A Novel Method of Responsible Multi-Path Transmission Based on Energy Efficient Flag Model with proficient Data Transmission

A.Kamalraj[1], G.Angeline Prasanna[2]

[1]Research Scholar in Computer Science, AJK College of Arts and Science, Email: Kamalraj.asvk@gmail.com
[2]Former Associate Professor & Head, Department of Computer Science, AJK College of Arts and Science, Email: drgangelineprasanna@gmail.com

Received: 10.04.2024 Revised : 18.05.2024 Accepted: 29.05.2024

ABSTRACT
Wireless Sensor Networks (WSNs), this study suggests a multi-path routing technique that uses less energy. The main constraints that restrict the lifespan of sensor networks are the low battery life of sensor nodes and ineffective protocols. The goal of this research is to create a more effective routing system that might be applied to wireless sensor networks. The most noteworthy achievement of the proposed protocol is the use of fixed clustering and the reduction of unnecessary overhead often found in most routing protocols by using idle CHs and fixed CHs to minimize the number of cluster head changes. This paper describes the acceptance of the sans flag concept and introduces the concepts of data transfers with no flag, flag 0 and flag 1. According to the performance analysis, reducing overhead significantly lengthens sensor node lifetime because energy-efficient protocols can reduce sensor node energy consumption. Consequently, a wireless sensor network's scalability can be improved. Additionally, the usage of relay nodes improves network energy dissipation.

Keywords: Wireless Sensor Network, Multi-Path selection, Secured Data Transmission, Energy Efficiency Model, Network Lifetime.

1. INTRODUCTION

In WSNs, sensor nodes sense the surrounding environment and subsequently transmit the data sequentially to the networks. After that, a number of wireless nodes relay the data, sending it all the way to the original node. Two main issues with data transmission over the Internet when using wireless sensor networks (WSNs) are energy saving and stable routing. [1].

In contrast to traditional wired networks, wireless sensor network technology is widely used in the military, environmental monitoring, security monitoring, and other fields. Its deployment is more flexible and less expensive in a variety of unwired monitoring environments. Many thousands of sensor nodes are deployed on a wireless sensor network (WSN) using batteries; these nodes are often dropped from an aircraft to the monitoring region, making it impossible to change the sensor's battery.

Data transmission's primary issue is its high energy consumption and network overhead. Thus, in the changing sensor environment, a good routing protocol should provide transmission stability. Remaining energy, hop count, and link quality are used to calculate network stability. These features are employed to reduce the network's excessive energy usage and preserve network stability [2].

One of the most important considerations when using a wireless sensor network is optimizing the network's efficiency. In a wireless sensor network, information is sent from each mote to its cluster head, which subsequently forwards it to the base station. Greater energy consumption occurs during transmission when the sensor nodes are spaced apart, and interrupted energy consumption can result from direct transmission from the mote to the base station. A cluster is a collection of mote in a certain sensor network. The motes are grouped into several groups or clusters based on the data that the mote is supposed to sense if the network is very big. When a network is clustered, all of the data gathered by the mote is transmitted to the cluster head, which then forwards it to the base station [3].

A wireless sensor network (WSN) is a network system made up of geographically dispersed devices that use wireless sensor nodes to keep an eye on environmental or physical conditions like motion, sound, and temperature. A message authentication code is a brief piece of information used in cryptography to verify the authenticity and dependability of a communication. While accuracy assurances confirm the message's origin, integrity declarations identify unintentional and deliberate message modifications. Since the

message sender and the recipient must exchange a secret key, the symmetric key based solution is not scalable and is not resistant to large-scale node compromise attempts [4]. The dispatcher creates a message authentication code (MAC) for each transmitted communication using the shared key. However, with this method, the node possessing the collective key is the only one able to confirm the message's authenticity and integrity. It is possible for an intruder to negotiate the key by seizing a single sensor node.

Routing systems that synchronize the trade-off between a node's minimum energy consumption and stability must take these measures into consideration. These metrics are residual energy and node stability [5]. Many network architectures, including ad hoc networks, mobile ad hoc networks, and Internet border gateway routers, have issues with unstable routes. One of the main issues facing WSNs today is route stability. As multihop networks become more unstable, routing loops and imbalances in energy usage occur, which negatively impacts overall performance. In wireless sensor networks (WSNs), stability is a valuable parameter for assessing routing algorithms. It implies that network stability affects the design and execution of routing tasks such energy consumption minimization and aggregation. Route restoration is necessary for additional stabilization activities.

2. Review of Related Literature

Three components make up the data transmission technique that Fengyong et al. proposed: data ensemble recovery, data delivery, and data deconstruction. Using a matrix decomposition process, the first perceived data can be divided into several data shares in the first section, which is directed towards each sensor node. The subsequent sensor node receives these shared data in a sequential manner. Every data exchange is supplied into intricate sensor networks in the second section. They might block noise, interfere with the channel, or cause a sensor node malfunction, which could cause some data to be delivered lost or damaged. In the third section, we build an ensemble method based on shared data that can restore the original perceived data, even in cases when the received data is heavily corrupted or involves a lot of digital hopping.

