JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

QoS Analysis of Customized WSN through Recurrent Neural Network

[1] Mr. Gaurav, [2] Dr. Rishu Bhatia, [3] Dr. Rakesh Joon, [4] Mr. Nitin Kumar,
[1] M. Tech. Scholar, [2] Associate Professor, [3] Associate Professor, [4] Assistant Professor
[1,2,3,4] Ganga Institute of Technology & Management, Kablana, Jhajjar

Abstract: *The use of repeat neural networks with high iterating values to identify and avoid packet losses is expected to result in a more successful WSN test randomization technique, which will further reduce packet losses. According to the planned research results, it was discovered in the first seven GUI tests and recommended seven times as a result of the findings. Given that only a small number of packets were lost in a single packet, it is clear that a certain number of packets were initially sent when specific packets were sent. As a result, when it comes to digital data, the results of the necessary effort are immediately visible. It nearly doubled when compared to the previous year. It is thus clear that when a repeating neural network employs large iteration values, the use of very active pattern recognition methods ensures that the network also repartees packet loss issues, thereby reducing packet loss. As a result of this change, overall latency and performance are only marginally improved. As a result, the proposed approach performs admirably in terms of packet drop during transmission and estimation of packet loss.*

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

I. INTRODUCTION

There was a lot of debate in WSN about a new one developed by researchers. The WSN ecosystem is frequently made up of large nodes that are randomly dispersed throughout the area; the network has evolved into a powerful and well-known piece of technological infrastructure. The ability of wireless sensor nodes to connect, compute, and generate electricity is limited. Broadcast messages are based on a well-known concept that allows a large number of people to mix and disseminate information effectively.

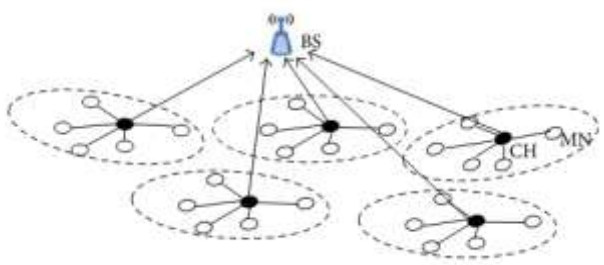

Fig. 1: Cluster-based WSN architecture

WSN has set up a massive one that makes use of less expensive energy. It is thus critical to use energy effectively and efficiently in WSN nodes in order to enhance network life, which is used by a variety of kinds including civic safety, identity, and, in particular, sunlight of subjects, a type of limited node, among others. In addition to the capacity to connect with, detect, and analyses a greater number of transmissions, it is also named for the ability to send limited signals across long distances via intermediary sensitive epidemics.

Because of their limited resource availability, they are often unable to deal with a difficult opponent. It is necessary in this scenario to implement an extra defensive phase known as the Intrusion Detection System (IDS) to protect the system against intrusion [8]. The usage of effective intrusion detection systems (IDS) can identify the different attack methods employed by the attackers. Unfortunately, because of WSN capabilities, most sensor networks are highly vulnerable to attack, and adversaries can only generate packets with the same message content as the original packets or alter the original message content. As a result, the network employs authentication methods to ensure that node-to-node communication is secure. The transfer of data between nodes in WSNs must be done securely.

Significant amounts of information must be transferred between endpoints for the modern communication system to function properly. This can only be accomplished through a wireless connection, which is currently the only reliable method of communication available in the digital era. The open-channel wireless environment is used as a transmission medium to send data from source to destination nodes. Wireless sensor networks (WSN) and wireless body networks (WBN) are two kinds of wireless networks (WBAN). WBAN networks are implanted in people and detect bodily conditions in various areas of the human body, which are then sent to a remote unit for analysis. In the case of WSN networks, the number of sensors is distributed at random, and all of the sensors transmit data. The detected data is received and processed by an external device. The number of sensors under the control of a single node is collected by the cluster head. Cluster heads collect all sensitive

information from their clustered nodes and send it to a dish located a distance away from each cluster head.[1-7]

