to-end delay and packet drop rate performance for a wireless sensor network with a cluster-tree topology. *Wireless Communications and Mobile Computing, 14*(7), 729-744.

PUBLICATIONS

" A STUDY OF WSN AND ANALYSIS OF PACKET DROP DURING TRANSMISSION "

is visible on Google Scholar-

https://scholar.google.co.in/scholar?q=A+Study+of+WSN+and+Analysis+of+Packet+Drop+During+Transmission&hl=en&as_sdt=0&as_vis=1&oi=scholart

Publishing link: https://ijircst.org/view_abstract.php?title=A-Study-of-WSN-and-Analysis-of-Packet-Drop-During-Transmission-&year=2021&vol=9&primary=QVJULTU3MQ==

or

https://www.ijircst.org/current_issue.php

WSN and Analysis of Packet Drop During Transmission

Nagma Shakeel[1], Mohd Haroon[2], and Faiyaz Ahmad

[1,4] M.Tech Research Scholar, CSE, Integral University, Lucknow, India
[2] Associate Professor Dept of CSE, Integral University, Lucknow, India
[3] Assistant Professor Dept of CSE, Integral University, Lucknow, India

Correspondence should be addressed to First Author Nagma Shakeel; nagmashakil5@gmail.com

ABSTRACT-WSN is a low-power system and are often used in numerous monitoring uses, such as healthcare, environmental, and systemic health surveillance, in addition to military surveillance. It is important to reduce network resource usage since many of these applications need to be installed in locations that are virtually inaccessible to humans. Many protocols for WSN to extend the presence of the network have been established to solve this problem. In the energy efficiency of WSN networks, routing protocols play an important role since they help minimize power usage and response time and provide sensor networks with high data density and service quality. This study also employed a Hopfield neural network and the findings from this study are presented next to each other to enable comparison. This paper also discusses how to easily and accurately capture and handle WSN collisions. Future experiments that require the usage of neural networks and so many fuzzy structures will be able to prevent a crash in these respects.

KEYWORDS- WSN-wireless sensor networks, PDT-packet delivery ratio, TP-throughput, e2e-delay

I. INTRODUCTION

Information is known as process data, information means some meaningful content, in wireless sensor computing, the information will propagate from one node to another through communication media and the various application protocol [1]. One characteristic of WSN is the ability to communicate through the wireless communication channel and sensor nodes in the real world for detecting and manipulating the specific entity. Any or more of these nodes must work together to achieve their goals. the nodes are linked with one-to-one and one-one employing wireless connection an underpowered wireless sensor network (WSN) can connect and function together to achieve a shared objective. They can function in highly dynamic settings, such as combat and surveillance environments. Since they operate on their own, WSNs are seldom unattended, several novel attacks are feasible. Recently, owing to their large acceptance in both military and civilian contexts, WSNs have gained a lot of coverage. WSN are widely used in covert and often adversarial locations such as the military and the domestic intelligence services. Thus, authentication protocols that accomplish the overall goals of congeniality, data privacy, nonrepudiation, and trustworthiness are critical to maintaining the integrity of the network. These days, the world's technology is going to base on the artificial intelligence technique, several artificial intelligence devices and protocols are used for various purposes.in wireless sensor nodes, artificial intelligence agents and protocols are playing a significant role [2].

A. Sensor nodes

The sensor nodes would be on the network handling the tasks. Although Task Manager measurements and queries could be taking place, the sensor nodes may send data based on these algorithms. Computations can be made on a node, depending on the device requirements If the model has been built, it may either transfer the data to the other nodes or give it to the Task Manager as is. In sensor nodes, the sensor may be either a source or a relay: The root is a means of figuring out and obtaining what is wanted. The world then is the source. Meanwhile, a sink or actuator is a device that is involved in receiving data from a sensor.

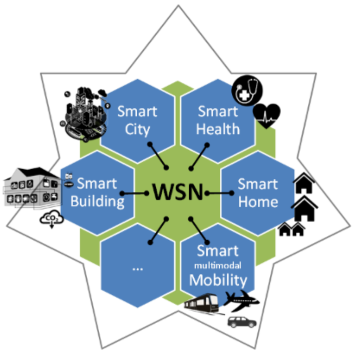


Fig 1: Illustration of sensor network and peripherals [15]

B. System Components and Operations in a Wireless Sensor Network

i. Communication Architecture

This section focuses on the sensor infrastructure. The sensors in the nodes' components and sub-of-world will be tested. We begin with a brief architectural and data-processing overview of the wireless sensor network before moving on to the protocols and systems that are employed in building a sensor network. to consider the total amount of power and hardware/software savings is crucial One of the aims of this study is to collect data on sensor nodes and to suggest hardware for their usage. More specific guidance may be obtained by referring to the equipment in depth.

ii. Sensor Node in communication architecture

In the first instance, a sensor is a low-power wireless device that is used in communication. A sensor node will usually act as a data processor, data repository, and communicator all at the same time. The standard sensor node contains the controller, memory, sensors, communication system, and power supply in this list (see Figure 2). The task of a controller is to perform is to process all the pertinent data, able to implement arbitrary algorithms. Data and program memory are the functions in memory. Input sensors and output actuators are the methods of communication with the environment. Any or all of these devices enable one to monitor or regulate environmental parameters. The unit interacts using radio waves. Lastly, the power supply is required to sustain the electronic components. One of the maximum significant architecture factors in WSN is power efficiency Thus, these entangled elements need to make the most of the minimum number of resources with the will to work.

