Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7761089

TRUST AWARE ENERGY EFFICIENT ROUTING IN WIRELESS SENSOR NETWORKS

R. Tamilaruvi1, D.Suresh2

1Assistant Professor, Department of Computer Science and Engineering Annamalai University, Chidambaram, Tamilnadu, India.

2Assistant Professor, Department of Information Technology, Annamalai University, Chidambaram, Tamilnadu, India

1tamil2party@yahoo.com, 2deiveekasuresh@gmail.com

Abstract

The Wireless Sensor Networks (WSNs) have developed to the point that they may be used as a reliable instrument for monitoring the physical environment, thanks to the rapid and historic improvement in communication technology over the past two decades. Wireless Sensor Networks are employed in crucial monitoring and tracking applications since they are made up of resource-constrained sensors. Therefore, the trustworthiness and energy of the sensor node should be taken into account by routing protocols for such networks. The former scheme designed a Fault Tolerance based Energy Efficient Routing (FTEER) mechanism for WSN. However, since the unsecure environment, the sensor nodes are vulnerable to numerous forms of attacks. The suggested system created a Trust Aware Energy Efficient Routing (TAEER) mechanism to increase energy efficiency and security to address this issue. Initially, sensor nodes are deployed randomly. Then use neighbour discovery to locate the nodes that are closest. The network's nodes each carry out at least one neighbourhood. To improve the energy efficiency, clustering is performed based on the distance and Improved Convergence Factor based Whale Optimization Algorithm (ICFWOA) is utilized for Cluster Head selection (CH). For the purpose of choosing the CH, the node parameters together with the distance, the residual energy of something like the node and its neighbours, the node weight, as well as the node's reachability are examined. In order to progress the security, malevolent nodes are detected using improved fuzzy based trust management. Finally, schedule and transmit packets using Time Division Multiple Access (TDMA). The research findings show that, in terms of Packet Delivery Ratio (PDR), energy consumption, end-to-end delay, and Average Remaining Round, the suggested system outperforms the prior method.

Keywords: WSN, energy efficiency, node trust, improved fuzzy framework, Improved Convergence Factor based Whale Optimization Algorithm (ICFWOA) and Cluster Head selection (CH)

1. OVERVIEW

WSN have been established and are being widely used as a result of recent developments in Micro-Electro-Mechanical Systems (MEMS) and low power, highly integrated electronic components [1]. Rechargeable battery pack technology uses sensor nodes that make up WSN [2-4]. These sensors are frequently dispersed at random in the field. Applications for sensor networks include battlefield administration, logistics and inventory control, energy management, medical monitoring, and emergency preparedness networks. In order to extend the WSN's existence, an energy-efficient algorithm with security is required [5].

The performance of WSNs may deteriorate and the network lifetime may be shortened due to limited energy resources. The dependability and scalability of performance in WSN become dependent on clustering [6-7]. Clusters of nodes are collections of nodes grouped according to the demands of the application and the properties of the network. Member nodes plus a unique node called the Cluster Head make up clusters (CH). The acquired data can be advanced to the CH by member nodes. The information is then immediately transmitted to a BS by CHs. To effectively optimize CH selection, however, a number of characteristics must be taken into account. As a result, the evolutionary algorithm is crucial in resolving this challenge because it has the capacity to adaptively resolve complex difficulties in polynomial time. According to the reviews, swarm intellectual ability evolutionary algorithms like Cuckoo Search (CS) and Particle Swarm Optimization (PSO) and genetically-based evolutionary algorithms like Genetic Algorithm (GA) and Differential Evolution (DE) are primarily used for CH selection.

We should think about the finest and most appropriate security strategy against adversaries in WSN due to the resource-constrained nature of these networks [9]. Sensor nodes are extremely vulnerable to malicious attacks due to the growing size of WSNs, the constrained resources of sensor nodes, and the ambiguity of the layout environment. Unfortunately, because to their high overhead in memory, processing speed, and transmission bandwidth, typical cryptographic security techniques are neither practical nor affordable for WSNs with limited resources. As a result, an alternate technique needs to be developed, and one of the best, most ideal solutions for WSNs is Trust Management in the data routing protocol.

In this proposed research work, Trust Aware Energy Efficient Routing (TAEER) mechanism is introduced for increasing energy efficiency and security in WSN. The sensor nodes are alienated into clusters in this case, and the CH is chosen using the Improved Convergence Factor based Whale Optimization Algorithm (ICFWOA) based on node specifications. In order to detect the malevolent nodes, improved fuzzy framework is utilized. Finally, Fault tolerant based routing is performed for packet transmission.

The paper is organized as shown: Section 2 shows the reviews on routing and security mechanisms. Section 3 offers a TSEER mechanism for WSN. Section 4 depicts the results and Section 5 accomplishes the paper.

2. LITERATURE REVIEW

AlFarraj et al (2018) developed an Activation Function-based Trusted Neighbor Selection (AF-TNS) to expand system safety for resource-constrained WSNs. This runs in dual segments: confidence rating with an energy limitation. This aids in maintaining the neighbours' degree of reliability. By identifying trusted and untrusted nodes to maintain network performance, it makes the complicated decision-making process of the AF simpler. According to the results of the simulation, AF-TNS increases the likelihood that malicious activity will be detected.

To find and separate malicious nodes, Yang et al. (2018) introduced Energy-Optimized Secure Routing (EOSR). With the trust level, residual energy, and track span all taken into consideration, the EOSR routing protocol developed a multi-factor routing approach. This method stabilizes energy usage while simultaneously ensuring that data is sent through the same. This practice performs well in terms of PDR, network throughput, and node average energy ingesting by emulating the existing routing algorithms [11].