In WSNs, sensor nodes sense the surrounding environment and subsequently transmit the data sequentially to the networks. After that, a number of wireless nodes relay the data, sending it all the way to the original node. The receiver (computer or processing center) at the source node reconstructs the original data in a predetermined order. Regretfully, during transmission, these perceived data could be targeted or compromised by issues including network noise, channel interference, or sensor node malfunction. Assuming that the source node can receive the data precisely and completely in this instance would be unrealistic. Because perceived data is incomplete when it is lost, there could be major issues. Researchers have experimented with a variety of interpolation techniques, but the problem of incomplete and inaccurate perceived data remains challenging to resolve [05].

Uras et al,outlines a four-stage security level (FS-SSL) for Zigbee networks based on various application security needs, including elevated BER or user demands. The data is usually sent to the physical layer to be transmitted across the network once it has been encrypted at the application layer. In this instance, the data is encrypted at the MAC layer rather than being sent to the application layer for further encryption in the event of network expansion or user request to modify the encryption technique.

In addition to extending network lifetime, BER reduction lowers node energy usage. The network status (traffic volume, level of security, etc.) presents the greatest opportunity for a user to choose a different encryption technique at the physical layer. AES offers the highest level of security; if there is a BER drop at the physical layer, the system will encrypt to an algorithm with a lower weight as defined in the weight table. The user or the system can dynamically choose one of the lightweight block cipher algorithms based on the desired security level by using reserved bits of the frame control field in the Zigbee MAC header.

To enable the user to select one of the five modes, the authors exploited reserved bits (9–12–13 bits) of the frame control field. There are two ways to access these modes: either by the user via the attribute menu (by adding C code) for every node in the Riverbed Modeler network simulator, or dynamically in the event of a BER drop by the system (Cross-layer). Based on the results of our simulation and parameters like computed throughput and energy consumption, the weight of each algorithm in the MAC layer through reserved bits was determined. Five modes are available for selection by the user [06].

Marcin et al, The goal of the suggested approach was to minimize data transfers between nearby sensor nodes that work together to identify events. This technique can be used in conjunction with threshold-based event detection algorithms, machine learning, periodic or adaptive sampling, and more. By considering the utility of sensor readings for a certain event detection job, it greatly expands the concept of dual prediction. The suggested method does not employ prediction error to determine whether the sensed data must be communicated, in contrast to the dual prediction system.

This approach, on the other hand, checks to see if the anticipated facts are accurate enough to identify the relevant occurrences. The investigated wireless sensor network's goal is to identify spatial occurrences that cause values from nearby sensor nodes to deviate. There are parent and child nodes in a wireless sensor network. A parent node receives the sensor readings from the child node. The parent node's job is to identify events by combining sensor readings from the child node with its own sensor readings. The parent node notifies a base station when an event is recognized. [07].

Shuiyan et al, After clustering, create the best hybrid routing possible from each cluster head to the sink. The transmission inside a single cluster is one-way direct transmission, which means that the nodes within the cluster send the gathered data to the cluster head directly over one hop in order to simplify the algorithm. The cluster head must move the data to the sink after it has been collected within the cluster. Several researchers frequently utilize the following four tactics: (1) The cluster heads send Sink the gathered data straight over a single hop. (2) The Sink creates a multi-hop routing to the cluster heads using the greedy technique, and the routing only contains cluster heads. (3) The multi-hop routing to the cluster heads is created by the Sink using the greedy method. The routing only contains non-cluster heads; all cluster heads are deaf nodes that are never again utilized as relay nodes. (4) The best route from the cluster head to the sink is created via hybrid routing. Relay nodes can be created from cluster heads or non-cluster heads nodes [08].

Jogendra et al, This work is a development of reformist control that displays all affiliations allocated to various social affairs. Every pack adheres to the driving standard. In essence, Group Heads (CHs) are central figures who can assist BS with bundling and controlling. By regulating the energy-efficient information transfer from source to target, this lowers the significant division transmission overhead of standard points that must be sent to nearby CHs. Another problem in WSNs is transmission delay when applications such as those used by clinical organizations need time-sensitive information. Examine the energy-able presentation and follow careful planning guidelines to increase energy consumption.

They investigate the several approaches to reduce the transmission latency for time-basic and open applications. Subheadings that follow look at a few reformist planning shows in detail. The Medium Access Control (MAC) protocols used in WSNs are transparent, low force, and able to convey information with unfathomable accuracy. In order to meet the different requirements, such as energy capability, bundle disaster, and transmission latency, several MAC processes were reviewed and investigated. In the present location, the evaluations and the indisputable advancements of the suggested computation to be expressed as Proposed-LEACH are discussed [09].

Lin et al, A wireless network made up of sensor nodes is called a wireless sensor network (WSN), and it is extensively utilized in the industrial, military, and agricultural domains. In these real-world application scenarios, the problem of a relatively short network lifecycle arises from the restricted routing search capability of wireless sensor nodes and the small coverage range of a WSN. As a result, expanding a WSN's coverage area and lowering node energy usage are highly valuable. This article suggests a technique for determining a WSN's best routing using the ant colony algorithm (ACOD), clustering data using the K-means algorithm, and extending a WSN's coverage range using the whale algorithm (WOA) and a back-propagation (BP) neural network.Following several tests, the WSN's coverage area has grown, its lifespan has been prolonged, and its overall energy consumption of nodes has been significantly decreased [10].