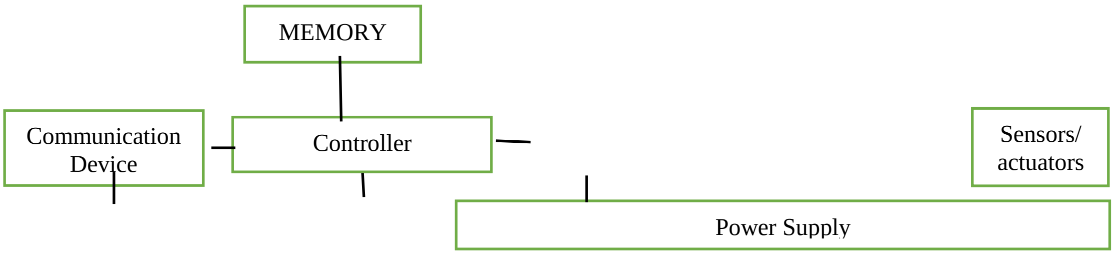


Fig 2: Overview of sensor node hardware component. [14]

II. BACKGROUND

Each responsive node senses an occurrence in a densely distributed sensor network and broadcasts it via multi-hop connexions to a particular party. additional data transmission and control packets are needed for sensor nodes installed near the basin node and are therefore subject to much higher energy depletion rates and therefore have much less expected network existence. in the paper, in the presence of the issue of power holes in the wireless sensor network, they addressed the performance of ad-hoc on-demand distance vector, dynamic state routing, and Temporally Ordered Routing Algorithm protocols. for each protocol, productivity, average power usage, and end-to-end latency, work performance, packet transmission rate, packet drop rate, active nodes, and routing expenses under various node densities were demonstrated. to mitigate this problem, the effectiveness of some of the prevalent approaches was applied and simulation conclusions were used to authenticate the study. compared with ad-hoc on-demand distance vector and Temporally Ordered Routing Algorithm, the number of active nodes in the dynamic state routing protocol is larger [3].

In recent years, because of the heavy burden of transmitting data to sensor nodes near the basin, WSN has faced the overall energy issue as the most significant problem. The Mobile Sink (MS) method is the best-proven alternative defined by the new existing approaches to the entire energy crisis. Allowing MS to visit each node to collect data, though, results in high data latency, which might not be possible in applications that are lag-sensitive. In this article, restricted mobile pelvic activity is also regarded, since MS ends at an imperfect number of sites listed as residence sites and all nodes publish their data at neighboring residence sites. Therefore, the suggested protocol range parameter is used in this article to preserve network coverage even though certain nodes are down. The suggested routing algorithm, focused on the residency positions, guarantees that all data in the cluster is propagated to the MS following the minimum hop route to minimize the gap in the transmission of data. About dissimilar constraints such as network life, coverage rate, energy efficiency, packet transmission rate, end-to-end delay, etc., the experimental findings reveal the efficacy of the proposed protocol over several modern protocols [4].

The growing need for different facets of the usage of wireless sensor applications renders service quality one of the maximum critical problems of wireless sensor applications. It is very difficult to maintain the standard of operation in wireless sensor (WSN) since the tools accessible to the numerous sensors and applications running on those networks have multiple limitations in terms of design and specifications. QoS has historically concentrated on the level of the network, paying attention to metrics like latency, efficiency, and volatility. The decentralized and complex topology of WSN has several essential criteria, including reducing power usage and extending the network's existence. The simulation results include overall network output that, along with a variety of dead nodes, total power consumption, community header settings, and performance, depends primarily on some factors [5].

There are several nodes in WSN whose primary functions are to track and manage ecosystems. Additionally, depending on network use, the sensor nodes are spread. The power usage of the sensor nodes one of the principal problems of this type of network. Nodes close to the basin serve as a data transfer interface in fixed basin networks for other nodes to sink. Also, the pelvic motion orientation route for the transmission of CH data is observed by the Hopfield neural network. Also, detailed simulations conducted in an NS-2 setting can test the WSN-FAHN technology here. Compared to modern schemes focused on efficiency measurements such as packet distribution rate (PDR), average throughput, detection rate, and life, the supremacy of the WSN-FAHN technique is shown by simulation outcomes. Useful network when the average residual capacity is reduced [6].

High saturation streams increase the capacity for collision and congestion in data transmission in the field of Wireless Multimedia Sensor Networks (WMSN), which dramatically degrades QoS efficiency. To ensure the consistency of operation, multi-channel deployment technology is also extended to simultaneous transmission. Find an efficient performance measure and design an efficient performance selection or scoring method centered on the required parameters that can be used for the multichannel allocation process as parameter inputs. The findings reveal that, after some phases of the self-learning phase, the deep reinforcement learning paradigm effectively achieves a stronger multichannel allocation approach. Due to the discovery of the main atmosphere in the first step of the learning phase, the primary weight fusion system helps one to minimize energy expenditure [7].

WSN has tremendous potential to serve numerous applications such as military and intelligent transport, wellbeing and medical sectors, environmental surveillance, etc. This paper outlined and examined the root and description of wireless sensor network faults focused on the national and international study status of fault diagnostic technologies. Centralized techniques and distributed algorithms were then developed according to the main location of the diagnostic error in error detection techniques. Finally, there is talk of potential research and development problems for sensor network malfunctions [8].

A very promising wireless technology approach for industrial applications is WSN(WSN). However, four key characteristics, namely, energy consumption, scalability, flexibility, and timeliness, must be met for the reliable implementation of WSN networks in an industrial setting. However, this increase in communication efficiency is accomplished at the cost of higher latency, which might not be sufficient for strict timing specifications in industrial applications. Often, this is only feasible in certain circumstances by selecting MAC parameter values that are not officially allowed by the specification [9].

In mission-critical industrial applications and delay critical industrial applications, WSN(WSN) is the most common because they have low latency and efficient message delivery. The stable relationship between the sump and the sensor nodes is very necessary for applications including gas leak detection, pressure management, and industrial process control, etc. Sensor nodes are positioned very densely in WSN in diverse locations and also without a particular network configuration. The positioning of the sensor nodes plays an enormous role in an industrial setting and, most significantly, improves overall machine productivity by accurately communicating optimized readings and ensuring optimum protection for industrial equipment. By positioning the sensor nodes in three separate topological designs: linear, level one, and split level one, we measured the efficiency of the wireless sensor network (WSN) [10].