To rise the energy effectiveness of the WSN, Liu et al. (2019) created a revolutionary modified routing protocol. The recently introduced Improved Energy-Efficient LEACH (IEE-LEACH) protocol takes into interpretation both the average energy of the networks and the residual node energy. The technique that is being discussed takes into consideration the quantities of the finest CHs in order to get an adequate depiction that minimizes the use of sensor energy.

In a fuzzy environment, Puneet Azad and Vidushi Sharma (2013) introduced a novel mechanism for CH selection in WSN. Sensor nodes are grouped together during clustering, and Cluster Heads (CHs) are chosen for each cluster. Data from each cluster's nodes is collected by CHs, which then send the aggregated data to the BS. It is recommended to introduce a strategy for the collection of CHs. Three factors are taken into consideration while choosing CHs. The imitation findings show that this strategy outperforms the DHAC protocol in homogenous surroundings in terms of extending network lifetime [13].

Jain and Bhola (2019) introduce the Optimal Cluster Head Selection (OCHS) method, which is also dependent on environmental factors. Because we considered the Received Signal Strength Index (RSSI) of the Sensor Nodes (SN) from the Base-Station, this work is unique (BS). The primary goal of the OCHS algorithm is to maximize system longevity. The performance of the OCHS algorithm is evaluated against the current LEACH and HEED protocols using Cooja Simulator simulations. The OCHS algorithm may successfully increase the network time by two whiles, which makes it an energy-efficient method to select a CH, according to simulation study and results [14].

3. PROPOSED METHODOLOGY

The Trust Aware Energy Efficient Routing (TAEER) mechanism is designed for improving energy efficiency and packet delivery ratio. The proposed system consists of network model, neighbor discovery phase, cluster formation and CH selection, trust management and Fault tolerant based routing.

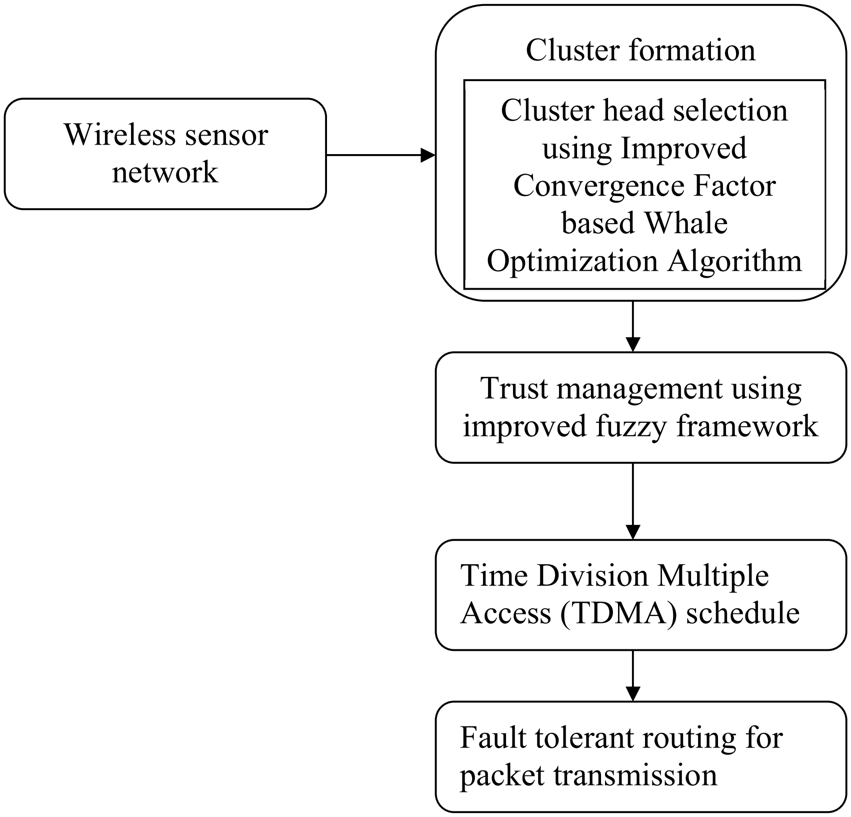
Wireless sensor network
Cluster formation
Cluster head selection using Improved Convergence Factor based Whale Optimization Algorithm
Trust management using improved fuzzy framework
Time Division Multiple Access (TDMA) schedule
Fault tolerant routing for packet transmission

Figure 1: Schematic illustration for the proposed scheme

3.1 Network model

In WSN, nodes are evenly and arbitrarily disseminated over the section. They are dispersed around a square region, with the sides' lengths denoted by the letter "M". We assume that each node has access to sufficient energy for communication with the BS and is also capable of using various power levels. Nodes and the BS are immobile, and no support is provided for mobility. We analyse a network where the BS is roughly positioned near the field's center, despite the fact that the BS may be situated further from the monitoring field. Within the cluster range of the networks, all of the nodes can communicate with their neighbours in a single hop. It is expected that at the start of each phase, all nodes synchronized at least once. In the interest of simplicity, we'll undertake that the wireless transmission channel is protected. We'll also undertake that the system's functioning time is separated into rounds, with cluster formation occurring at the start of each round.