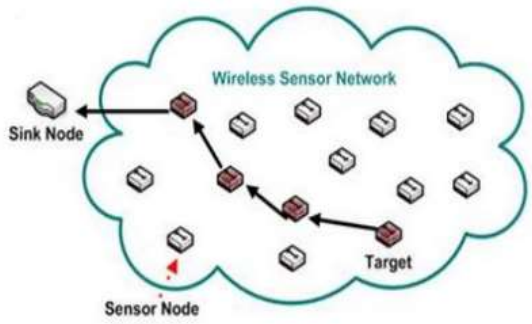

Fig. 2: Node's deployment in WSN network

Any number of cluster heads connected to a single sink node can be accessed in WSN networks. Every WSN node has a sensor, an analogue to digital converter, and a digital processor. In analogue mode, the sensor detects the parameters in its environment and converts the analogue data it collects into digital data using an analogue to digital converter. The processor unit processes the converted digital data and transmits it to another node via the integrated wire antenna that is connected to the node in which it is located. In the WSN environment, Fig.2 depicts the deployment of sensor nodes in conjunction with a sink node that is connected to the WSN networks. An external attacker or hacker changes the behavior of nodes internally, and these nodes are malicious and difficult to detect. The number of malicious or hidden nodes in modern WSN networks [10,11] has a negative impact on network efficiency. As a result, the technique described in this article for identifying thesis nodes in WSNs, which can be used to improve performance, is very effective.

1.1 Malicious Node Detection using recurrent neural network s

Using a recurring neural network predictor, detect and remove fake sensor nodes. Analytical redundancy is used in this technique to estimate the value of a sensor based on the values provided previously and now by adjacent sensors. This estimate is compared to the sensor's actual value in order to increase or decrease its confidence factor.

1.2 Sensor Network Model

We accept the following assumptions about the sensor network:

(a) The network sensor is static; e.g., the sensor nodes are not mobile; the sensor node knows its own location even if it is disseminated via aerial distribution or physical installation. If not, via the placement process the nodes may reach their own location. Furthermore, all sensors have completed one-time authentication after deployment in the field.

b) the sensor nodes may be compared to the current sensor nodes, e.g., in computation and communication capacity and power resources of Berkeley MICA motes. We assume each node has space to store up to 100 bytes of keystones to guarantee symmetrical data transmission cryptography.

c) The base station, commonly referred to as the access point, operating as a controller and key server, has to be equipped with long-term power as a laptop class device. We also assume that the base station will not be compromised.

d) We rely on the design of the mobile wireless network (WCN). There are already a lot of base stations in this configuration. Each base station builds a cell covering part of the area.

If they are within cell range, mobile wireless nodes and other devices can connect wirelessly. The main distinction in the cellular network is that base stations are considered mobile, so each cell has different boundaries and mobile wireless nodes as long as they are within the range of mobile access points.

The following two types of architecture (WCN and SENMA) have important features that have been evaluated in order to establish a safe sensor network: Node-to-node communication; multi-CNN data transfer; sensor synchronization is not required; sensor-to-node communication is only required if polled for; complicated protocols are avoided; individual sensor systems are far less trustworthy; mobile nodes do not require system reconfiguration.

1.3 WSN Infrastructure and peripherals Basic

Wireless Sensor Networks (WSN) [4] is a novel technology which has received significant interest from scientists. In general, overhead requirements are underpowered by big randomly positioned nodes in terms of networking, computation and energy. The message sent is an efficient and common network of wireless capabilities [12,13], allowing many users to rapidly combine and relay messaging packets.

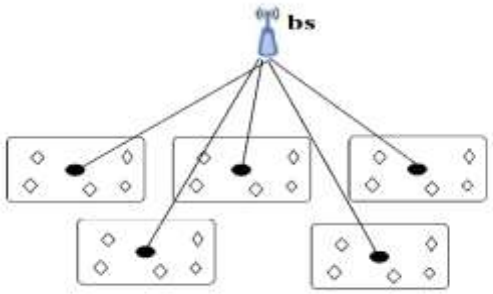

Fig. 3: WSN presenting Clustering formation

Wireless sensor networks [5] are used in a variety of civil and military systems for mapping, surveillance, environmental recognition, and weather prediction. Because the node battery has insufficient storage capacity for this type of network, it is critical to use resources in WSN nodes to extend the network's life in an effective and appropriate manner.

Sensor nodes are small lightweight devices that interact, sensor, and analyses data across a larger network than a node to a destination node. As a result, there is a limited distribution of contact information consumer transmission spectrum. Because of their limited resources, they frequently have little ability to repel a powerful assault. Active IDS can identify attackers who have devised massive attack methods. Unfortunately, because of WSN features, most sensor networks have a sensitive effect, and opponents may only generate network traffic and cause significant packet losses (6, 9) when the packet is sent or the original content is changed. To get the packet out there. To ensure secure connections between nodes, the network employs authentication methods. Inside WSN networks, secure data transfer between nodes is critical.

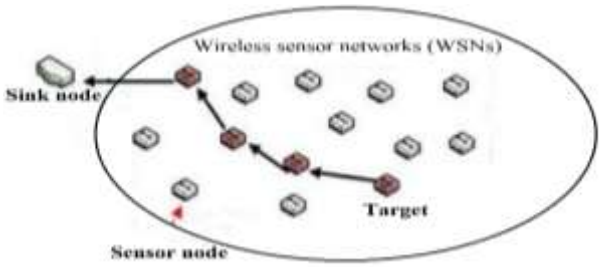

Fig. 4: Node's deployment in WSN network

The design of an electronic network necessitates the use of reliable data transmission standards from one end to the other. Because the internet age currently employs encrypted interaction, this can only be accomplished via a mobile network. As a transmission method, an open wireless channel environment between the source and destination nodes is used. Wireless Sensor Networks (WSN) [9] and Wireless Body Field Networks (BFN) are two types of wireless networks (WBAN). WBAN is used in humans, and it detects bodily conditions and communicates this information to a remote computer in many areas of the human body.

For WSNs, sensor numbers are transmitted at random, and data from all sensors is collected. This detected data is sent to the remote computer as a recipient. The head of the block indicates the number of sensors grouped in a node. The block's header receives all physical information from its clustered nodes and is sent to a remote torrent by each community's head.

WSN networks can connect to a number of community headers with a single node in the basin. Each WSN is equipped with a sensor, an analogue to digital converter, and a CPU. The sensor detects the environment in analogue mode and converts the analogue sensor data to digital data using an analogue to digital converter. This converted digital data is processed by a processing system and transmitted to another node via an integrated wired antenna connected to the node. Figure 1.2 depicts the sensor nodes integrated within the WSN environment, as well as the basin nodes associated with the WSN networks. Remote attackers or intruders disrupt node activity, causing these nodes to become hostile. The number of malicious/hidden nodes reduces the efficiency of modern WSNs. As a result, this article proposes a critical solution for locating WSN nodes in order to improve performance.

A wireless sensor network is made up of a wireless network of devices known as sensor nodes (called nodes). Circular, robot, micro power, and low-power systems are examples of these devices. Naturally, these networks include a diverse set of dispersed and battery-powered portable networked computers for data collection, aggregation, and dissemination by operators, as well as enhanced computing and processing expertise. Nodes are small computers that connect to form a network.

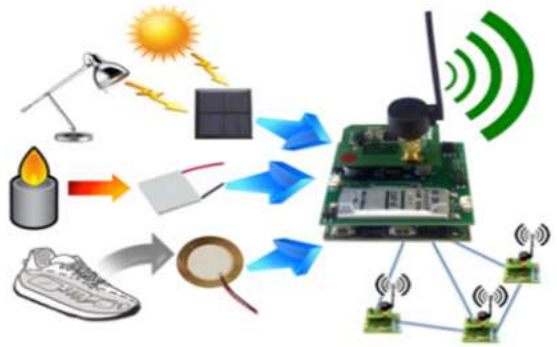

Fig. 5: wireless sensor network

The energy-efficient and versatile wireless system. Applications of industrial foods are widespread. The sensor node assembly collects data from the surrounding areas to achieve defined application objectives. The dying person may communicate using transmitters and receivers. The mortality toll of hundreds or even thousands of people on a network of wireless sensors [15-16]. Ad hoc networks, unlike network sensors, contain few nodes and no architecture.

1.4 Packet Loss Detection using recurrent neural network s

A method to identify and remove fraudulent sensor nodes using a recurrent neural network predictor. This measurement is compared with the actual raise/reduce conviction rate sensor data.

1.4.1 Packet Loss Detection in complex dynamic scenes

The Giant Lopula Motion Detector is a specific neuron in the lobster brain that responds strongly to images of an approaching object like a predator (LGMD). The computer model can deal with unexpected circumstances without using specific methods to detect artifacts. In this paper, we propose a recurrent neural network focused on LGMD by incorporating the thrill of packet loss detection into a dynamic environment. The network features a new feature optimization method and can optimize the extended edges of Packet Loss objects. The new method filters out the separate emotions generated by context data. The benefits of the recurring neural network based on LGMD were shown through offline study in various settings. The use of recurrent neural networks focusing on LGMD as the sole sensor mechanism has shown in real-time tests that the platform has succeeded in a variety of situations. Well-organized courtyards can be crossed by robots, in particular ones with complicated history.