In the era of networked networking, WSN plays a crucial function. With a vast number of sensors connecting within the range of the network, exponential development in connectivity technologies has allowed the wireless sensor network to evolve faster and faster. This present several strategies for soft computing and data mining that will be applied to evaluate the answer to these issues in the wireless sensor network. These strategies can function quickly and reliably and cause issues with the wireless sensor network [11].

Table 1: extracted research previews

Author	**Technique Used**	**Area of research**	**Result**
Sharma & Lobiyal (2015)	ad-hoc on-demand distance vector, dynamic state routing and temporally ordered routing algorithm	WSN	performance of ad-hoc on-demand distance vector, dynamic state routing and temporally ordered routing algorithm protocols
Roy et. al. (2020)	block-based routing protocol	WSN	suggested routing algorithm, focused on the residency positions, guarantees that all data in the cluster is propagated to the ms following the minimum hop route to minimize the gap in the broadcast of data
rai et al. (2017)	quality of facilities (Qos) for wireless sensor network	WSN	simulation results include overall network output that, along with a variety of dead nodes, total power consumption, community header settings, and performance, depends primarily on a number of factors
Fotohi & Bari (2020).	filtering algorithm based on firefly, and the neural network of Hopfield (WSN-fahn)	WSN	to modern schemes focused on efficiency measurements such as packet distribution rate (pdr), average throughput, detection rate, and life, the supremacy of the wsn-fahn technique is shown by simulation outcomes
Liu (2017)	utilizing the deep q network augmented learning system 9DQMC),	wireless multimedia sensor networks (WMSN)	present the incorporation of a progressive machine learning methodology into the multichannel personalization process

III.PROBLEM STATEMENT

It is quite hard to detect the suspicious activities in WSN communication. This research has main focus of detection of Malicious Nodes in WSN using Neural Network. For this we are considering the Neural Networks as the mechanism to perform the random creation of test and differentiate the time domain activities. The performance of every classifier is check based on various parameters like packet delivery, end-to-end transmission, and delay, and throughput.

IV. METHODOLOGY

The first phase in understanding the efficiency of wireless communications in the ecosystems and densities in which we anticipate sensor networks to be implemented is taken in this paper [1,4]. Packet transmission efficiency is the key feature of wireless performance that we are worried about. The key output metric is, to be more accurate, the packet loss rate (the number of packets sent but not returned within the time frame) or the supplementary receipt rate. In a wireless communication device, several, many variables control the efficiency of packet representation: environment, network topology, traffic trends, and therefore the real physical phenomena that drive the communication operation of the node. It is hard to distinguish these phenomena to research the effect of multiple influences on the efficiency of beam transmission. Also, from a more mechanical viewpoint, this white paper addresses the packet transmitting performance of two different layers in the network stack: the physical layer and the layer of medium access. We do this in a structured manner, which suggests that we have a certain influence over the topology of the network, the output of traffic, and the time and length of our experiments [5,6]. Our studies are not fully monitored, however, since our measures are sensitive to external influences, such as environmental variability. This is deliberate because we want (at least in part) to consider how contact is influenced by environmental influences. We would use the widely utilized model of the sensor network since it helps to explain the distribution of the data packet on the sensor network. Implemented Network Stack in Mica mote [7], RF Monolithic [8], Tiny OS [9]. This is a shifting target; the numerous radios and protocols will start to move as the platform begins to develop. We fix this by not creating a single difference that can be overridden by the current platform's gradual progress and by mentioning our assumptions that are likely to be influenced by technical shifts. We discuss these experiences in more detail in the following subsections.

A. Proposed Algorithm

```
Create a network of 20 nodes organized in elliptical form.
Select the source and destination of the node and the node of the sensor.
It's though (data is not received by destination)
Reflect this
If so (sensor node detect collision)
And,
Apply a neural pattern recognition network to alter the location of the node where the collision is observed.
And launch the transmission again from the source node.
Now, Else
Transmit the data from one node to the next.
End if it is
End as Network needed.
Exit, exit.
```

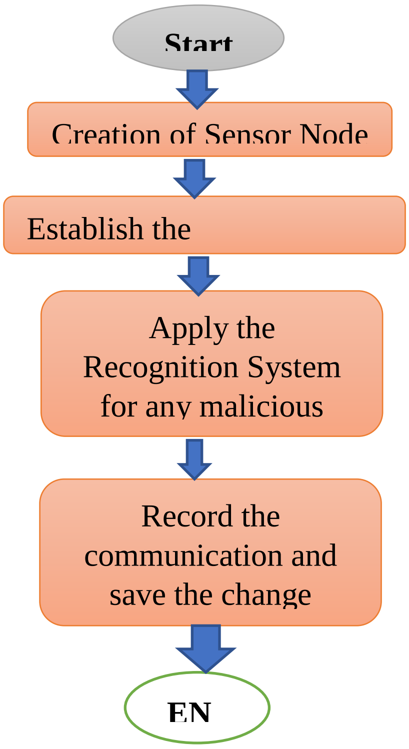

Start
Creation of Sensor Node
Establish the
Apply the Recognition System for any malicious
Record the communication and save the change
EN

Fig 2: Flowchart for the proposed algorithm

.B. Result Estimator

The performance of every classifier is check based on various parameters like packet delivery, end-to-end transmission, and delay, and throughput gets. for better comparison for the classifier by the given matrices.

C. Packet delivery ratio-

Tt signifies that the total number of messages received by the computing nodes and the total number of messages generated by the computing nodes.
Packet delivery ratio calculated by the given formula
PDR= ((Packet Transmitted- loss packet)/ Packet Transmitted) *100.

D. *End to end delay*

Delay means after the successful broadcast of the packet from the source node, packet reach to the destination nodes, then how much time it will take to reach to the destination node that is known as an end-to-end delay.

E. Throughput

Throughput means the number of data packets set from transmitter end known as throughput. In terms of the communication channel. How many packets are traverse to the channel per unit time.