3.2 Neighbor Discovery (ND) Phase

The Neighbors Discovery (ND) protocol is crucial for wireless sensor networks' startup. Each node in the system conducts at least one neighbourhood discovery during the WSN build. In order to give oneself a strong foundation for selecting neighbours, the purpose of this segment is to accumulate as much data as you can about nearby neighbours. To exchange information and alert the selected neighbours, various sorts of messages must be exchanged between the originator and surrounding nodes. The neighbourhood is discovered by the establishment of a neighbours table, as shown in figure 2.

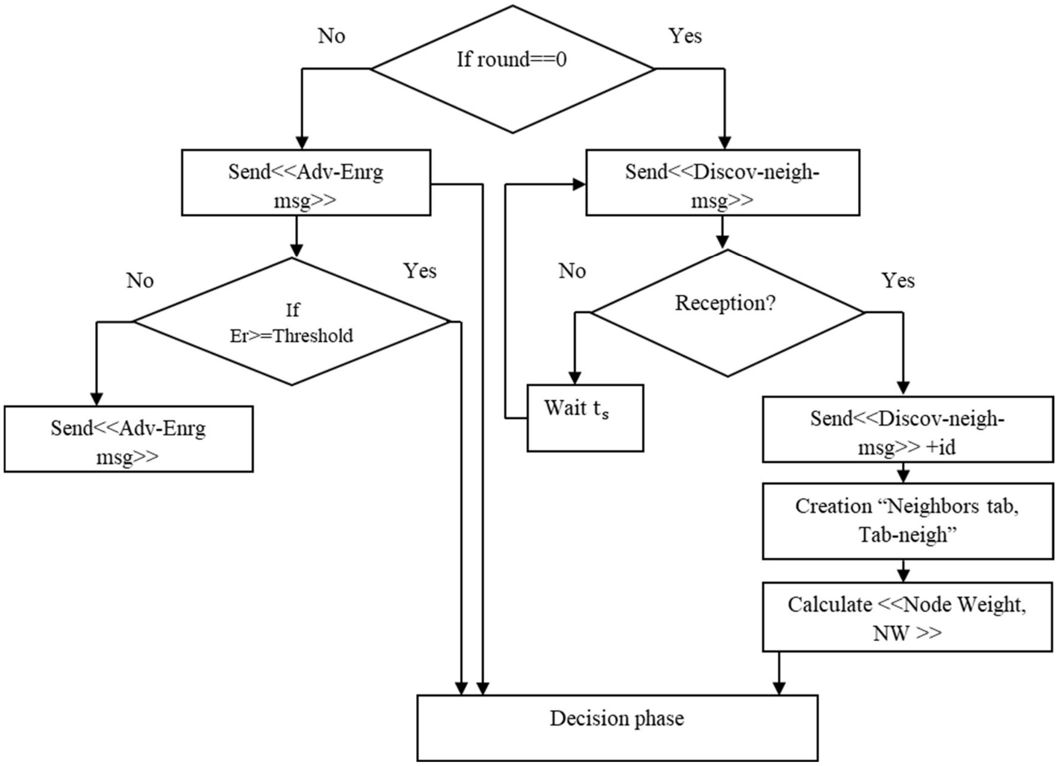

Figure 2. Neighbor finding

To calculate the node-weight, every node in a suggested commitment directs a note called a Discov-neigh-msg that includes its identifier. So, every node immediately transmits a message of the same type upon getting the message. Then, each participant can access the table of its companions to calculate its cost. Making the optimal decision for the needs of the entire WSN is to choose the neighbours procedure. A timer called ts-discov is begun at the same moment the discoverer transmits at the commencement and the very first broadcast. A node that receives a notice adds the foundation as neighbour (or neighbours) of the neighbour and communicates an acknowledgment (ack) announcement posterior to the originator while the timer is running. When the discoverer receives an ack notification, they also add the source as a neighbour. The neighbourhood discovery is finished once the discoverer creates a neighbour table after receiving all ack notifications.

3.3 Cluster formation and CH selection

In this proposed work, distance-based clustering is performed. The CH selection is done by using Improved Convergence Factor based Whale Optimization Algorithm (ICFWOA). The objective functions are

(i) The separation seen between base station as well as the node.

(ii) Residual energy.

(iii) The separation amongst the neighbors' nodes.

(iv) The quantity of neighbouring nodes.
(v) The reachability of Node

For the purpose of computing the Cluster head, we therefore assumed the following equations (Equations 1-3):

$$\beta_1(i,j)=1-\alpha_1(1-\frac{D_{BS,i}}{D_{BS,j}}) \qquad (1)$$

Where,

$D_{BS,i}$: The distance amongst “i” and BS.

$D_{BS,j}$: The distance amongst “j” and BS.

$$\beta_2(i,j)=1-\alpha_2(1-\frac{NW_i}{NW_j}) \qquad (2)$$

Where,

NW_i - Node-weight of «i»

NW_j −Node-weight of «j»

$$\beta_3(i,j)=1-\alpha_3(1-\frac{E_i}{E_j}) \qquad (3)$$

Where,

$E_{r,i}$: Residual energy of « i ».

$E_{r,j}$: Residual energy of « j ».

Node’s reachability is assessment of how accessible the node is reachable to its neighbour nodes inside its own communication range. The definition of reachability (r(i)) is

$$\beta_4 r(i,j,)=\frac{1}{N.(\sum_{j=1}^{j=N-1} d_{ij})} \qquad (4)$$

Where N is the total quantity of nodes discovered during neighbour discovery, and d_{ij} is the separation between nodes i and j. Anodes need to have more neighbouring nodes and a lower reachability value in order to become CHs.

$$P_{ch}(i,j) = \text{Max}\ [1-\sum_{i,j=1}^{n}\beta_1(i,j), \beta_2(i,j), \beta_3(i,j), \beta_4\ r(i,j),)] \qquad (5)$$

Where,

$P_{ch}(i,j)$- Disorder to be CH for node « CH ».