Amir et al, Because the authors' metaheuristic algorithms naturally fit the problem suit and have a balanced behavior, they were employed as the problem-solving methodology in this research. Several methods based on metaheuristics have been used to comparable systems, as the literature section explains. Although metaheuristic-based approaches are known to not always yield optimal results, they do strive to identify solutions that are near to the ideal, resulting in more effective execution times and CPU power usage in terms of both time and space complexity.Every metaheuristic approach that has been suggested in the literature has benefits and drawbacks. In order to provide thorough and precise techniques that can be applied in WSN and DIoT, this study focuses on wider factors.

A novel fitness function has been defined as a result. The formed neighbor list of each node, residual energy, traffic status, buffer rate, and BS-hop are all included in the established fitness function that is used to determine the cost of every link in the network. The hop counts of every node to BS are shown by BS-hop. It is assumed that BS is the destination node in this investigation. In order to determine the best path (between each node and itself), the BS node considers other useful factors that are specified in the new fitness function in addition to the distance or number of hops that each node makes in relation to itself.It considers the network's changing parameters as well as the dynamic resources of the system's nodes. A new fitness function is defined with this objective in mind. Hop values are used to select the pathways between the source and destination nodes, which are then run through the fitness function. [11].

3. METHODOLOGY

3.1. Methodology Design

By using the route provided by the cluster head, or CH, the proposed model is an enhanced design that finds the shortest path with the most energy-efficient means to transfer data from the source to the destination. The cluster head selection procedure will announce the CH in accordance with the guidelines given in 3.2.1 as soon as the source node sends out a request for data transmission. As illustrated in 3.2.2, the CH will choose the fastest path and create a data transmission link with high energy level nodes when it is proclaimed. The data will be transferred from the source node to the destination node after the CH has been chosen and the data transmission path has been established [12]. The information relevant to data transfer in the proposed paradigm was illustrated in Figure 1.

Three sets of transmission data: zero with no flag, one with a flag, and one with a flag. In order to preserve the integrity of the data during transmission, these flag concepts were included in the suggested model. Any type of active node can be used to transmit this data if the data transmitted without the flag indicates that there is no risk involved. Without a flag, the transmission data is shown in Figure 2. Only active nodes with more than 25% energy can be utilized to transmit data if the data communicated with flag 0 indicates that the sending data has a moderate risk. Flag 0 transmission data is shown in Figure 3. Only active nodes with more than 90% energy can be utilized to transmit data if the data communicated with flag 1 indicates that the transmitting data has a high risk. With flag 1, the transmission data is shown in Figure 4.