Throughput=total number of packet/ ends to end delay.

These parameters estimated through the pattern recognition method which has to be used under the neural network implement in MATLAB for execution. These parameters reflect the overall communication and any type of malicious activities in WSN.

F: Proposed Flow Chart

V. CONCLUSION AND FUTURE WORK

A fundamental function of all sensor network implementations is being able to detect intrusion. Sensors networks cannot be used for traditional network defense because of the special features of sensor networks. To begin with, sensors are responsive to production costs since they need a large number of sensors said that sensor networks require a low production cost. As a result, sensor nodes are mostly power, memory, and computation/ Sensor nodes usually draw power from batteries and must be done infrequently. Consideration of network energy use becomes essential for most sensor network protocols. Secondly, Sensor nodes are vulnerable to physical assaults by adversaries who may be put in public locations. Enemies are usually expecting that this research may access a sensor node without leaving any evidence of their activity. Furthermore, the size of sensor networks is immense, and the topology is modified dynamically when certain nodes become unavailable due to lack of resources or become inaccessible due to malfunction.

REFERENCES

[1] S. Srivastava, M. Haroon, and A. Bajaj, “Web document information extraction using class attribute approach,” Proc. - 4th IEEE Int. Conf. Comput. Commun. Technol. ICCCT 2013, pp. 17–22, 2013, doi: 10.1109/ICCCT.2013.6749596.

[2] H. S. Kharkwal, “Automated Task Allotment in Unmanned Submarines by Smart Searching Algorithm,” vol. 13, no. 2, 2017.

[3] R. Sharma and D. K. Lobiyal, “Proficiency Analysis of AODV, DSR and TORA Ad-hoc Routing Protocols for Energy Holes Problem in Wireless Sensor Networks,” Procedia - Procedia Comput. Sci., vol. 57, pp. 1057–1066, 2015, doi: 10.1016/j.procs.2015.07.380.

[4] M. S. Husain and D. M. Haroon, “an Enriched Information Security Framework From Various Attacks in the Iot,” Int. J. Innov. Res. Comput. Sci. Technol., vol. 8, no. 4, 2020, doi: 10.21276/ijircst.2020.8.4.3.

[5] Mazumdar, N., & Pamula, R. (2020). An energy and coverage sensitive approach to hierarchical data collection for mobile sink based wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 1-25.

[6] R. Fotohi, “A Novel Countermeasure Technique to Protect WSN against Denial-of- Sleep Attacks Using Firefly and Hopfield Neural Networks (HNN) Algorithms.”

[7] Liu, Z. (2017). Self-Adaptive Bandwidth Control for Balanced QoS and Energy Aware Optimization in Wireless Sensor Network (Doc Temporally Ordered Routing Algorithm dissertation).

[8] F. Zhu and J. Wei, “An energy-efficient unequal clustering routing protocol for wireless sensor networks,” vol. 15, no. 9, 2019, doi: 10.1177/1550147719879384.

[9] Anastasi, G., Conti, M., & Di Francesco, M. (2010). A comprehensive analysis of the MAC unreliability problem in IEEE 802.15. 4 wireless sensor networks. IEEE Transactions on Industrial Informatics, 7(1), 52-65.

[10] Rai, P. K., Bharti, P. K., & Yadav, R. K. (2017). An Approach to Comprehend the Quality of Services (QoS) For Wireless Sensor Network. International Refereed Journal of Reviews and Research, 5(6), 1-5.

[11] M. S. Husain and D. M. Haroon, “an Enriched Information Security Framework from Various Attacks in the Iot,” Int. J. Innov. Res. Comput. Sci. Technol., vol. 8, no. 4, 2020, doi: 10.21276/ijircst.2020.8.4.3.

[12] Khan, M. F., Felemban, E. A., Qaisar, S., & Ali, S. (2013, December). Performance analysis on packet delivery ratio and end-to-end delay of different network topologies in WSN(WSNs). In 2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks (pp. 324-329). IEEE.

[13] Sunitha, R., & Chandrika, J. (2016, February). A study on detecting and resolving major issues in wireless sensor network by using data mining and soft computing techniques. In 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS) (pp. 1-6). IEEE.

[14] Kodali, Ravi & Muraleedhar, Anupama. (2015). WSN in spice cultivation. 10.1109/ICGCIoT.2015.7380640.

[15]https://www.openaccessgovernment.org/dependable-secure-trustable-wireless-sensor-networks/27971/

ABOUT THE AUTHORS

	Nagma Shakeel, M.Tech research Scholar, CSE, Integral University, India.
	Mohd. Haroon is working as Associate Professor in the Department of Computer Science & Engineering at Integral University, Lucknow (U.P), India. He has completed his PhD in "Dynamic Load Balancing in Distribution System" in 2016. research area: distributed machine learning, artificial intelligence.
	Faiyaz Ahmad is working as Assistant Professor in the Department of Computer Science & Engineering at Integral University, Lucknow (U.P), India. He has completed his PhD in "Soft Computing" . research area: Soft Computing machine learning, artificial intelligence, Cyber Security.