α_1, α_2, α_3, α_4- constant coefficient «0» or «1» n

Improved Convergence Factor based Whale Optimization Algorithm (ICFWOA)

A swarm intelligence optimization programme called the WOA mimics the behaviour of whale predators. The whale constructs a bubble net along the spiral path after locating its target and then travels upstream to the prey. This is the basic idea behind whale bubble-net foraging. The three stages of this predatory activity are encircling the prey, launching a bubble-net attack, and pursuing the prey [15–16].

A. Surrounding Prey Stage

Set the number of nodes in the whale population X_i (i=1, 2,..., n). In the WOA procedure, the whale initially locates the target and then backgrounds it, but then again in reality, it is unable to predict the prey's precise location. As a result, the other members of the group all relocate to the node's current ideal position, which is assumed to be the target prey. The following mathematical model can be used to represent the enclosing stage:

$$D = |C.X^*(t) - X(t)|(6)$$

$$X(t+1)= X^*(t)-A.D(7)$$

Where t is the existing repetition count, X^*(t) signifies the current optimal solution for the prey spot, X(t) denotes the prey position vector, A. D denotes the neighboring step size, and

$$A=2\vec{a}.rand-\vec{a}(8)$$
$$C=2.rand\ (9)$$

In the formula above, $\vec{a}$ is a control parameter that declines linearly from 2 to 0. rand is a random number between [0, 1]. The convergence factor is changed using the formula below to guarantee that the algorithm converges more quickly and stays away from the local optimal.

$$\vec{a}= 2*(1-\frac{Current\ iteration}{Maximum\ iteration})\quad(10)$$

B. Bubble-Net Attack Stage

The humpback whale uses a spiral path to travel near its meal in a confined space as part of its bubble-net foraging strategy. Therefore, two methods shrinking and encircling instrument and spiral apprise positions are developed in WOA to characterise the predation behaviour of whales.

Shrinking and surrounding mechanism: Reduce the convergence factor to achieve.

Spiral update position: To imitate a whale capturing food in a spiral, first determine how far each whale (or its nodes) is from the current best position. It is possible to express the scientific model as trails:

$$X(t+1)=D'.e^{bl}.\cos(2\pi l) + X^*(t) \quad (11)$$

$$D' = |X^*(t) - X(t)| \quad (12)$$

l takes the random number [1, 1], D' is the detachment amongst the recent ideal spot and the ith whale (node). The whale must also reduce the space around the prey while circling around it during the predation phase. Therefore, spiral envelopment and contraction envelopment are carried out with the same possibility in order to establish this synchronous model.

C. Stalking Target Stage

If $|A| \geq 1$, choose a whale (node) at random to substitute the present finest solution. This will enable the algorithm to better explore the entire world while keeping the whale gone from the existing orientation target. The following is the precise typical:

$$X(t+1)=X_{rand}-A.D \qquad (13)$$

$$D=|C.X_{rand}-X(t)| \quad (14)$$

where X_{rand} means randomly selecting the position vector of the whale.

Algorithm 1: ICFWOA

```
Step 1: Set the number of sensor nodes $X_i$(i=1,2,…,n)
Step 2:  Set a, A, C, l and p
Estimate fitness $P_{ch}(i,j)$
X*= the finest search agent
while (it <Maxiter)
 for
if(p<0.5)
if(|A|<1)
Update the location by equation (6)
        Else if (|A|≥1)
Select a random search agent
Update the location by the equation (13)
end
else if(p≥0.5)
Update the location by the equation (11)
End
End
Verify and adjust any search agents that travel outside the search area.
Determine each search agent's fitness
Update   X_(best )if there is a healthier key
t = t+1
end-while
Step 3: return X_(best )
```

3.4 Trust management using improved fuzzy framework

The network security is compromised as a result of the actions of malicious nodes. Accordingly, the main objective of this research is to strengthen system security by identifying malicious nodes. Therefore, an efficient fuzzy based trust management mechanism is used for the detection of hostile nodes. This algorithm enhances the triangle affiliation function of the fuzzy framework's input constraints. After estimating each node's trust score, a threshold-based decision component is used. In this segment, the trust score is compared to the cutoff worth to determine whether or not the node is malicious.

Fuzzy Inference System (FIS)

Fuzzification, fuzzy rule base generation, fuzzy inference system, and defuzzification are the four processes that typically make up the fuzzy framework.