The Wireless Sensor Network is a geographically distributed, autonomous wireless system of devices which use sensors that monitor physical and environmental variables, such as temperature, sound, vibration, pressure, movement or pollution, in collaboration. The network nodes are connected through wireless channels. Electricity is obtained from each sensor node or battery. There are numerous sensor networks, each having a small, lightweight and portable capacity called sensor nodes. Each sensor node contains the transducer, microcomputer, transceiver and power supply. Depending on the physical and sensitive impacts, the transducer generates electric impulses. A packet is a binary data unit which may be routed through a network computer. The drop of packets is a node that drops all or part of the packets to be transmitted. The Wi-Fi sensor network is a little device called a sensor node containing the RADI, CPU, memory, battery and sensor hardware (WSN). The environment may be monitored carefully using these sensors. Radio range, CPU speed, memory and power are limited to sensor node resources. The resource-free nature obliges designers to develop solutions for specific uses. This leads to specific communication patterns on WSNs. It's not as unreliable transport as it is in ad hoc networks. WSN traffic by Karlof and Wagner is classified into one of three groups:

1. **Many-to-one:** Readings from numerous sensor nodes are received from the base or aggregation point of a network.
2. **One-to-many:** A single node (typically a base station or an add-on) transmits query information to many sensor nodes or control information.
3. **Local communication:** Nearby nodes provide localized messages to locate and coordinate tasks.

Furthermore, sensor nodes often stay stationary and the traffic in WSNs is very modest. There is also an ongoing traffic flow. Long periods of idleness may take place during which the sensor

nodes turn off and sleep to conserve power while listening idle. To exploit this WSN characteristic, MAC protocols like S-MAC and TDMAMAC have been created to save energy. Because battery-dependent sensor nodes, energy is a finite resource. Recharging or replacing batteries is expensive and may not be possible in certain instances. WSN applications thus have to be very energy-conscious. The information should be transferred from one node to another through a communication channel and an application protocol in wireless sensor computing. One characteristic of WSN is the ability to communicate in the real world through wireless and sensor nodes to detect and control anything specific. Any of these nodes must work together to achieve their goals. On line connections between the o-one and one node through wireless connection enable the connection and shared operation of the Wireless Sensor Network (WSN). They may operate under highly dynamic circumstances, such as combat and surveillance. Since WSNs are self-employed, many distinctive attacks are seldom overlooked. WSNs have lately gained a significant lot of attention in the military and civic contexts due to their widespread adoption. WSN is usually used in underground and frequently unfavorable locations, such as military and domestic intelligence. In order to maintain the integrity of netbook, authentications are needed that meet the overall aims of convenience, data privacy and confidence. Artificial intelligence technology has been used in the world today, and numerous artificial intelligence devices and protocols are used for various purposes. In wireless sensor nodes, artificial information agents and protocols play a significant role.

A. Sensor nodes

The sensor nodes are used to control network assignments. While the Task Manager may include measurements and queries, data may be sent through sensor nodes, depending on these ways. Calculations may be done with a node depending on the system needs if the model is built. It may either send data to the other nodes or it can be sent to the Task Manager as it is. Either in the sensor nodes: how to find out how to obtain it. The globe is thus the source. A gadget that receives data from a sensor is called a sink or an actuator.

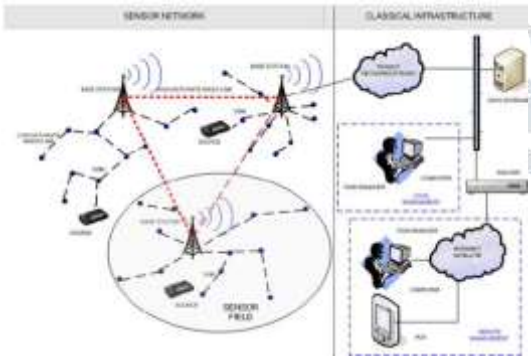

Fig. 6: Illustration of sensor network and peripherals

1.5 Sensor Network Model

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

(a) The sensor network is static, the sensor nodes not moving; even if dispersed or fixed with an antenna, each node knows its own position. If not, via the placement process the nodes will have their own location.

(b) Computing, networking and power tool nodes are comparable to current sensor nodes, such as MICA Berkeley. We suppose that every node is able to store up to a hundred bytes of core material to provide symmetrical encryption of information transfer.

(c) The base station, also known as an input point, which serves as a master and server controller, is a laptop, with long-term energy supply. We thus presume that it will not impact the base station.

(d) The wireless cellular network design is our emphasis (WCN). A number of base stations were previously constructed in this design. A cell is formed around it that covers a part of the area of each base station.

II. REVIEWOF LITERATURE

Roy et, al. (2020). In the following article, the limited mobile pelvic activity is also considered, since MS ends at a limited number of residential sites and all nodes transmit data from adjacent residential areas. A block-based routing protocol aimed at retaining the strength of the sensor nodes to enhance the network's existence accomplishes the information sent to the resident site. Additionally, extending the presence of the coverage is equally important for many WSN-sensitive coverage projects as is network life. **Fotohi & Bari (2020).** There are numerous nodes in Wireless Sensor Networks (WSN) whose major responsibilities include monitoring and controlling ecosystems. The sensor nodes are also dispersed depending on the use of the network. Consumption is the major problems of the network. Closing knots serve as a data transmission route for other nodes to sink in fixed basin networks. The repeating neural network also monitors movement performed surroundings. Simulated findings demonstrate the superiority of the WSN-FAHN approach, compared with current systems that assess the mean network useful for reducing average residual capacity. **Zhu et al. (2019).** This article describes and analyzes the cause and description of the network errors of wireless sensors, which focus on national and global failure diagnostics. The main site techniques are utilized to develop centralized approaches and algorithms. Finally, potential research and development problems are addressed in connection with sensor network failures. **Sharma & Lobiyal (2015).** Each node monitors the circumstance inside a widespread sensor network and transmits it to a particular party through multi-CNN connections. In the event of power gaps in the wireless network, the required extra data transmittance control packages are dealt with in the presence of performance protocols AODV, DSR and TORA. Costs with various node density were indicated for each protocol. The effectiveness of some of the popular techniques was employed to reduce this problem and simulation results were used for study verification. **Rai et al. (2017).** The growing demand for wireless sensor applications is one of the most significant problems in wireless sensor applications for service quality. Wireless Sensor Networks are very difficult to maintain operational standards, because there are numerous limitations on the tools available for different sensors and applications in these networks. Traditionally a network focused on latency, efficiency and volatility metrics. **Anastasi et al. (2010)** They focus in this paper on the IEEE 802.15.4 WSN and argue that they may have a substantial reliability problem. This problem arises when the power management method permits energy saving and resulting in a very low packet delivery rate, and also when the number of sensor nodes on the network is extremely low (for example, 5). To investigate the underlying causes of the issue using simulations and testing on a genuine WSN, it is caused by the MAC protocol used for the channel access and the default parameter values. They also found that the problem can be minimized and the delivery rate reached by defining more acceptable MAC settings at least in the scenarios addressed by this study is up to 100 percent. Nevertheless, this enhancement increases cost and may frequently lead to sufficient strict requirements in situations when expressly allowed. **Khan et al. (2013),** This study aims to investigate how different topological

designs affect PDR and absolute delay in wireless sensor networks. This study also analyzes the output of three different network topological topologies for mission-critical applications. Three alternative topological designs were used to assess the efficiency of the sensor nodes: linear, level 1 and divided level 1 (WSN). **Sunitha, & Chandrika (2016),** In the era of networking, wireless sensor networks play a crucial role. The exponential development of connectivity technologies allowed the wireless network of sensors to spread more rapidly with a high number of sensors on the network. Due to the mobility of sensor motes, many risks are generated to maintain the dependability and protection of the network. Data mining is also a thriving technology in the area of data production; different preprocessing of data, data interpretation and data mining policies and techniques such as data aggregation, correlation, grouping and prediction are advanced. Several researchers nowadays are faced with significant issues in the wireless sensor network, including restricted capacity, processing limits, node storage restrictions, power use for each sensor, broad range coverage and protective protection. Various studies identify many algorithms, techniques and privacy procedures; however, they are not yet 100% optimal. **Singh & Dhaka (2016),** Wireless sensor networks monitor dynamic situations that change rapidly over time. This complicated activity is driven by external factors or started by the device programmers. Deep learning techniques are also used by sensor networks to eliminate the need to revamp these circumstances. Machine learning frequently generates many practical solutions that optimize energy use and extend the existence of the network. In this document they provide a comprehensive review of the literature 2002-2014 on machine learning methods in the Wi-Fi Sensor Networks (WSN). The advantages and disadvantages of each method are evaluated against the relevant issue. They also offer a comparison reference in order to assist WSN programmers develop machine learning methods suited to their application issues. **Gupta & Pal (2016),** They describe applications for embedded networks and address the criteria that emerge from this debate. They also discuss chosen processing methods inside the Network and highlight the similarities among neural and post-propagation networks. In the context of the ad hoc network, it is addressed in the following recurring neural network s. In the ad hoc networks, the rationale and operational state of recurring neural networks are defined and the initial results produced by the use of experiments are analyzed. They argue that these models have a great potential, promising a significant impact on future research, particularly when applied as hybrid technology.

III. PROBLEM FORMULATION AND METHODOLOGY

3.1 How Packet Loss Occur In WNS

Packet loss happens whenever a packet is concurrently sent across a network by two or more nodes. The sent packets must be rejected and transmitted, which increases energy use and delay by retransmitting those packets. Attack Packet Loss is a DOS type attachment in the Data Link Layer. Packet loss happens when two or more nearby stations broadcast a packet simultaneously. This may result in packet loss and network failure. To prevent packet losses, such as the B-MAC. These protocols can minimize packet loss effectively. However, owing to concealed terminal issues and packet loss, all packet losses cannot inherently be deleted if multiple nodes simultaneously feel media free. In addition, packet loss is significantly impacted by WSNs. Loss of crucial control data from base stations may lead to the loss of packages and failure of applications.

3.2 Role of Recurrent neural network in WSN

Although recurring neural networks and sensor networks are generally regarded as two completely distinct topics, one element is similar. A one-to-many communication, specifically broadcasting, to all nodes within its range. The suggested calculation time paradigm applies to networks where broadcasting is a basic communication, such as brain biology or wireless telecommunications networks. The computation of the capabilities suggested by et al. who discovered that analog data could be stored in action potentials of firing periods and timing of actions may be utilized to conduct a support vector method is another example of such a paradigm. There was no particular need for the capacity to communicate on broadcast. At specific times, the neuronal characteristic is to be achieved. The first neuronal fire thus happens spontaneously when the neuron's property variable is compared to the minimal value. Instead of overlapping the method, a winner with the required optimality must be chosen.

3.3 Feed Forward Back Propagation

ANNs are biologically based computer programs that mimic how human brain information processes. It is a powerful method to establish a complicated, nonlinear connection between a number of inputs and outputs. The power of the computer comes from a network connection. Each neuron weighs inputs, simulation functions, transfer functions and output. The weighted sum of inputs reflects the function of neural activity. An activation signal is transmitted via a transmission function that adds non-linearity and generates output. During the training phase, interconnections are optimized. The test output will be computed using fresh unseen input information once the network is trained. In the recurring neural network, various back propagation techniques are utilized but mainly the retrospective neural network feedback (FBNN).

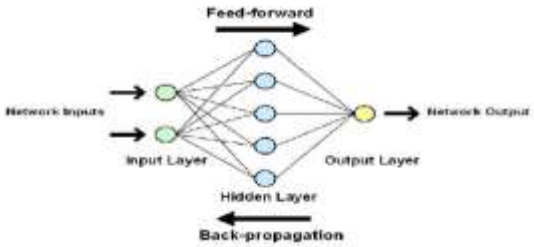

Fig. 7: Simple two-layer feed forward back propagation recurrent neural network

There are often three levels in a basic two-layer feedback network.

3.4 Recurrent neural network

Weight network. Weight network. The network nodes are huge simplifications for real neurons, which can only be triggered or not in one of two possible states. Node modifications are always set aside and on appropriately. The initial settings are the number of units and the degree of activation (V0, V1, V2...Vi). The network behavior is determined by an appropriate energy function. This function is based on the neural state, weight and bias value from issue data. The neuron updating rule is based on the energy function.

3.4.1 Network Applied to The Single Sensor Node

Wireless communication often suffers from poor channel conditions. This has to handle incorrect or even missing data packets using algorithms or other methods such as retransmission. HN shows promising characteristics such as associative memory, strength and the capacity to rectify mistakes in this environment. Associative memory does not save

a single neuron pattern but a network feature. The weights inside HN thus preserve the average correlations between all the components created. The provided network may then reconstruct the whole model with a partial or distorted pattern with correlations. As in the case of HN itself, it is robust. The HN is a fully linked one-layer feedback network without direct feedback connections, so that every feature displays the sensor input pattern received from three sensors, as illustrated in Figure below. After repeated processing, the optimized, i.e., completed or corrected pattern may be used to produce the data packet shown with a dashed box.

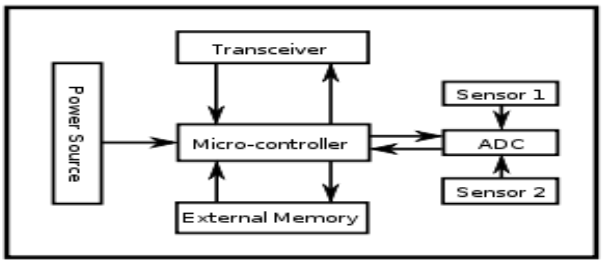

Fig. 8: The network applied to the single sensor node.

IV. SIMULATION & RESULT

The parameter was placed in a MATLAB code and simulated many times. The PDF, E2E, and throughput were calculated at the MATLAB command line. The MATLAB code may also compute this. However, this requires an enormous time and self-insertion of the test condition. The result may change, but the substance of the result remains the same. The simulation via the built GUI follows.

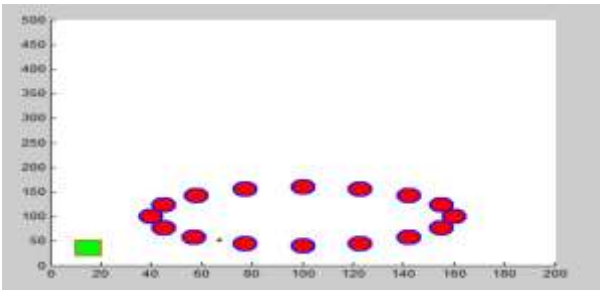

Fig. 9: Layout for WSN – CNN

The GUI was built in MTALAB-2013. Since we have a topology of the elliptical nodes and two sink nodes that serve as a base station.

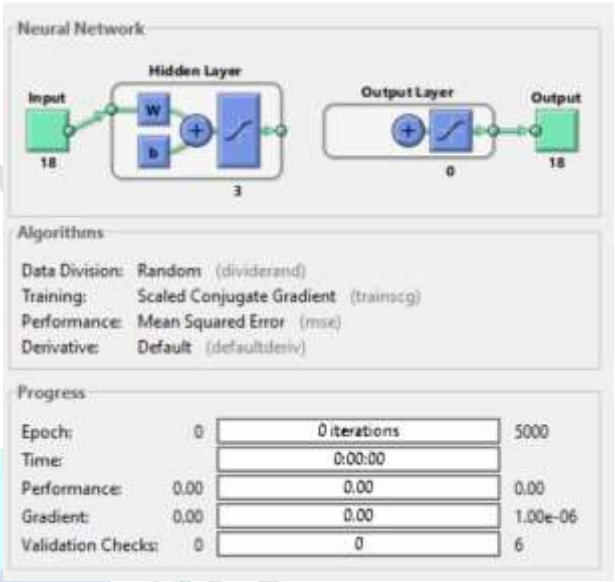

Fig. 10: Status of neural network (CNN Neural Network)

The above is the Competitive neural network that applies over WSN nodes and network parameters. By which the packet state may be assessed.

4.1 Result -FFBP

Table 1: 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

The previous model used the feed forward back propagation techniques in the estimation of packet loss may be evaluated in Packet transmitted, Packet drop PDR, e2edelay, Throughput format. This option was related to the QoS network.

4.2 Result – CNN

Table 2: CNN

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

The previous model used neural network techniques to estimate the packet loss may be calculated as a Packet Transmitting, Packet Drop, PDR, e2edelay, Throughput.

Table 3: Throughput of FFBP and CNN

S. No.	Throughput-FFBP	Throughput-CNN
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**

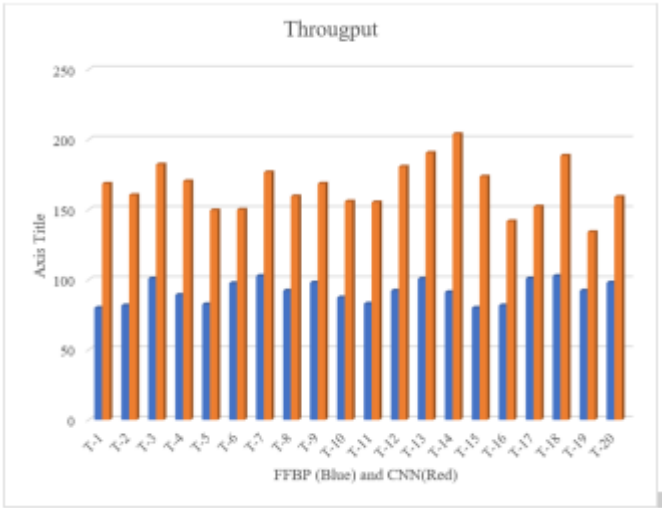

Fig. 11: comparison between throughput of FFBP and CNN

The following table was produced after a table and graphical comparison was conducted for the WSN simulation suggested

for 20 rounds of communication and performance for FFBP and CNN.