Paper 2

Research paper communicated and accepted in "Multidisciplinary International conference FTSE-2021" in Rai University. (Springer)

https://www.raiuniversity.edu/conference_2021/reg.html

Soft computing approaches are used for packet drop and energy-saving policy during transmission of data in WSN

Nagma Shakeel1 [] , Mohd Haroon2 [0000-0001-7967-7302 ,] Faiyaz Ahmad3, Manish Madhav Tripathi 4 ,[0000-0003-3441-5733]

nagmashakil5@gmail.com1, mharoon@iul.ac.in2, faiyaz@iul.ac.in3, mmt@iul.ac.in4

1,M.Tech Research Scholar, CSE, Integral University, Lucknow, India
2 Associate Professor Dept of CSE, Integral University, Lucknow, India
3 Assistant Professor Dept of CSE, Integral University, Lucknow, India
4Associate Professor Dept of CSE, Integral University, Lucknow, India

Abstract. Machine learning also inspires a slew of practical solutions that help you make the most of your resources and extend the life of your network. We will cover the literature review section of machine learning and deep learning into the many applications of wireless sensor networks in this study, as well as the numerous benefits and drawbacks of machine learning applications on wireless sensor networks. This study sees as a comparison guide to assist WSN designers in selecting the best machine learning solution for their application difficulties. This analysis provides an overview of embedded network applications as well as a discussion of the needs that this analysis generates. In addition, we explored the various in-network processing approaches and drew parallels between the Hopfield neural network and other neural networks. On the MATLAB-2013 command prompt and the GUI established throughout the investigation, more comprehensive simulations were run. It was discovered that all terms, including transmission, throughput, E2Edelay, and PDR, have an increasing value. As a result, using a neural network with a high iterating value for WSN test randomization to detect packet drops will provide a superior solution, further avoiding packet drops. As a result, the digital data has very clear implications for the proposed work. When compared to the previous year, it has nearly doubled. As a result, it's evident that when neural networks use high iterating values, they're much better at limiting packet loss thanks to very active pattern recognition algorithms that help fix packet loss issues. As a result, throughput and end-to-end latency have improved slightly.

Keywords: *wireless sensors network, energy-efficient routing, machine learning, fuzzy logic.*

1 Introduction

The Wireless Sensor Network is a geographically dispersed, self-contained wireless network of devices that collaborate to monitor physical and environmental factors such as temperature, sound, vibration, pressure, movement, and pollution at various locations. Because of the sensor network's vast scale, sent as well as received Transmission, processing, and data storage in a large-scale sensor network are simply impossible due energy constraints and channel bandwidth limitations. For better system usage and energy utilization, machine learning algorithms are used in a wireless sensor network.

Wireless channels connect the network computer nodes. Each sensor computing node's or a battery's electricity is acquired. Sensor computing nodes are a type of sensor network that has a small, lightweight, and portable capacity. Each sensor computing node is equipped with a transducer, microprocessor, transceiver, and power source.

Each sensor computing node is equipped with a transducer, microprocessor, transceiver, and power source. Electric impulses are generated by the transducer because of physical and sensitive processes. A packet is a binary data unit that may be sent via the internet. A cooperative computing node that loses all or portion of the packets to be delivered is known as packet dropping.

The Wi-Fi sensor network is made up of a small device called a sensor computing node, which contains the RADI, CPU, memory, battery, and sensor hardware (WSN). The broad deployment of these sensors allows for detailed monitoring of the surroundings. Sensor computing nodes are limited in terms of radio range, CPU performance, memory capacity, and power.

Designers are compelled to build systems for specific applications due to the lack of resources. As a result, certain communication patterns emerge on WSNs. In contrast to ad hoc networks, transportation is less unpredictable. Karlof and Wagner split WSN traffic into three categories:

1.1Many-to-one: A network's base station or aggregation point receives readings from many sensor computing nodes.

1.2 One-to-many: A single computing node (usually a base station or an aggregator) sends query or control information to numerous sensors computing nodes.

1.3Local communication: Neighboring computer nodes provide localized signals to locate and coordinate jobs. Furthermore, sensor computing nodes in WSNs are often stationary, with a low traffic rate. There's also a steady stream of vehicles. Long periods of idleness may occur, during which sensor compute nodes turn off their radios and go to sleep to save energy. MAC protocols such as S-MAC and TDMAMAC have been designed to take use of this WSN characteristic while conserving energy.

Energy is a restricted resource since sensor computing nodes rely on batteries. Recharging or replacing batteries is expensive, and it may not be possible in some circumstances. As a result, WSN applications must be very energy efficient. The term "process data" refers to data that has been processed, "information" refers to meaningful content, and "information" refers to data that has been sent from one computer node to another through a communication channel and an application protocol in wireless sensor computing. In addition, one feature of a WSN is its capacity to interact with one another in real time via a wireless channel, while employing sensor computing nodes to identify and operate a particular item.

To achieve their goals, any of these computer nodes must collaborate. Connectivity and shared operation of the underpowered Wireless Sensor Network are enabled by on-line connections between the computer nodes o-one and a one via a Wireless Connection (WSN). They may be called upon to work in high-stress situations, such as combat and surveillance. Because WSNs are self-contained, numerous novel attacks are seldom overlooked. WSN have lately garnered a lot of attention due to their extensive employment in both the military and civilian contexts. A broad range of clandestine and often hostile settings, including military and domestic intelligence, make extensive use of WSN.

Therefore, preserving netbook integrity requires authentication methods that are both convenient and secure while also meeting the overall objectives of data privacy and trustworthiness. At this time, artificial intelligence technology is being used all over the globe, and a range of artificial intelligence devices and protocols are being used for a number of applications. Artificial evidence agents and protocols, as well as wireless sensor computing nodes, play a significant part in wireless sensor computing.

A. Sensor computing nodes

The network's jobs are managed by the sensor computing nodes. Although measurements and queries can take place in the Task Manager, data can also be transmitted via sensor computing nodes if these techniques are used [1]. Depending on the device, calculations may be performed on a computational node. Depending on how the model is constructed, it may either transmit data to more compute nodes or provide data directly to the task manager [1]. Sensor computing nodes may function as either a source or a relay, depending on the sensor used: The root refers to a way of identifying and getting what you are looking for in life. As a consequence, the globe serves as the source. A sink or an actuator, on the other hand, is a device that receives data from a sensor or an actuator. [1].

2.System Components and Operations in a Wireless Sensor Network

This is where the sensor infrastructure is concentrated [2]. The computer node as well as the sub-world sensors are put to the test. The sensors are put to the test. Before we go into the protocols and systems needed to set up a sensor network, let's have a look at the WLAN network's architecture and data processing [2]. It's critical to look at all the power and hardware/software savings. One of the goals of this study is to gather information and provide recommendations for hardware that may be used on sensor computing nodes. [1] This may get a comprehensive explanation of the equipment.