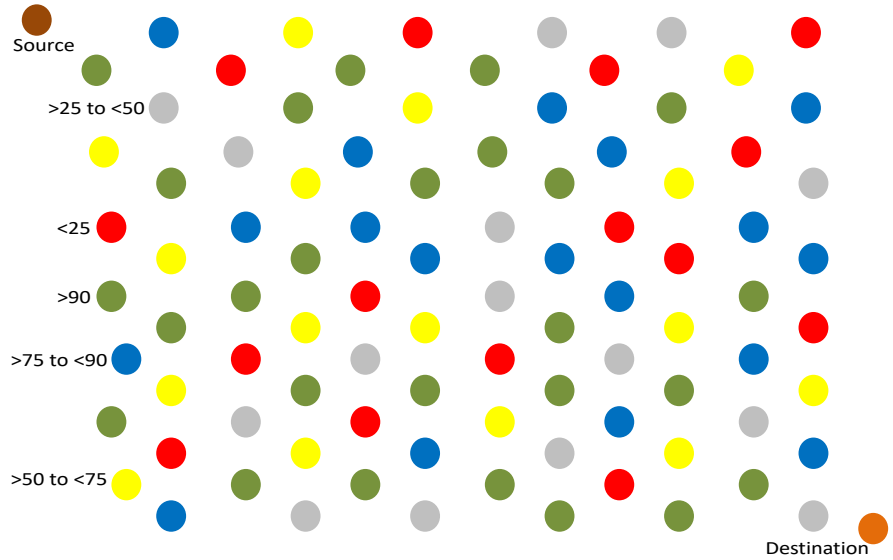

Figure 1. Proposed Methodology Design

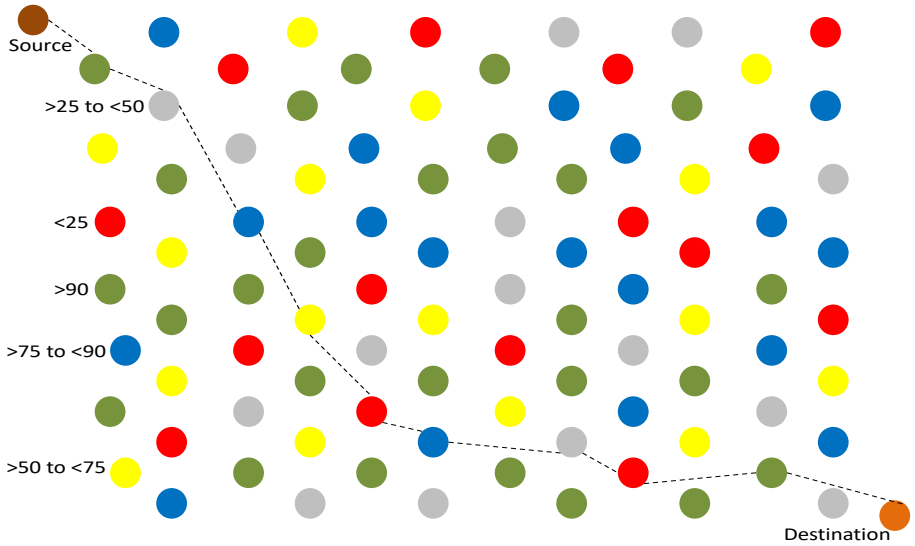

Figure 2. Proposed Methodology Design with Flag 1

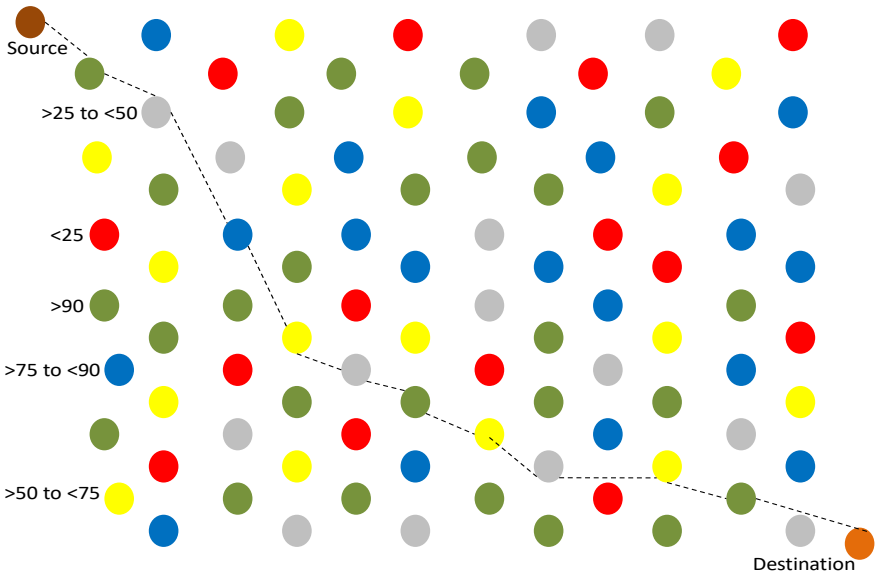

Figure 3. Proposed Methodology Design with Flag 0

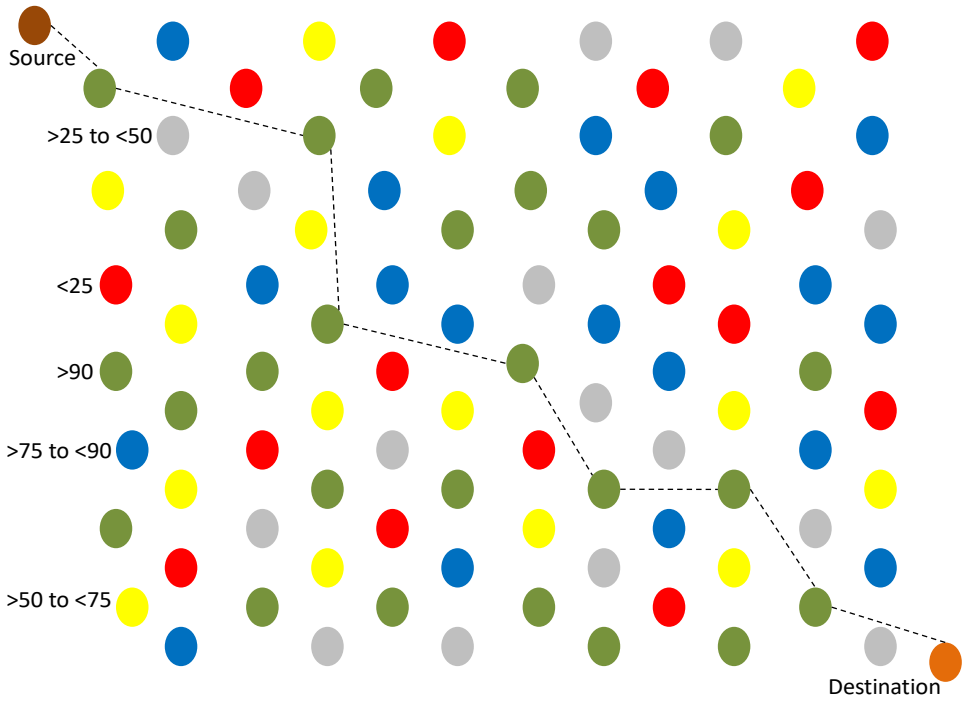

Figure 4. Proposed Methodology Design without Flag

3.2. Procedure

3.2.1. Cluster Head Selection Algorithm

Begin
Search for the nodes
Choose the >90 energy level nodes
Encircle the nodes with up to 25 nodes
Select any three nodes randomly which are having >90 energy level
Declare any one of the node from three nodes as CH
Idle the remaining two nodes as idle CH
Fix the selected node and declared it as CH
If the CH crashed due to any reason
Pick and Fix the highest energy contain as next CH from the idle CH
End

3.2.2. Routing Algorithm

```
Begin
    Source node identifies the data type without flag, flag 0 or Flag 1
    Source node forwards the request message to active CH for data transmission
    CH verifies the available nodes status with highest energy level
    CH analyze the available shortest route to reach the destination with highest energy level
    Detect the paths to reach the destination
    If more than one path is identified
        If the data type without flag1
            If more than one route is available with each node having >90% energy then
            selects any one of the route randomly with all the nodes having >90% energy
            Then
            Fix the available any one route randomly as default route to send the data
        If the data type without flag0
            If more than one route is available with each node having >25% energy then
            selects any one of the route randomly with all the nodes having >25% energy
            Then
            Fix the available any one route randomly as default route to send the data
        If the data type without flag
            Check the energy level of the nodes and then sorted it based on overall energy
            level
            Then
            Fix the available any one route randomly as default route to send the data
    Set the path as default path which was received from CH
    Instigate the data transmission
    Verifies the data transmission end with the source node
    End the transmission
    End if
    End if
End
```

3.3. Comparison Metrics

3.3.1 Average Latency

Network latency is a well-known barrier to communication between sets of connections. It shows the time it takes for data to move between a collection of connections. Squat latency networks counter quickly, while high latency networks have a greater barrier or lag. When calculating the typical latency of information communication from the resource to the target node, the amount of time that needs to elapse between starting at the source and arriving at the destination is taken into account. It is crucial to minimize the delay period as much as possible.

3.3.2 Packet Delivery Rate

The PDR is the total number of packets that are efficiently sent to the intention node that is alienated by all of the packets that were sent in the first place. Divide the entire number of packets sent by the total number of packets successfully received to find the packet delivery rate. Then, multiply the result by 100 to get a percentage. A standard routing protocol needs to show that the packet delivery ratio is both reasonable and as high as is practically possible.

3.3.3 Packet Loss Rate

The packet loss rate is defined as the total number of packets transmitted minus the total number of packets received over a specific time period. Packet loss is usually caused by network congestion or errors in data transfer. The packet loss rate, expressed as a percentage, is the quantity of packets lost relative to the total number sent.

3.3.4 Energy Efficient Analysis

The planning, configuration, and upkeep of network infrastructures and protocols with the aim of reducing the energy consumption of data centers and network devices is referred to as energy-efficient networking. A device's energy efficiency can be assessed and established by comparing the productivity it generates with the amount of electricity it consumes during manufacturing. An estimation of the power

use of the sensory nodes is made based on the duration of the simulation. The amount of energy expressed in joules that is still available in the sensory nodes after a predefined number of instances.

3.3.5 Network Life Time Analysis

The term "network lifetime" refers to the amount of time that passes between the deployment of a network and the point at which it ceases to function (for instance, when a specific number of nodes fail or the network divides).

If the overall outstanding power level in the set of connections is more significant than the power collapse in a single node, the lifetime can be defined as the total outstanding power of all the nodes in the set of connections.

The definition of network lifespan determines the most effective strategy to improve energy efficiency. The lifetime of the network is evaluated with respect to the duration of its simulation. As the lifespan of the sensor rises, the set of connections will have more time to function as planned. When all of the nodes that have been active throughout a certain period of time are added together, the life span of the network remains constant. As the number of full zip nodes in the set of connections grows, so does the lifespan competency.

4. RESULTS AND DISCUSSIONS

Table 1. Average Latency

Methods	0	25	75	125	175	200
CS	16	19	23	24	25	26
CS+HS	11	13	15	17	20	24
FR	8	9	10	11	15	16
RP	6	8	9	10	11	12
Proposed I	5	7	8	9	10	11
Proposed II	5	6	7	8	9	10

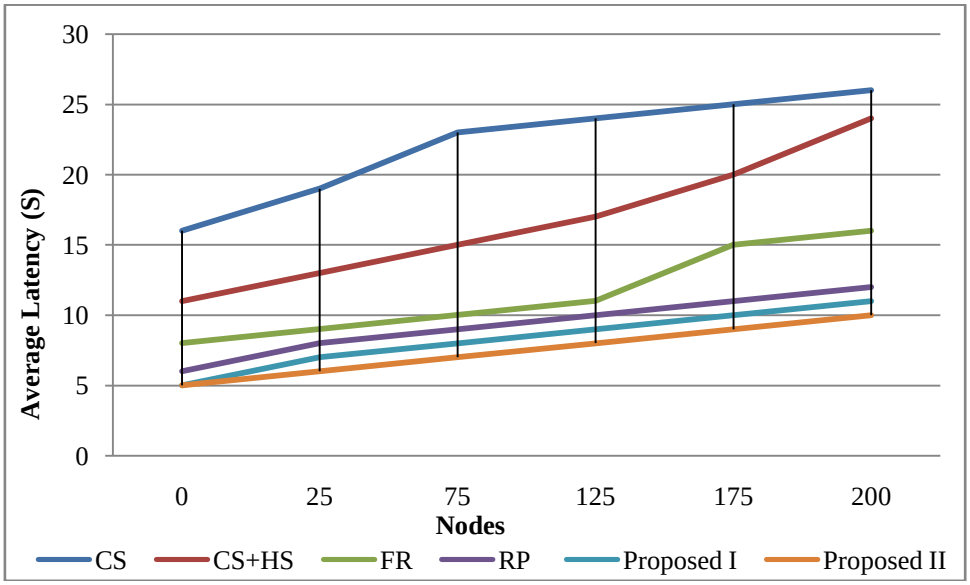

Figure 5. Average Latency

Table 2. Packet Delivery Rate

Methods	0	25	75	125	175	200
CS	100	88	87	87	86	81
CS+HS	100	94	92	91	89	86
FR	100	98	96	94	93	91
RP	100	99	97	96	95	94
Proposed I	100	99	98	97	96	95
Proposed II	100	99	99	98	97	96

The comparison between the projected representations and the previously published model for average latency is shown in Table 01 and Figure 02 of the document. It illustrates how the projected representation outperforms the previously described approach in terms of average latency.

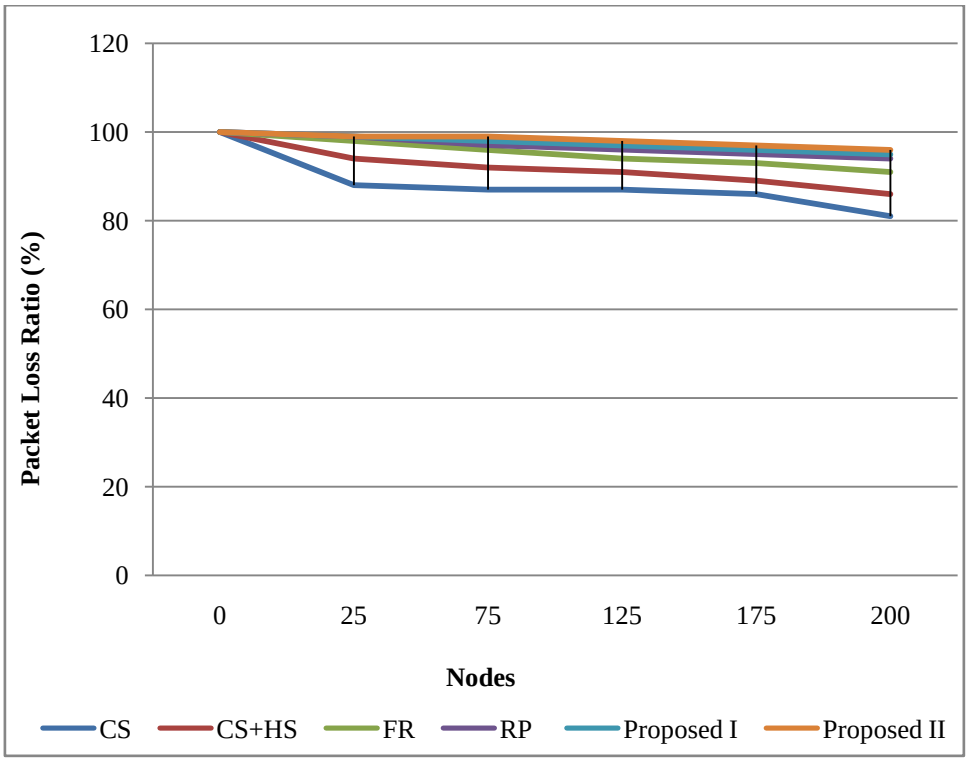

Figure 6. Packet Delivery Rate

Table 3. Packet Loss Rate

Methods	0	25	75	125	175	200
CS	0	12	13	13	14	19
CS+HS	0	6	8	9	11	14
FR	0	2	4	6	7	9
RP	0	1	3	4	5	6
Proposed I	0	1	2	3	4	5
Proposed II	0	1	1	2	3	4

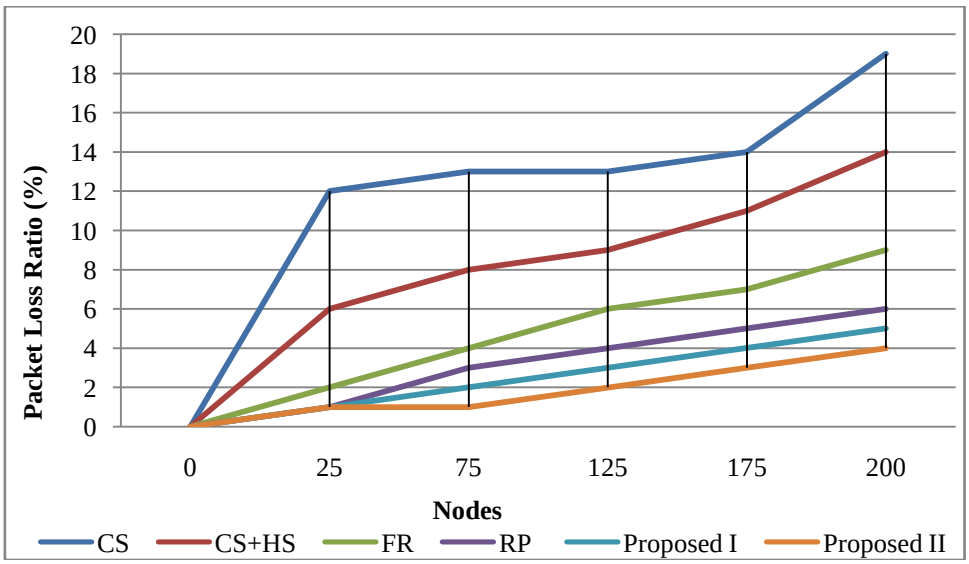

Figure 7. Packet Loss Rate

The comparison of the projected representations with the PDR model that has already been provided is shown in Table 02 and Figure 3. It shows that the method in the packet delivery rate that has already been presented is inferior to the predicted representation.
Table 03 and Figure 04 show how the projected representations and the previously available Packet Loss Rate model compare. It shows that the proposed representation outperforms the previously described approach in terms of packet loss rate.

Table 4. Energy Efficient Analysis

Methods	100	150	200	250	300	350	400	450	500
CS	0.4	0.41	0.43	0.45	0.48	0.52	0.57	0.6	0.7
CS+HS	0.3	0.35	0.39	0.45	0.47	0.5	0.51	0.53	0.55
FR	0.1	0.13	0.15	0.17	0.24	0.27	0.29	0.3	0.32
RP	0.1	0.11	0.13	0.15	0.22	0.25	0.27	0.28	0.3
Proposed I	0.1	0.1	0.11	0.14	0.2	0.22	0.24	0.26	0.28
Proposed II	0.1	0.1	0.11	0.12	0.15	0.18	0.2	0.22	0.25

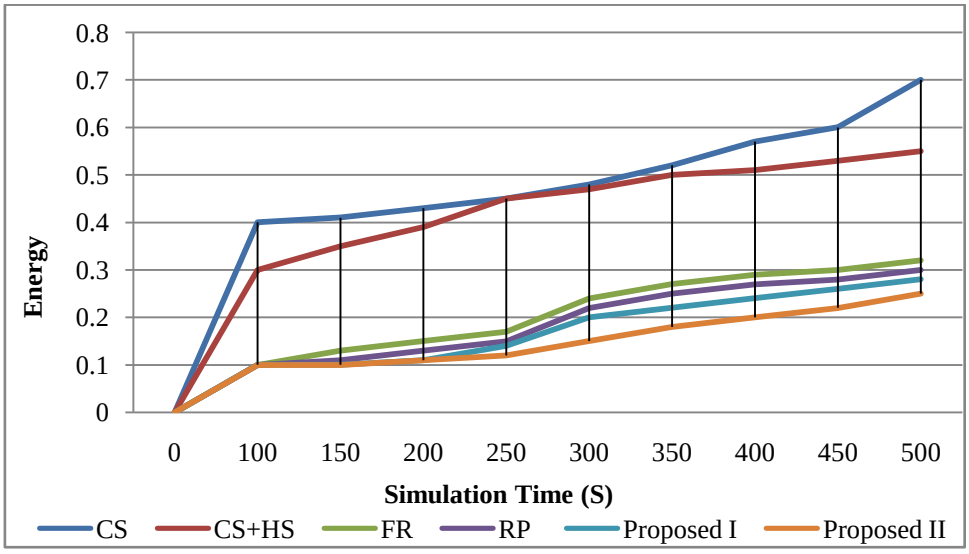

Figure 8. Energy Efficient Analysis

The comparison between the projected representations and the previously released model for energy-efficient analysis is shown in Table 04 and Figure 05. It proves that the proposed representation is superior to the approach that was previously provided in the Energy Efficient Analysis.

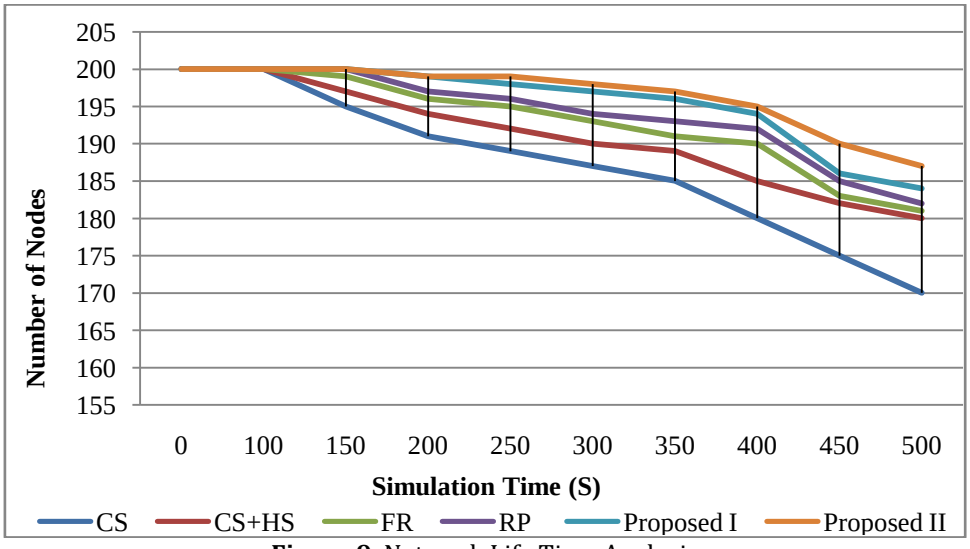

Figure 9. Network Life Time Analysis

Table 5. Network Life Time Analysis

Methods	0	100	150	200	250	300	350	400	450	500
CS	200	200	195	191	189	187	185	180	175	170
CS+HS	200	200	197	194	192	190	189	185	182	180
FR	200	200	199	196	195	193	191	190	183	181
RP	200	200	200	197	196	194	193	192	185	182
Proposed I	200	200	200	199	198	197	196	194	186	184
Proposed II	200	200	200	199	199	198	197	195	190	187

Table 05 and Figure 06 show how the projected representations and the previously released Network Life Time Analysis model compare. It shows that compared to the method previously described in the Network Life Time Analysis, the projected representation is superior.

5. Conclusion and Future Enhancement

The sensitive nature of the data to be transferred from the source node to the destination node and the path's dependability are both taken into consideration by the path selection system described in this research study. Given the severe sensitivity of some data, it is possible that it will be altered or deleted during routing. On every path, there may be trustworthy and malicious nodes.

For very sensitive data, the path with hostile nodes present is not the best choice because the malicious nodes might do unwanted things. Given this, this study proposes a path selection method that allows the user to calculate the expected energy score of the path and includes the notions of without flag, with flag 0 and with flag 1. Once again, the path that satisfies the target energy score is filtered with respect to its length. To conserve energy, a CH manages each stage of these processes. This idea conserves energy and extends the lifetime of the network. Only the data transmission without flag notion was used in this paper. In order to achieve the required level of data security, future work on this project intends to expand with different path selection models for different data transmission purposes using the flag 0 and flag 1 idea.

REFERENCES

[1] Li Yuefei and Zhang Hua, “Data transmission technology in wireless sensor network”, BioTechnology- An Indian Journal, Vol. 10, No. 15, ISSN: 0974 – 7435, 2014, pp. 8832 – 8840.

[2] Jetendra Joshi, Prakhar Awasthi, Sibeli Mukherjee, Rishabh Kumar, Divya Sara Kurian and Manash Jyoti Deka, “SEED: Secure and Energy Efficient Data Transmission in Wireless Sensor Networks”, 2016 Fourth International Conference on Information and Communication Technologies (ICoICT), 2016, pp. 01 – 06.

[3] J. Manikandan and K. Thilaka, “Secure and Efficient Data Transmission in Wireless Sensor Networks”, International Journal of Engineering Research & Technology (IJERT), NCICCT-2015 Conference Proceedings, Vol. 03, No. 12, ISSN: 2278-0181, 2015, pp. 01 – 06.

[4] Suzan Shukry, “Stable routing and energy-conserved data transmission over wireless sensor networks”, EURASIP Journal on Wireless Communications and Networking, Vol. 2021, No. 36, 2021 , pp. 01 – 29.

[5] Fengyong Li, Gang Zhou and Jingsheng Lei, “Reliable data transmission in wireless sensor networks with data decomposition and ensemble recovery”, Mathematical Biosciences and Engineering, Vol. 16, No. 05, 2019, pp. 4526 – 4545.

[6] Uras Panahi and CuneytBayilmis, “Enabling secure data transmission for wireless sensor networks based IoT applications”, Ain Shams Engineering Journal, Vol. 14, No. 101866, 2023, pp. 01 – 11.

[7] Prakash, G., P. Logapriya, and A. Sowmiya. "Smart Parking System Using Arduino and Sensors." NATURALISTA CAMPANO 28.1 (2024): 2903-2911.

[8] Marcin Lewandowski and BartłomiejPlaczek, “Data Transmission Reduction in Wireless Sensor Network for Spatial Event Detection”, Sensors, MDPI, Vol. 21, No. 7256, 2021, pp. 01 – 21.

[9] ShuiyanWu ,Xiaofei Min and Jing Li, “Optimal Data Transmission for WSNs with Data-Location Integration”, Symmetry, Vol. 13, No. 1499, 2021, pp. 01 – 15.

[10] Dr.M.Jogendra Kumar, Dr.G.V.S.Raj Kumar, Mr P S R Krishna, Dr.N.Raghavendra Sai, “Secure and Efficient Data Transmission for Wireless Sensor Networks by using Optimized Leach Protocol”, Proceedings of the Sixth International Conference on Inventive Computation Technologies, ICICT 2021, ISBN: 978-1-7281-8501-9, 2021, pp. 50 – 55.

[11] Lin Wu, Ahmad Yahya Dawod and Fang Miao, “Data Transmission in Wireless Sensor Networks Based on Ant Colony Optimization Technique”, Applied sciences, MDPI, Vol. 14, No. 5273, 2024, pp. 01 - 41.
[12] Kumar, E. B., Rajeshkumar, M., Muthusamy, A., Yookesh, T. L., &AshfaukAhamed, A. K. (2023). Predicting the Fake Review of Products Using Graph Recurrent Neural Network. International Journal of Interdisciplinary Organizational Studies, 18(1).
[13] Amir Seyyedabbasi, Farzad Kiani, TofighAllahviranloo ,Unai Fernandez-Gamiz, Samad Noeiaghdam, “Optimal data transmission and pathfinding for WSN and decentralized IoT systems using I-GWO and Ex-GWO algorithms”, Alexandria Engineering Journal, Vol. 2023, No. 63, 2023, pp. 339 – 357.
[14] A.Kamalraj and Dr.G.Angeline Prasanna, “Enhanced Trustworthy Multi-Path Assortment Based On Energy Efficient Model With Competent Data Transmission”, Machine Intelligence research, ISSN:2731-538X, Vol. 18, No. 01, 2024, pp. 1210 - 1222.
[15] Navatha, S., et al. "Multitask Learning Architecture for Vehicle Over Speed As Traffic Violations Detection And Automated Safety Violation Fine Ticketing Using Convolution Neural Network And Yolo V4 Techniques." Chinese Journal of Computational Mechanics 5 (2023): 431-435.