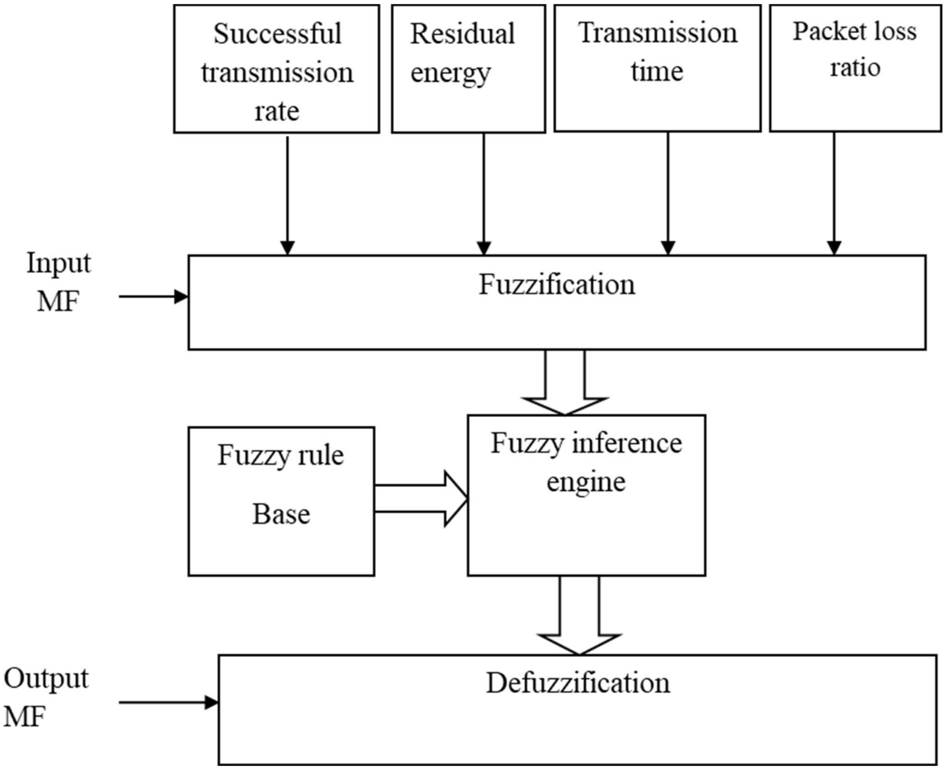

Figure 3: Improved fuzzy framework

3.4.1 Fuzzifcation

In this step, input values that are crisp are implemented as fuzzy variables. The degree to which these values correspond to the linguistic membership values (between 0 and 1) in the supplied fuzzy membership functions is determined by the fuzzification of the input. Table 1 shows the fuzzy membership functions for node parameters as LOW (L), MEDIUM (M), and HIGH (H). Every opinion in the input space is plotted to a membership amongst 0 and 1 according to the Membership Function (MF), which is a curve. The Fuzzy model employs both triangular and trapezoidal MFs to produce the desired results.

3.4.2 Fuzzy rule base generation

The rule base consists of many IF-THEN fuzzy rules. A set of fuzzy implication IF-THEN rules are used to indicate the relationship between the inputs and outputs (inferential). The full list of IF-THEN rules to determine a node's trust score is provided in Table 1.

Table 1: Fuzzy rule base

Rule no	RE	TR	TT	PLR	Trust score
Rule 1(R1)	M	L	H	H	Low
Rule 2(R2)	H	L	M	L	Low
Rule 3(R3)	L	M	H	M	Medium
Rule 4(R4)	H	M	L	H	Low
Rule 5(R5)	H	H	M	M	High
Rule 6(R6)	M	H	L	L	High

3.4.3 Inference engine

Using IF-THEN rules, input and output fuzzy sets, and the fuzzified inputs as inputs, the inference engine extracts the fuzzified inputs and transforms these inputs into fuzzy output. The minimal operator in fuzzy rules that chooses the lower of the two connected membership values is the fuzzy connective operator 'AND'. For each rule, the implication is put into practice, which truncates the output fuzzy membership function based on the lowest value produced by connecting the antecedents with a "AND" link. The aggregated output is created by combining each rule's individual fuzzy set output into a single output fuzzy set. Taking into account the n fuzzy rule set of the form.

Rule i: R_i = IF X is A_iAND Y is B_iTHEN Z is C_i where i = 1, 2, 3, …, n

3.4.4 Defuzzification (D)

This stage involves turning a set of fuzzy values into crisp values. The MFs of the input and output constraints are to be changed for each iteration in order to modify the fuzzy rule basis. Therefore, selecting the right combination of the characteristics is essential. The strategy calls for improving the Fuzzy model's default settings. The process improves input values in a triangle shape to achieve the desired result. It is necessary to improve input values at triangular MFs. Assuming, for instance, that we use the triangle shape depicted in figure 4. The input variables need to be increased. The system will be able to achieve the precise trust score value with the help of the most ideal solution being determined.

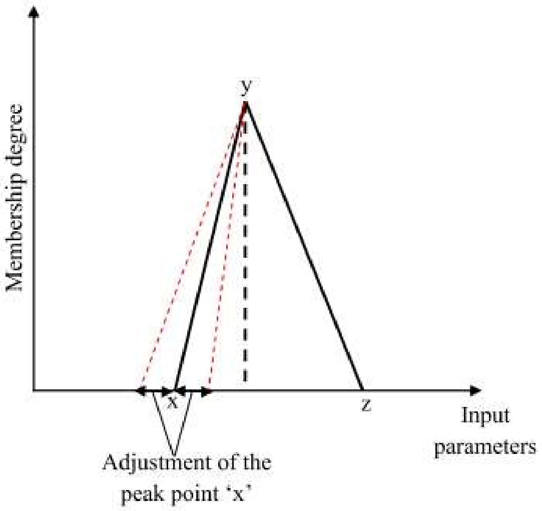

Figure 4: Positioning of peak points

The decision module is executed after the trust score of each node is finished. To determine if a node is malicious or not, the trust rating is estimated to the threshold value in this step.

3.5 Fault tolerant routing

Sensor nodes obtain a time slot for data broadcast through a TDMA plan that is created by the cluster head. The TDMA checking up paradigm states that the control phase and the data phase help to compensate the TDMA super session. The control slots are used to broadcast control packets including route request, route response, and route update protocols. Each network service node has an independent control slot for the control phase. Data packets are transmitted during the data phase, utilizing the data slots.

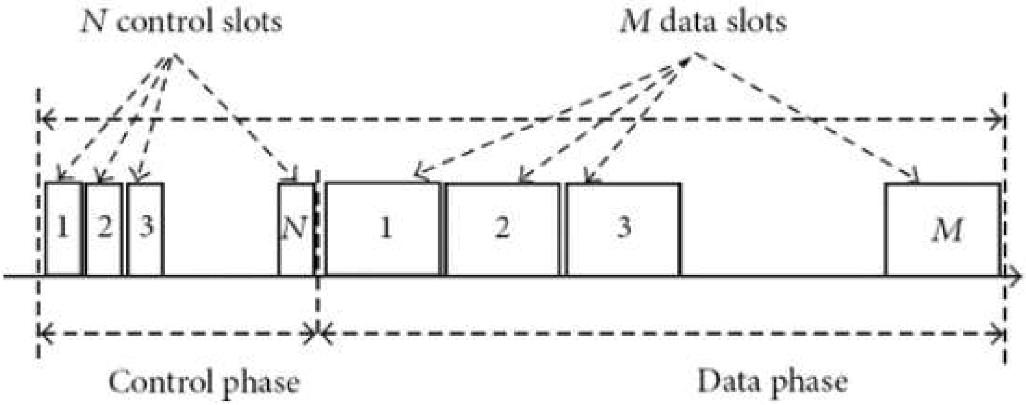

Figure 5: Traditional TDMA frame assembly model

When a defect in the system arises during packet transmission, the algorithm seeks for a new solution so that the communication can continue while using the backup nodes. Each network node can best to address with any other nodes within the transmission range. By selecting the backup routes or backup nodes, communication is restored when faults (node or connection failure) occur. In this proposed work find the eligible node in cluster. If the node is already selected as CH then select next eligible nodes for packet transmission. And also find node status in memory table.

4. EXPERIMENTAL RESULTS

The experiments are evaluated using NS2simulator. The presentation of the designed TAEER mechanism is compared with earlier DEEAC, Hierarchical Energy-Balancing Multipath routing protocol (HEBM) and FTEER in terms of PDR, delay, energy ingesting and average outstanding round. The reproduction settings are represented in Table 1.

Table 1: Replication constraints

Parameter	Values
Number of nodes	200
Area	200mX 200 m
Size of data packet	4000 bits
Size of control packet	512 bits
Initial energy	2J
Location of Base station	(50,50)

Table 2: Performance comparison

Number of nodes	Energy consumption (J)				Packet delivery ratio				End to end delay (s)			
	DEEAC	HEBM	FTEER	TAEER	DEEAC	HEBM	FTEER	TAEER	DEEAC	HEBM	FTEER	TAEER
0	0	0	0	0	75	77	79	85	0	0	0	0
50	62	57	62	50	113	123	126	132	230	180	155	140
100	110	73	80	70	152	159	162	178	450	360	310	310
150	131	98	97	92	204	198	226	235	655	590	540	462
200	162	146	121	110	257	268	278	290	765	680	620	580

Table 3: Average remaining round comparison

Time	Average remaining round			
	DEEAC	HEBM	FTEER	TAEER

0	0	0	0	0
400	45	75	120	145
800	105	125	175	183
1200	155	225	255	278
1600	255	290	300	322

1. End to end delay

The period occupied by a data to communicate from foundation to terminus transversely through the network.

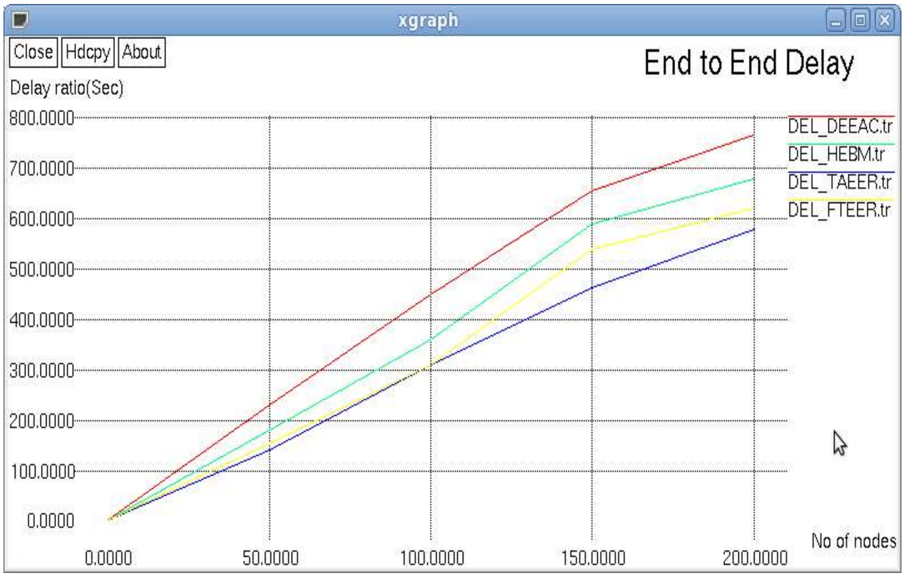

Figure 6: End to end delay comparison

End to end delay comparison of the proposed TAEER mechanism is compared with earlier DEEAC, Hierarchical Energy-Balancing Multipath routing protocol (HEBM) and Fault Tolerance based Energy Efficient Routing (FTEER) mechanisms. The investigational fallouts show that the anticipated system attains 580s of end to end delay for 200 nodes whereas other method such as DEEAC, HEBM and FTEER attains 765s, 680s and 620s respectively.

2. Energy consumption

The amount of energy expended to broadcast data from the source to the destination.

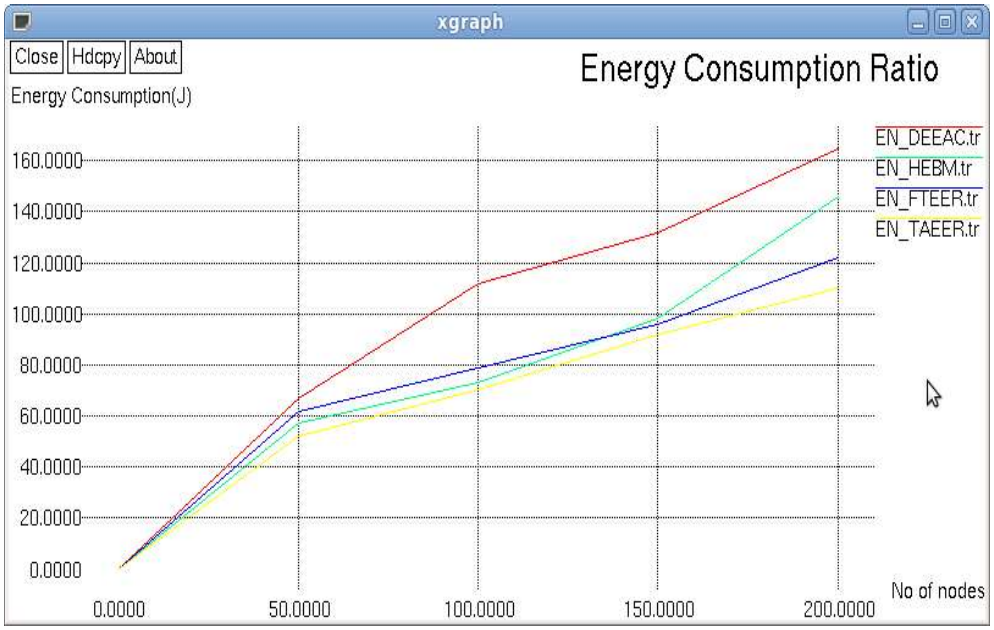

Figure 7: Ratio comparison

To improve the energy efficiency, distance-based clustering is done. Based on the node parameters CH selection is performed using ICFWOA. From the diagram, it can be concluded that the planned system attains 110j for 200 nodes which is better than previous DEEAC, HEBM and FTEER methods.

3. Packet delivery ratio (PDR)

The proportion amongst the quantity of packets effectively transferred to the destination and the quantity of packets broadcasted from the source.

$$\text{PDR}= \frac{\text{Number of packets received}}{\text{Number of packets transmitted}} \qquad (15)$$

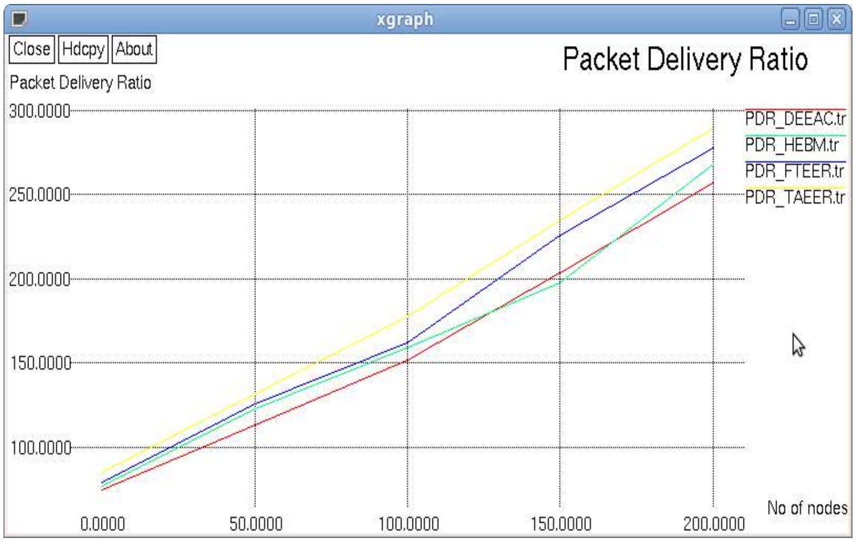

Figure 8: PDR comparison

Figure 8 illustrates the PDR of the planned mechanisms. In this planned work, the cluster head is used to generate a TDMA schedule. It improves the PDR. From the graph, it can be concluded that the proposed system attains packet delivery ratio of 290 where as other methods such as DEEAC, HEBM and FTEER achieves 257, 268 and 278 respectively for 200 nodes.

4. Average Remaining Round

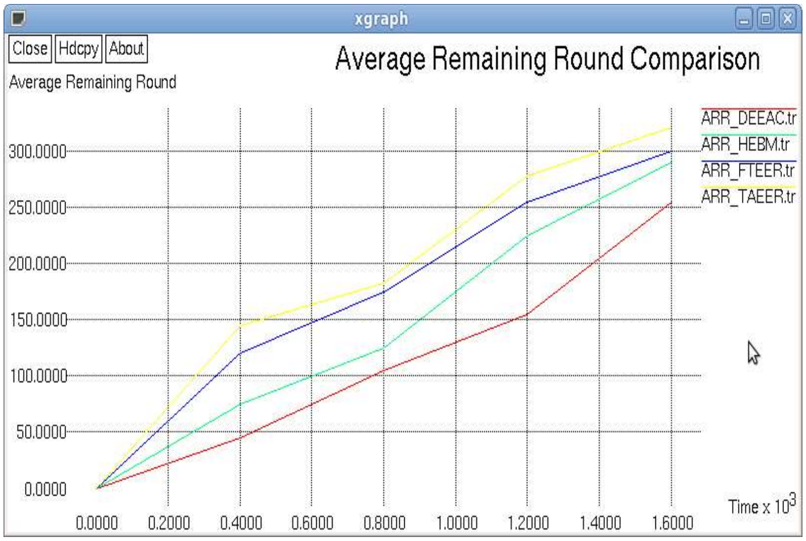

Figure 9: Average Remaining Round

The above figure represents the Average Remaining Round of the proposed protocol and FTEER mechanisms. In x-axis time is taken and average remaining round is taken as y-axis. The investigational outcomes show that the presented framework has greatest excess round contrasted with previous strategies.

5. CONLUSION

The proposed system designed a TAEER approach for WSN. To increases the energy efficiency of sensor network, clustering is performed and CH selection is done by using Improved Convergence Factor based Whale Optimization Algorithm (ICFWOA). To improve the network security, the malevolent nodes are detected by using improved fuzzy based trust management. Finally, perform TDMA based scheduling and fault tolerant routing for effective packet transmission. The investigational outcome show that the proposed system accomplishes higher performance compared with the previous system in terms of PDR, energy consumption, end to end delay and throughput. Future work will expand the protocol to incorporate more indicators like link quality and provide adaptive weights, enabling, for instance, the weight for energy to rise over time. We also want to evaluate the protocol on a bigger, actual network.

References

[1] Min, R., Bhardwaj, M., Cho, S. H., Shih, E., Sinha, A., Wang, A., & Chandrakasan, A. (2001, January). Low-power wireless sensor networks. In VLSI Design 2001. Fourteenth International Conference on VLSI Design (pp. 205-210). IEEE.

[2] Elsmany, E. F. A., Omar, M. A., Wan, T. C., & Altahir, A. A. (2019). EESRA: Energy efficient scalable routing algorithm for wireless sensor networks. *IEEE Access*, *7*, pp.96974-96983.

[3] Tabibi, S., & Ghaffari, A. (2019). Energy-efficient routing mechanism for mobile sink in wireless sensor networks using particle swarm optimization algorithm. Wireless Personal Communications, 104(1), 199-216.

[4] Mohamed, R. E., Saleh, A. I., Abdelrazzak, M., & Samra, A. S. (2018). Survey on wireless sensor network applications and energy efficient routing protocols. Wireless Personal Communications, 101(2), 1019-1055.

[5] Latha, A., Prasanna, S., Hemalatha, S., & Sivakumar, B. (2019). A harmonized trust assisted energy efficient data aggregation scheme for distributed sensor networks. Cognitive Systems Research, 56, 14-22.

[6] Wang, T., Zhang, G., Yang, X., & Vajdi, A. (2018). Genetic algorithm for energy-efficient clustering and routing in wireless sensor networks. Journal of Systems and Software, 146, 196-214.

[7] Kaur, S., & Mahajan, R. (2018). Hybrid meta-heuristic optimization based energy efficient protocol for wireless sensor networks. Egyptian Informatics Journal, 19(3), 145-150.

[8]Sahoo, B. M., Amgoth, T., & Pandey, H. M. (2020). Particle swarm optimization based energy efficient clustering and sink mobility in heterogeneous wireless sensor network. Ad Hoc Networks, 106, 102237.

[9] Mohammad Javad Shayegan Fard. Full Review of Attacks and Countermeasures in Wireless Sensor Networks.International Journal of Information Security and Privacy, 6(4), PP.1-39, 2012.

[10] AlFarraj, O., AlZubi, A., & Tolba, A. (2018). Trust-based neighbor selection using activation function for secure routing in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, pp.1-11.

[11] Yang, T., Xiangyang, X., Peng, L., Tonghui, L., & Leina, P. (2018). A secure routing of wireless sensor networks based on trust evaluation model. Procedia computer science, 131, pp.1156-1163.

[12] Liu, Y., Wu, Q., Zhao, T., Tie, Y., Bai, F., & Jin, M. (2019). An improved energy-efficient routing protocol for wireless sensor networks. Sensors, 19(20), 4579.

[13] Azad, P and Sharma, V. (2013). Cluster head selection in wireless sensor networks under fuzzy environment. International Scholarly Research Notices, 2013.

[14] Jain, K and Bhola, A. An Optimal Cluster-Head Selection algorithm for Wireless Sensor Networks. WSEAS Transactions on Communications, ISSN/E-ISSN, pp.1109-2742, 2020.

[15] Gharehchopogh, F. S., and Gholizadeh, H. (2019). A comprehensive survey: Whale Optimization Algorithm and its applications. *Swarm and Evolutionary Computation*, *48*, pp.1-24.

[16] Nasiri, J., and Khiyabani, F. M. (2018). A whale optimization algorithm (WOA) approach for clustering. *Cogent Mathematics & Statistics*, *5*(1), 1483565.