2.1 Sensor computing node in communication architecture

Initially, a sensor is a low-power wireless communication device that communicates with other sensors. A sensor computing node is frequently used as a data processor, storage device, and communicator all at the same time [1]. This is known as multitasking. This list includes the conventional sensor computing node controller, memory, sensors, communication system, and power, all of which are traditional in nature (see Figure 2). A controller's responsibilities include processing all relevant data and performing arbitrary algorithms. The memory functions are responsible for the data and memory of the programmer. Input sensors and output actuators are the means through which the environment is communicated with by the system. These devices enable for the monitoring and regulation of one or more environmental iterating inputs. Radio waves interact with the gadget. Finally, electronic components require electricity to function. One of the primary architectural issues in WSN is energy efficiency. As a result, these interrelated components must work with the fewest resources possible [1].

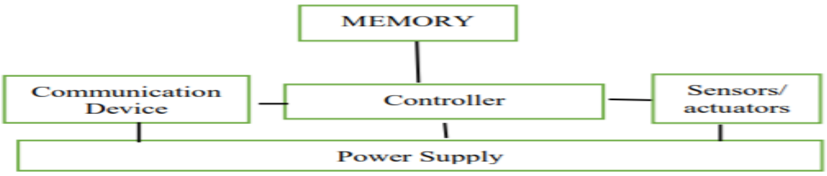


Fig. 1: Overview of sensor computing node hardware component.

2.2 Wireless Sensor Network Applications

Low sampling rate, seismic, magnetic, thermal, visual, infrared, radar, and acoustic sensors are all used in these sensor networks, and they all have one thing in common: they all allow for monitoring of several elements of the environment. Sensor computing nodes are frequently used for continuous sensing, for events such as event identification or state change, as well as event detection and local actuator control [1]. Commercial, military, environmental, home, and other health and welfare applications all employ wireless sensor networks [2].

3. Designing Problems of Wireless Sensor Network Architecture

Coverage

The routing algorithm employs a coverage algorithm for the identification and transmission of sensors in a network of wireless sensors. The sensor computing nodes for the entire network should be chosen. Lowest and maximum exposure route algorithms, as well as a coverage design tool [2], are suggested as efficient techniques.

3.1 Clocks

The wireless sensor (WSN) is an important service for clock synchronisation. This synchronisation primarily entails supplying an ordinary time scale to the computing nodes of local clocks in the sensor networks. Such clocks must be synchronised in some applications, such as monitoring and tracking [1].

3.2 Computation

The computation may be defined as the total amount of data that travels through each processing node. The main issue with computers is that it must reduce resource consumption. Data processing will be completed at each computing node before data is transmitted to the base station if the base station's life expectancy is in jeopardy. If each compute node has resources, the entire calculation should be done at the sink [2].

3.3 Production Cost

A WSN is made up of many sensors computing nodes. As a result, if the cost of a single computer node is too high, the cost of the entire network will be prohibitively high as well. Ultimately, the price of each sensor processing node must be kept low. As a result, figuring out how much each sensor compute node in a wireless sensor network costs is challenging [2].

3.4 Hardware Design

Any sensor network's hardware, such as the power control, microcontroller, and communication unit, must be energy-efficient when designed. It may be designed in such a manner that it consumes less energy.

3.5 Quality of Service

The sole need for service quality, or QoS, is that data be exchanged in a timely manner. Because certain sensor-based applications are heavily reliant on real-time information. As a result, if the data is not sent to the receiver in a timely manner, it will be useless. Many types of QoS issues have been found in WSNs, including network topology that may change frequently and the available information state used for routing that may not be correct. In this study, QoS mostly includes PDR, E2Edelay, and Throughput [2].

4.0 End to end routing protocol using machine learning approach

Because wireless sensor computing nodes have two major constraints, memory and computational power of the computing nodes, communication cost between computing nodes, adhoc infrastructure of the network, limited energy of the computing nodes, mobility of the devices, and the network's dynamic topology, machine learning approaches are widely used in wireless sensor networks. In wireless sensor networks, several machine learning algorithms such as network associated rule and application associated rule are employed. Machine learning approaches are employed in the network related rule for optimum deployment of computer nodes, data routing, and overall network security concerns. Quality of service, resource allocation, data aggregation, and a variety of other issues are among them. Machine learning is utilized for information processing, evet identification, target class identification, and many other things in application associated rules [11].

5.0 Fuzzy logic-based end to end delivery of the data:

Zohre and Arabi have proposed a fuzzy logic-based routing method for wireless sensor networks. In this algorithm, two techniques are used: the earliest first tree and source-initiated data dissemination. This fuzzy model is built entirely on fuzzy logic, and it is used to choose cluster heads as well as provide routing algorithms between computing sensor computer nodes. Initially, the entire sensor network is transformed into a cluster, with the fuzzy variable determining the suitable cluster head among the cluster. The total number of energies consumed by the wireless sensor network is given by

ETX (K, D)= { KE ELEC + K∈FSD2 where D<D0 and { KE ELEC + KampD4 WHERE D>D0 (1)

Where D is the distance between the receiver and the sender, and E ELEC is the consumed energy of radio transmission, ∈FS and amp are the power amplification for the sender and receiver communication channel, and the d0 is the distance threshold, which is further evaluated by the following given equation [12].

Now D0=∈FS/ amp

And Erx (K)= KE ELEC+ k (1/a-1) EDA

Here (1/a-1) EDA, represent the energy consumed by the system

6.0 CLUSTER HEAD SELECTION BY FUZZY RULE:

The cluster head of a wireless sensor network can be chosen using a fuzzy inference algorithm. The sensor computing node acquires its own energy as well as the energy of neighboring sensor computing nodes, as well as the number of neighboring computing nodes; these three variables are the input variables of the fuzzy inference system; the output of the fuzzy inference gives the value, and cluster head can be determined because of that value.