Table 4: comparison between PDR of FFBP and CNN

S. No.	PDR_FFBP	PDR-CNN
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

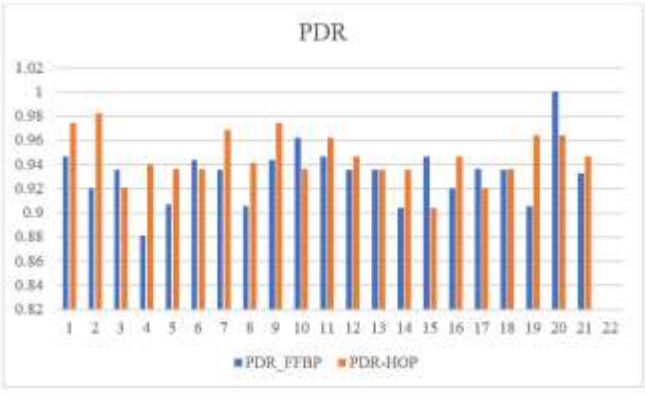

Fig. 12: comparison between PDR of FFBP and CNN

The following table was produced after the simulation of WSN during the 20 communication rounds and comparisons were made in tabular and graphical terms of FFBP and CNN PDR.

Table 5: comparison between e2e delay of FFBP and CNN

S. No.	e2edelay-FFBP	e2edelay-CNN
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

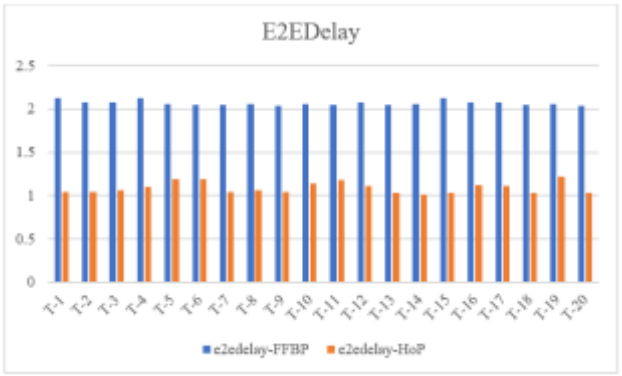

Fig. 13: comparison between e2e delay of FFBP and CNN

The above-mentioned table was produced following the simulation of the WSN suggested in the 20 communication rounds, and the comparison of FFBP and CNN was carried out in table and graph.

4.3 Compare Results

Table 4. 6 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

As can be seen in the comparison above, the present model has been utilized to estimate the loss of packets using a neural network, as recommended by the model, in order to estimate the loss of packets. Methods for calculating the number of trails has been developed that use Feed Forward Back Propagation (FFBP). This thesis used a total of 20 different trails to get the WSN estimate.

V. CONCLUSION AND FUTURE WORK

WSNs are distinguished by the flexibility of their network forms and the mobility of their sensors. This dissertation looks at network transmission rate, latency, and packet transfer. To send packets, a jump field neural network is used. When the background propagation results are compared to the CNN transfer rate, throughput is increased while end-to-end delays are reduced. There is also discussion of methods for recovering from wireless sensor network congestion. Machine learning technologies may be used in the future to prevent packet loss through iteration. Before delving into the research requirements, this article provides a general overview of embedded network applications. We contrasted the neural CNN network with the back propagation network, emphasizing the physical similarities. The sensor network could expand. The following neural network adds a new context. The current model estimates packet loss using Feed Forward Back Propagation, whereas the proposed method employs a neural network and estimates the number of many trails more accurately. The WSN estimate in this thesis was derived from 20 traces. In this context, the explanation of neural network viability in a sensor network setting, as well as the assessment of early findings from our testing, are critical. To predict the outcomes, terms such as packet, packet drop PDR, e2edelay, and performance may be used. These metrics are used to assess the network's service quality (QoS). The final result of this thesis is superior to existing techniques. More sensor nodes allow for more topologies to be tested and simulated. Using recurrent neural networks with high iteration values to identify packet dropouts may be a better solution to WSN test randomization than the current options. The first seven GUI tests displayed and suggested it seven times, which corresponded to the intended study's conclusions. The degree of certainty is calculated using data from nearby sensor nodes that are geographically and temporally linked. (2) The Trust Model was developed in order to compute the number of interactions between trust, distrust, and uncertainty, as well as the direct and indirect trust values. A simple synthesis method is then used to assess the network's overall confidence in detecting rogue nodes. As a result, it's worth has nearly tripled year after year. The success of the trial will also help the VANET situation, which is being improved by 5G technology. This is a platform for WSN sensors that collects data primarily through 5G communication technologies.

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.