The remaining energy of the sensor computing node may be expressed by three fuzzy variables: low, medium, and high, according to Eres. REN={X1=” LOW, X2=”MEDIUM”, X3=”HIGH”}

NN={X1=”LESS”, X2=” AVERAGE”, X3=”ENORMOUS”}

RENN={X1=” NORMAL, X2=”STRONG”, X3=” WEEK”}

Using the fuzzy control defuzzied function gravity methods, the defuzzification can be achieved

$Z = \int U(Z)Zdz/UZdz$ Where z is fuzzy output and U(Z) fuzzy fusion function

6.0 Result and discussion These practical solutions may use machine learning to make more efficient use of network resources and increase the lifetime of your network. To summarize, this research presents a comprehensive literature assessment of machine learning approaches from 2002 to 2018, which are utilized to deal with commonplace challenges in wireless sensor networks (WSNs). The pros and cons of each algorithm are examined to decide which would be most suitable for the task at hand. This serves as a resource for WSN designers, who may use it to assist create the ideal machine learning solution for their application's unique issues. In the early stages of packet sending, a certain number of packets were transmitted because only a small percentage of packets were lost. Based on these findings, in the digital data, it is evident that the suggested task would be successful. Compared to the same period a year before, it has almost doubled. Since it is now known that when neural networks employ high iterating values, they perform significantly, it follows that when neural networks use high iterating values, they minimize packet loss owing to highly active pattern recognition algorithms, which also corrects packet loss issues. The improvements in end-to-end latency and throughput are secondary to this change. Since the suggested system performs a good job of collision detection during transmission and avoidance, then the suggested system performs an excellent job of collision detection during transmission.

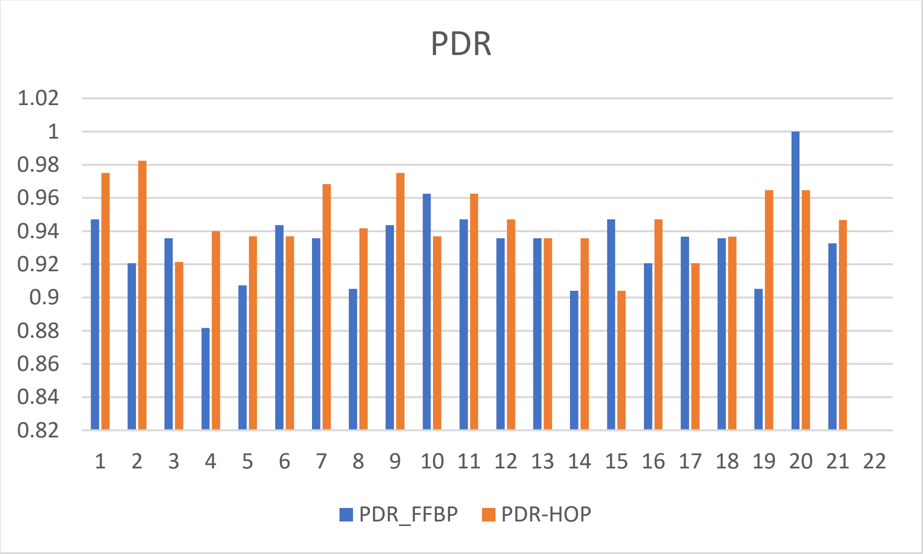


Fig2: PDR test result of 20 execution

As it appears in above figure that the PDR of the proposed neural network has 0.946655 slope compare it to existing FF Back propagation is 0.93256. The enhancement in overall 20 tests must be significant because the PDR is very concerning factors of WSN.

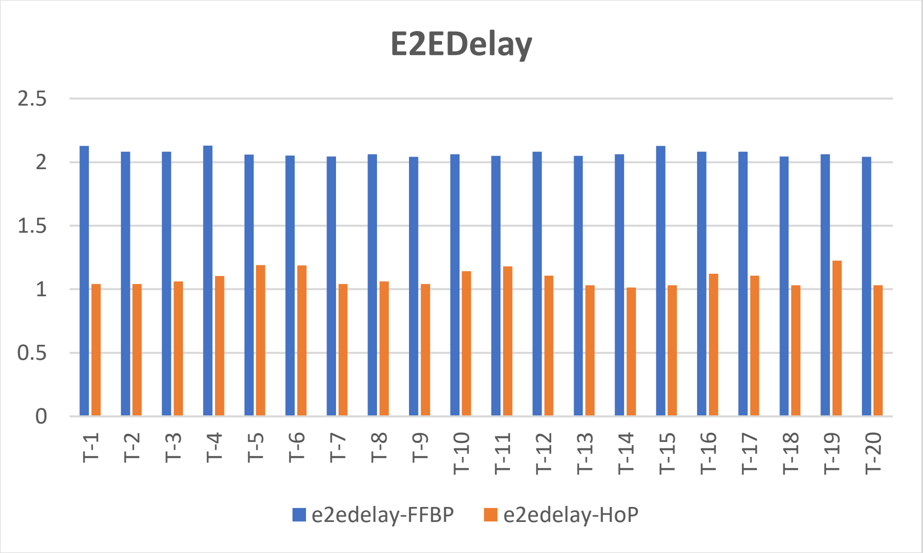


Fig3: E2EDelay test result of 10 executions

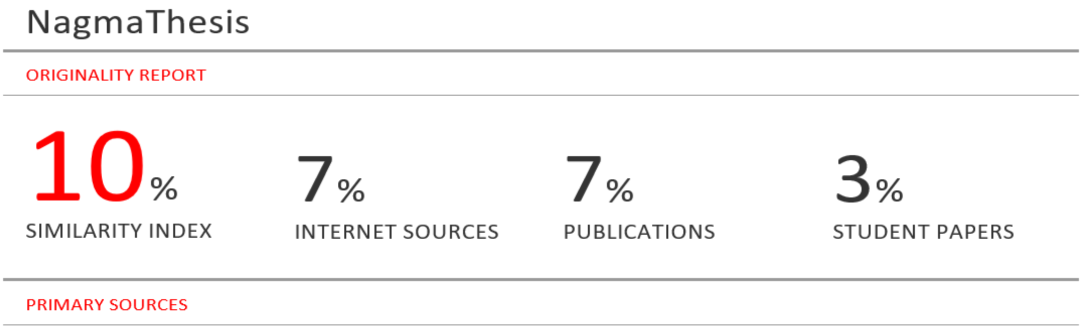
Conclusion: The key characteristics are as follows: WSNs are notable for their network form flexibility and sensor mobility. The throughput, latency, and packet transmission rate of a network are all discussed in this study. A jump field neural network is used for packet transfer. The backpropagation method's findings are compared to those of the Hopfield neural network. The jump field's outcome is superior to backpropagation in this comparison. Packet transfer rates and throughput rise, while end-to end delays fall. In addition, this article discusses how to efficiently recover wireless sensor network contention. In the future, machine learning applications can be applied to avoid packet drop using these iterating started. This paper presents an overview of embedded network applications and goes on to analyze the needs identified by this research. Additionally, we spoke about the chosen in-network processing approaches and compared the Hopfield neural network to the backpropagation network, emphasizing their resemblance in form. sensor network may be extended. A new context is added in the following neural network. The outlines of the practicality of neural networks in the sensor network environment, and assesses the early results acquired by our test implementation are quite significant

References

1. M. Haroon, and F. Ahmad, "A Study of WSN and Analysis of Packet Drop During Transmission," Int. J. Innov. Res. Comput. Sci. Technol., vol. 9, no. 2, pp. 79–83, 2021, doi: 10.21276/ijircst.2021.9.2.11.
2. [2]. M. Haroon, D. M. Husain, M. M. Tripathi, T. ahmad, and vandana kumari, "Server Controlled Mobile Agent," Int. J. Comput. Appl., vol. 11, no. 4, pp. 13–16, 2010, doi: 10.5120/1572-2101
3. [3] S. Srivastava, M. Haroon, and A. Bajaj, "Web document information extraction using class attribute approach," Proc. - 4th IEEE Int. Conf. Comput. Commun. Technol. ICCCT 2013, pp. 17–22, 2013, doi: 10.1109/ICCCT.2013.6749596.
4. [4] A. Saini, A. Kansal, and N. S. Randhawa, "Minimization of energy consumption in WSN using hybrid WECRA approach," Procedia Computer. Sci., vol. 155, pp. 803–808, 2019, doi: 10.1016/j.procs.2019.08.118.
5. [5] Z. Siqing, T. Yang, and Y. Feiyue, "Fuzzy logic-based clustering algorithm for multi-hop wireless sensor networks," Procedia Computer Sci., vol. 131, pp. 1095–1103, 2018, doi: 10.1016/j.procs.2018.04.270.
6. [6] M. Haroon and M. Husain, "Interest Attentive Dynamic Load Balancing in distributed systems," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 2015, pp. 1116-1120
7. [7] Lodhi, A. K., & Sattar, S. A. (2019). Cluster Head Selection by Optimized Ability to Restrict Packet Drop in Wireless Sensor Networks. In Soft Computing in Data Analytics (pp. 453-461). Springer, Singapore
8. [8] Faiyaz Ahamad, Manuj Darbari, Rishi Asthana "Service Mechanism for Diagnosis of Respiratory Disorder Severity Using Fuzzy logic for Clinical Decision support" Emerging Research in Computing Information Communication and Application. ERCICA, Volume 3, Pages: pp 309-317. 2016

9. [9] Faiyaz Ahamad, Manuj Darbari, Rishi Asthana “Review on A Clinical Decision Support System for Risk Based Prioritization Using Soft Computing Technique “International Journal of Scientific & Engineering Research, Volume 6, Issue 1, ISSN 2229-551,Jan-2015.
10. [10] Jaradat, Y., Masoud, M., Jannoud, I., Abu-Sharar, T., & Zerek, A. (2019, March). Performance analysis of homogeneous LEACH protocol in realistic noisy WSN. In 2019 19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA) (pp. 590-594). IEEE.
11. [11] Liu, W., Zhao, D., & Zhu, G. (2014). End-to-end delay and packet drop rate performance for a wireless sensor network with a cluster-tree topology. Wireless Communications and Mobile Computing, 14(7), 729-744.
12. [12] Thrimoorthy, N., Anuradha, T., & Kumar, A. (2017, September). A virtual model to analyze congestion in a wireless sensor network (WSN). In 2017 International Conference on Advances in Electrical Technology for Green Energy (ICAETGT) (pp. 28-32). IEEE.
13. [13] Vhatkar, S., Shaikh, S., & Atique, M. (2017, February). Performance analysis of equalized and double cluster head selection method in wireless sensor network. In 2017 Fourteenth International Conference on Wireless and Optical Communications Networks (WOCN) (pp. 1-5). IEEE.
14. [14] Tedeschi, A., Midi, D., Benedetto, F., & Bertino, E. (2017). Statistically-enhancing the diagnosis of packet losses in WSNs. International Journal of Mobile Network Design and Innovation, 7(1), 3-14.
15. Author, F.: Article title. Journal 2(5), 99–110 (2016).
16. Author, F., Author, S.: Title of a proceedings paper. In: Editor, F., Editor, S. (eds.) CONFERENCE 2016, LNCS, vol. 9999, pp. 1–13. Springer, Heidelberg (2016).
17. Author, F., Author, S., Author, T.: Book title. 2nd edn. Publisher, Location (1999).
18. Author, F.: Contribution title. In: 9th International Proceedings on Proceedings, pp. 1–2. Publisher, Location (2010).
19. LNCS Homepage, http://www.springer.com/lncs, last accessed 2016/11/21.

Plagiarism Report



NagmaThesis

ORIGINALITY REPORT

10%	7%	7%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES