Secure and Energy efficient-based Clustering and routing protocol of WSN using MCSA

DharmaTeja M[1*], Srinivasan R[2]

[1, 2]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai-62, Tamil Nadu, India.
Email: dharmatejamd@gmail.com[1],rsrinivasan@veltech.edu.in[2]

Received: 17.04.2024 Revised : 25.05.2024 Accepted: 28.05.2024

ABSTRACT
A Wireless Sensor Network (WSN) is containing of many Sensor Nodes (SN) that monitor various applications and collect environmental data. Before sending information to the Base Station (BS), the WSN collects and compiles the detected data. Because of the open environment, lack of centralized administration, and limited battery source, energy efficiency, and security are considered as difficult problems in the WSN. In this paper, implemented a Multi Objective-Trust Aware Chameleon Swarm Optimization Algorithm (M-TACSA) for obtained the secure reliable transmission over the WSN with BS. In this research, two important processes are existing there are: First, implemented M- TACSA is utilized to choose Secure Cluster Head (SCH) by employing the distance between BS to Cluster Head (CH), Node Degree, Residual energy, Distance between neighbour nodes, and Trust Threshold. Second, a secure route from SCH to BS is discovered by optimizing the M-TACSA with, distance between BS to CH, Residual energy, and Trust Threshold for a secure route from SCH to BS is identified.To optimize data delivery and prevent unwanted energy consumption, the implemented M-TACSA is utilized to avoid malicious nodes while choosing the route and SCH. The comparison of M-TACSA shows it has higher performance than the existing method of Trust Based Energy Based Routing (TBEBR) and Taylor-Spotted Hyena Optimization (Taylor-SHO).

Keywords: Energy efficient, Base stations, Sensor nodes, Security, Wireless sensor networks.

1. INTRODUCTION

A WSN is a network of specialized nodes that are uniformly deployed in space to monitor and record physical environmental parameters and then organize the acquired data in a centralized location [1] [2]. Data gathering parameters include soil moisture, temperature, pressure, and other physical variables. Over wireless links, the data are arranged at a single location called BS [3]. One of the initial hierarchical routing techniques is clustering, in which the nodes act as the infrastructure for the cluster and carry out various tasks. This method involves the formation of clusters, or small groups of nodes, within the network [4]. A two-level hierarchy builds this network structure [5]. In WSNs, clustering is a common method of achieving energy efficiency. The quantity of data transmission employing inter-cluster and intra-cluster communication is decreased by clustering-based architecture in WSNs [6]. The head of each cluster also known as the CH, collects data from sensor nodes and transmits it to the BS [7]. To monitor environmental and physical conditions like noise, humidity, temperature, smog, chemical level, pressure, fire detection, light, etc., an WSN consists of a large number of small, low-cost, battery-operated SNs [8].
Each SN in a WSN has the ability to sense, process, and send data directly or upon request to other SNs or BS [9]. WSN technology has advanced and is now widely employed in many industries, including healthcare, manufacturing, network communication systems in intelligent transportation, public security, smart homes [10]. WSN offer flexibility for physical divisions and are scalable. The network's lifetime is significantly increased by energy limit [11]. One of the most effective methods for moving data from remote locations to a central data processing station has proven to be WSNs [12]. The hierarchical or cluster-based routing and the flat routing protocols are the two categories of routing protocols that are based on the network structure [13]. By using multi-hop or multi-path routing, sensed data from the physical region is transmitted to a BS or sink. With a finite battery capacity, WSNs are self-organizing networks [14]. To efficiently transfer sensed data from source to destination, the choice of routing algorithms is a crucial consideration. Various energy-efficient routing techniques have been developed for WSNs, depending on the application domains and network architecture [15]. The main contributions are given below,

- In the implemented scheme, a robust CH selection approach for WSNs is given, and multi-purpose fitness criteria for clustering are defined as the average and residual energy of a node, its distance from the node, and the number of neighbours.
- Due to its capacity to perform rapid solution identification, the M-TACSA calculates the shortest path between CH and BS. Remaining energy, node density, and distance are used to optimize the M-TACSA to overcome the constraint of the unpredictable convergence time.
- The effective CH selection and best path design for data transmission extend the network lifetime. Furthermore, the total number of packets collected by the BS is increased by lowering the nodes' energy consumption when transferring data packets.

The remaining sections of this paper is structured as follows: the literature review is described in Section 2,the description of the proposed method is in Section 3. The result and comparison are described in Section 4, and the Conclusion of this paper is given in Section 5.

2. LITERATURE SURVEY

Bhukya Kranthikumar1 & R. Leela Velusamy [16] implemented a trust aware secured energy efficient fuzzy clustering-based protocol, which was utilized for increased the security and energy efficiency in WSN. In the implemented method, clustering was provided as the optimal approach for WSN metric energy management. As it chose a reliable path for data exchange and used trust-based fuzzy logic to identify malicious nodes. The implemented method reduced the consumption of energy while improved the lifetime of network and communication security. However, the implemented method required large network employed by agent-based communication for improved the trust modelling.

K. Dinesh & S. V. N. Santhosh Kumar [17] implemented a trust-aware neuro-fuzzy-based clustering along with sparrow search optimization algorithm (NF-SSOA) for secured data transmission in WSNs. The neuro-fuzzy clustering algorithm was used in the implemented technique to effectively cluster the nodes, while SSOA was used for routing. The implemented method increased the energy consumption, network lifetime analysis, and ratio of packet delivery. Additionally, the implemented method increased the network's service quality while showed a great capacity for resistance to various forms of security. However, the implemented NF-SSOA method required to increased the significant communication between the network nodes in an efficient manner.

Shivaraj Sharanabasappa Kalburgi & M. Manimozhi [18] implemented a Taylor-Spotted Hyena Optimization (Taylor-SHO), which was combined the Tayor series with SHO. The implemented method was utilized for energy-efficient and reliable cluster head selection based secure data routing and failure tolerance in WSN. The quality of data communication was increased by sending the data BS through CH, which in turn helps to improved the routing performance. However, for considering diverse optimization algorithm for selected CH was required to increased network performance and decreased the delay.

R. Renuga Devi & T. Sethukarasi [19] implemented Trust Based Energy Based Routing (TBEBR) method, which was utilized to decreased the energy consumption to improve the lifetime of network. The implemented method utilized to selected a short distance proper path for appropriately reduced energy consumption. The implemented method enhanced the network lifetime, security level, and effectively find the shortest routing path which makes transmission simple with less energy consumption. However, optimal path selection was required to enhanced for packet travel time, trust value, and reliability.

R. Anitha *et al*. [20] implemented a novel Fuzzy Trust-Based Energy-Aware Balanced Secure Routing Algorithm was utilized to provided the efficient delay limited secure routing. The implemented method employed fuzzy logic as a form of many-valued logic. In this method, the variables values were any real number among 1 and 0, all together for produced the final decision over sensor nodes. The implemented algorithm of secured routing was showed the performance in less delay, energy consumption, throughput with better security. However, the implemented method was required to focused on established the intelligent agent for enhanced the communication process and decision making.

M. Anuja Angel & T. Jaya [21] implemented the Hybrid Penguin Optimization (EPO), which was utilized to solve load balancing, security enhancement, and reduced energy consumption in WSN. The Atom Search Optimization (ASO) algorithm was combined with the implemented hybrid EPO for improved the updated function of the EPO algorithm. By applied the implemented hybrid EPO, the load balancing was achieved by scheme of optimal clustering. And this method increased the WSN performance such as, security enhancement additionally reduction of energy consumption, and load balancing. However, the implemented hybrid EPO method was focused to managed various attacked like node captured attack.

3. PROPOSED METHOD

In brief, The M-TACSA was developed by the study's inspiration of chasing the prey with its eyes, attacking the prey, and the following the prey. If we briefly summarise the algorithm's stages. Figure 1 shows the implemented M-TACSA method's block diagram.

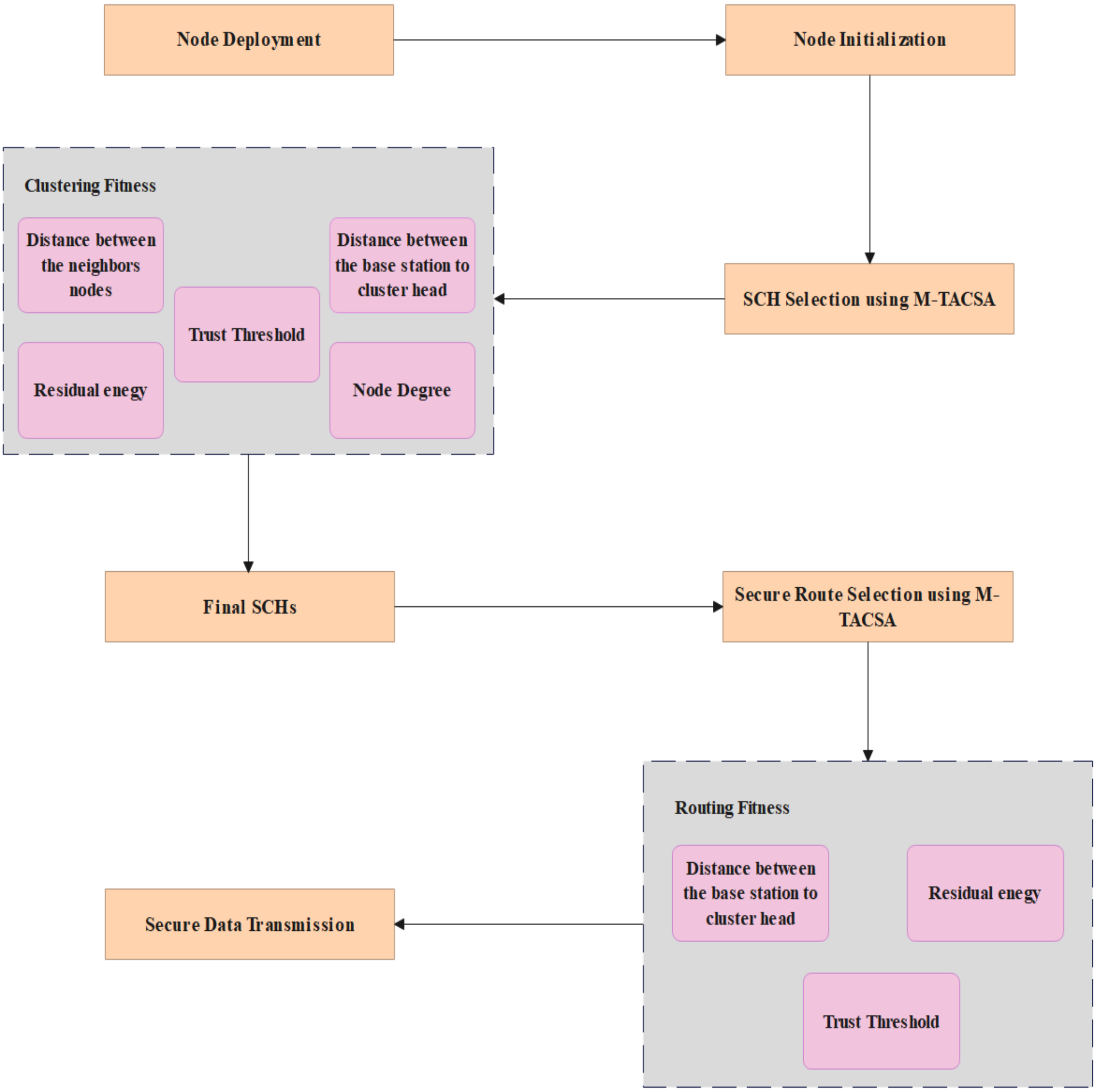
Node Deployment
Node Initialization
Clustering Fitness
Distance between the neighbors nodes
Distance between the base station to cluster head
Trust Threshold
Residual enegy
Node Degree
SCH Selection using M-TACSA
Final SCHs
Secure Route Selection using M-TACSA
Routing Fitness
Distance between the base station to cluster head
Residual enegy
Trust Threshold
Secure Data Transmission

Figure 1. The implemented M-TASCA method

3.1. System Model

This section shows the details about the WSN and energy model utilized to analyse the energy usage over the network. Figure 2 represented the architecture of the clustered WSN.

3.1.1. Network model

The WSN has a small Sensor Node (SN) for routine environmental condition monitoring, and the WSN system is composed of numerous SNs and a base station (BS). WSN clusters split the sensors to use less power. All SNs are categorized into two groups, specifically, the public node and the CH node. Common node frequently evaluates ambient data to connect with CH nodes. The CH nodes on the public nodes are selected by consensus and are responsible for collecting and delivering data to the base station after it is receiving data from the public nodes.

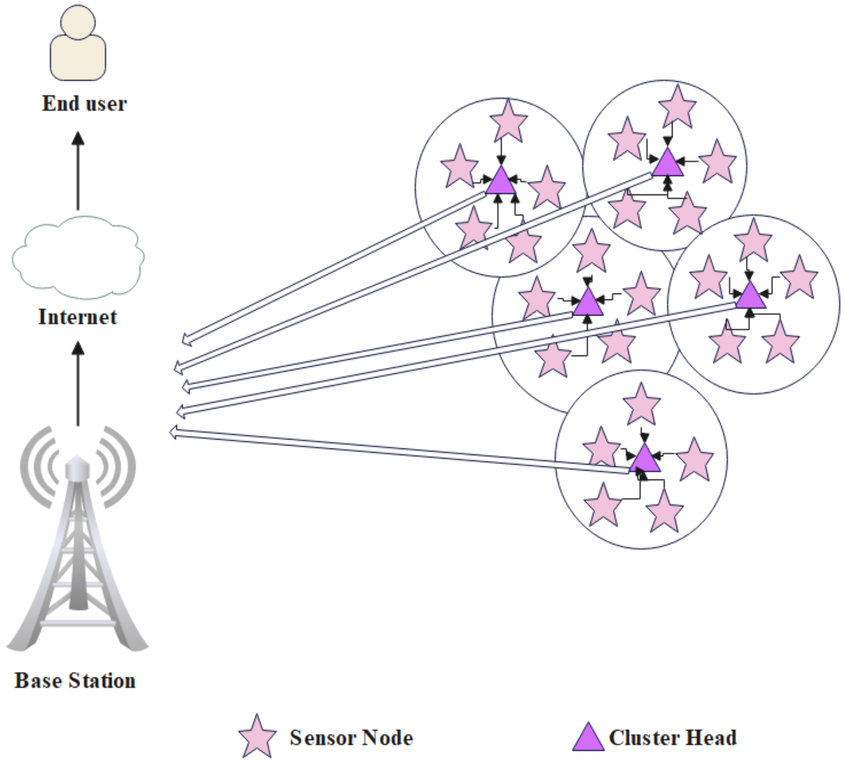

Figure 2. Architecture of the clustered WSN

3.1.2. Energy model

The architecture of system comprises various sensor nodes connected to a single BS. A radio energy model of an SN is using two different channel models: the free space path loss (d^2) model for single-hop communication, and the multipath propagation fading (d^4) model for multi-hop path communication. As a result, the energy required to transport as n-bit packet over distance d is calculated in equation (1),

$E_{TX}(n,d) = \{nE_{elec} + ne_{fs}d^2 \quad d < d_0 nE_{elec} + ne_{mp}d^4 \quad d \geq d_0 (1)$

whereE_{TX} denoted as expected transmission count, n denoted as packet length, d represented as distance among receiving and sender node, E_{elec} denoted as energy required to receive/ transmit 1-bit data. $d_0 = \sqrt{\frac{e_{fs}}{e_{mp}}}$ denoted as threshold distance.

In equation (2), it is determined the quantity of energy is used to receive an n-bit packet size at R_x.

$E_{RX}(n) = n \times E_{elec} (2)$

Three factors that affect the CH in energy consumption are the data packets quantity was received from SNs that are part of a particular data aggregation, cluster executed by CH, and aggregated packets quantity was transferred from CH to BS. Hence, the CH energy consumption is expressed in equation (3),

$E_{CH} = E_{RX}(n,d) \times SN_{num} + E_{DF} \times n \times (SN_{num} + 1) + E_{TX}(n,d) \qquad (3)$

SN_{num} → The number of SNs in a specific cluster E_{DF} → data fusion bit/ energy.

The energy consumption for all SNs other CHs is $E_{TX}(n,d)$.

Equation (4) evaluates the total energy remaining during the $k^{t\square}$ round.

$E_R(k) = E_R(k-1) - (\sum_{l=1}^{CH_{num}(l)} E_{CH}(l) + \sum_{m=1}^{SN_{alive}(k) - CH_{num}(k)} E_{SN}(m))(4)$

where $CH_{num}(l)$ denoted as number of CHs in the $k^{t\square}$ round, $E_{CH}(1)$ denoted energy consumed by $1^{t\square}$ CH, $E_R(k-1)$ denoted total remaining energy at $(k-1)^{t\square}$ *round*, $E_{CH}(m)$ denoted energy consumed by $m^{t\square}$ SN, and $SN_{alive}(k)$ denoted total number of alive nodes in the $k^{t\square}$ round.

3.2. Sensor Initialization

The sensors are first randomly placed in the WSN's interested area. The previous section contains the network and energy models utilized in this study. M-TACSA is used to find a SCHs and routes via SCHs to BS, are discussed in the following sections.

3.3. M-TACSA based SCH selection stage

In this stage, an optimum SCHs from the normal sensors are identified by using the M-TACSA. In short, the study's inspiration for the CSA is following the prey, chasing the prey with its eyes, and attacking the prey. In this section, the CSA is transformed into M-TACSA to discover the set of optimum SCHs.

3.3.1. Initialization and Function Evaluation

Because CSA is a population-based algorithm, the procedure begins here. Every Chameleon represents an answer to an issue in a d- dimensional search space, therefore if call n candidate solutions, the chameleon population can be characterised as the $n \times d$ dimensional two-dimensional y- matrix. If it were a vector, as defined in equation (5):

$y_t^i = [y_{t,}^i 1,\ y_{t,}^i 2, \dots,\ y_{t,}^i d]$ (5)

where the position in the $d^{t\square}$ dimension denoted by $y_{t,}^i d$, and $i = 1, 2, 3 \dots, n$ and t are valid iterations.

3.3.2. In Search of Prey

The following is a numerical description of the way chameleons move and update their positions while as they search for food is expressed in equation (6),

$y_{t+1}^{i,j} = \{y_t^{i,j} + P1(P_t^{i,j} - G_t^j)r_2 + p_2(G_t^j - y_t^{i,j})r1ri \geq P_p y_t^{i,j} + \mu\left((u^j - l^j)r_3 + l_b^j\right) sgn(ran - 0.5)r_i < P_p$
(6)

where $y_t^{i,j}$ denoted the chameleon's current position in the $j^{t\square}$ iteration stage in the $t^{t\square}$ iteration stage,

$y_{t+1}^{i,j}$ denoted the novel location of the $i^{t\square}$ chameleon in the $j^{t\square}$ dimension in the iteration step,

G_t^j denoted the global optimal location in the $j^{t\square}$ dimension attained by any chameleon in the $t^{t\square}$ iteration,

$P_t^{i,j}$ denoted the optimal location always taken by the $j^{t\square}$ chameleon's size in the $t^{t\square}$ loop of iteration,

r_1, r_2, and r_3 are denoted randomly numbers that are spaced evenly from 0 to 1,

p_1 and p_2 are two positive numbers that are controlling the ability of exploration,

P_p denote the detecting chameleon's prey probability, equal to 0.1,

r_i denoted a consistently generated random number in the range of 0 and 1 for the index i,

μ denoted a function parameter of decreasing iterations, and

$sgn(ran - 0.5)$ denoted an effect on the direction of exploration and can be -1 or 1.

3.3.3. Rotation of Chameleon Eyes

Chameleons use their eye's ability to rotate independently of one another to determine the location of their prey. The rotation matrix is explained, and the location is improved using the matrix, after the location has first been translated to the origin, or the centre. It is ten returned to where it originated at.

3.3.4. Prey Hunting

When the prey is quite close, chameleons unleash an attack to finish their chase. It is considered to be the best chameleon since it approached its prey the closest. Chameleons attack their prey with their tongue. As a result, tongue lengths could rise up to double, requiring the chameleon's position to be updated. All of this can be expressed mathematically in following equation (7),

$v_{t+1}^{i,j} = \omega v_t^{i,j} + c_1(G_t^j - y_t^{i,j})r_1 + c_2(P_t^{i,j} - y_t^{i,j})r_2$ (7)

Where $v_{t+1}^{i,j}$ denoted the chameleon's new speed in j.

Size $t + 1$ in iteration shows the current speed of $v_t^{i,j}$,$P_t^{i,j}$denoted the present chameleon's well-known location, and G_t^j denoted the familiar special location of chameleons. $\omega v_t^{i,j}$ denoted the present chameleon location in the $t^{t\square}$ dimension. two positive constants c_1 and c_2 determine the $P_t^{i,j}$ and G_t^j decrease when the chameleon tongue, inertia weight denoted by ω and $r_1$and r_2 are two random numbers dispersed among range 0 to 1.

3.3.5. Fitness for SCH selection

The multi-objective functions for the optimization algorithm for cluster routing path selection are detailed as given below,

- **Distance between the base station to the cluster head**

The separation between the SNs and BSs selected at random is calculated using the P_{sSNBS} function. Sending data from BS to CH over SNs energy-efficient if the distance among the two devices remains to a minimum. Equation (8) demonstrated the process to obtain this function,

$P_{sSNBS} = \sum_{i=1}^{x} dist(SN(CH_i), BS)$ (8)

- **Residual energy**

The quantity of energy remaining in each round determines the CH's essential factor. Energy is distributed throughout the network as a result of the CH rotation, which is based on the nodes of residual energy. In this proposed network, the maximum amount of energy is employed to select CH. The residual energy to total energy ratio is represented by this measure and it is evaluated in equation (9),

$$g_1 = \frac{1}{\sum_{i=1}^{R} \frac{W_r}{W_T}} \qquad (9)$$

where W_T denoted for total energy spent while W_r denoted for residual energy, R denoted for the maximum number of nodes. The possibility of choosing that node as CH decreases with decreasing g_1 value.

- **Trust Threshold**
- **Direct Trust:** The direct trust (DT) score is determined by the interactions of the two nodes. As a result, each node in the network may estimate of its neighbour nodes. Hence, DT_j is calculated using equation (10),

$$DT_j = \beta . \frac{ar_j}{nr_j} + (1 - \beta) . \frac{at_j}{nt_j} (10)$$

where DT_j denoted as direct trust, nr_j denoted to the total number of received packets, ar_j denoted the number of acknowledgement packets received by the j-th node. Same as, nt_j and at_j are related to packets sent from the j-th node. Furthermore, β impact coefficient between packets sent and received to measure direct score.

- **Indirect Trust:** The indirect trust (IT) is determined by a node interacts with its neighbours and is calculated using the information in the neighbour table. Hence, IT_j is defined using equation (11),

$$IT_j = \frac{\sum k \in nn_j \left[T_k + T_k^j\right]}{|nn_j|} (11)$$

where T_k^j denoted the recommended trust to s_j by s_k and T_k denoted the trust score s_k. Also, nn_j and $|nn_j|$ denoted to set of neighbouring nodes and their number, respectively.

- **Recent Trust:** The most recent trust (RT) is calculated using the node regression of the network nodes' indirect and direct trust, the authenticity of the key, and the sink node's acknowledgment, which is a function of time. The recent trust is expressed in the equation (12),

$$T_{i,j}^{recent} (t) = \alpha * T_{i,j}^{direct} (t) + (1 - \alpha) \times T_{i,j}^{indirect} (t) \ (12)$$

where $\alpha = 0.3$.

- **Authentication Trust:** To protect the network from malicious attack, the WSN evaluates the trustworthiness or quality of every node. Network channels may be permanent or temporarily distributed during a DoS attack. Accordingly, the same sensor node sends and receives a set number of packets to ensure a node's reliability.

Assume for example, that there are two nodes, 'a' and 'b', where 'a' needs to determine the whether 'b' is trustworthy. The node 'a' sends the node 'b' a series of packets (hello). The packets are accepted by node 'b', which then sends them back to 'a'. The node 'b' is trustworthy if the total amount of packets sent and received by node 'a' equals one another.

$$AT = \frac{Pfd_a}{Prd_a} (13)$$

where Prd_a denoted the sum of packets received by node 'a', and Pfd_a denoted the sum of packets forwarded by node 'a'.

- **Node Centrality**

The node's distance from its neighbours is determined by node centrality.

$$Node\ Centrality = \sum_{i=1}^{R} \frac{\sqrt{\left(\sum_{j \in m} S^2(i,j)/n(i)\right)}}{Network\ \ Dimensions} (14)$$

where $n(i)$ represented the number of neighbouring SNs.

- **Node Degree**

It gives the SNs number connected with every CH, the CHs with greater cluster lose energy over a longer period of time. The CHs with less sensors are select and the node degree's is expressed in equation (15),

$$Node\ Degree = \sum_{i=1}^{R} J_i \ (15)$$

where the number of SNs denoted by J_i.

3.4. Clustering Stage

Once selecting the SCHs using M-TACSA, the regular sensors are allocated to the appropriate clusters. Energy and distance measurements are taken consider while creating clusters in accordance with the possible function of equation (16),

$$Potential\ function\ (S_i) = \frac{E_{SCH}}{dis\,(S_i,SCH)}(16)$$

3.5. Route discovery stage using M-TACSA

The M-TACSA based secure multi hop discovery is done by employing distance, trust, and energy parameters. The route discovery steps utilizing M-TACSA are given as follows,

1. The chameleon solutions are initially fixed with probable pathways from the transmitter SCH to the BS, with diameter equal to the number of relays SCHs continue in the route.
2. The iterative process described in the previous section is similar to the location update for the portable pathways initialized in chameleon. Equation (17) specifies the fitness consider in the M-TACSA for finding the route.

$$f = \mu_1 \times (DT + IT + RT) + \mu_2 \times \sum_{i=1}^{d} E_{CH_i} + \mu_3 \times \sum_{i=1}^{d} dis(SCH_i, BS) \qquad (17)$$

The secure route that is utilized to prevent malicious attacks during the data transfer is identified by the fitness function discussed earlier. Using malicious node mitigation helps prevent packet loss and unwanted network energy consumption.

4. RESULTS AND COMPARISON

This section details the outcomes and comparative analysis of the M-TACSA method. The M-TACSA method is implemented and simulated using MATLAB R2020b with the system configuration of i7 processor, 16GB RAM and Windows 10 OS. The M-TACSA is used to obtain the secure and reliable data broadcasting over the WSN with BS. The simulation parameters considered to analyse the M-TACSA showed in Table 1. The node density is one of the main parameters for analysing the WSN performances, hence varying nodes are considered for evaluation.

Table 1. Simulation parameters

Parameter	Value
Number of nodes	50, 100
Network size	$200m \times 200m$
Initial energy	0.55J
E_{elec}	$50nJ/bit/m^2$
ε_{fs}	$10pJ/bit/m^2$
ε_{mp}	$0.0013pJ/bit/m^2$
Size of packet	4000 bits

4.1. Performance analysis

Initially, the M-TACSA is analysed with the LEACH, Centralized LEACH (CLEACH), Distributed Energy-Efficient Clustering (DEEC), Threshold DEEC (TDEEC) and Developed DEEC (DDEEC) whereas these classical approaches are implemented by using the similar specifications mentioned in Table 1. The M-TACSA is evaluated using alive nodes, energy consumption, delay, life expectancy, residual, and dead.

4.1.1. Alive node analysis

Alive nodes are the number of nodes in the WSN that have enough energy to complete data transfers. The alive node evaluation for 50 nodes and 100 nodes are shown in Figures 3 and 4. In that, the evaluation is produced among DEEC, LEACH, TDEEC, DDEEC, CLEACH, and M-TACSA. The results of the alive node analysis represented that the M-TACSA living nodes sustained longer than the DEEC, LEACH, TDEEC, DDEEC, and CLEACH. By avoiding malicious nodes during the SCH and route selection, the energy that exists in the M-TACSA nodes are saved. Additionally, the M-TACSA uses the distance parameters considered to reduce the energy consumption, helping in the production of a large number of alive nodes.

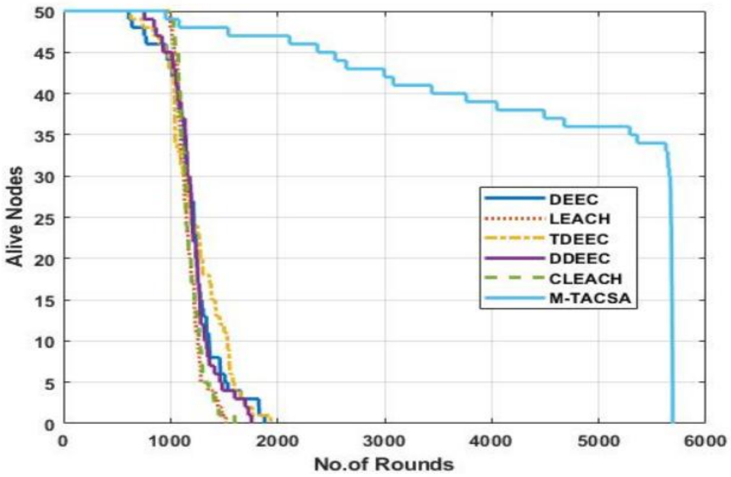

Figure 3. Alive node evaluation for 50 nodes

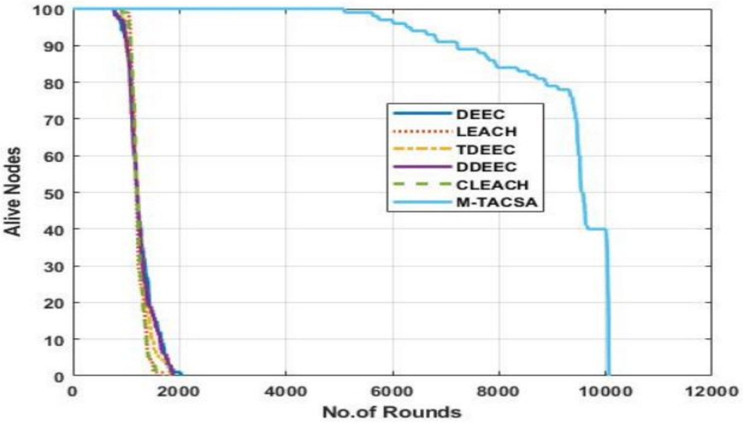

Figure 4. Alive node evaluation for 100 nodes

4.1.2. Energy consumption

One of the important measures used to evaluated WSN performance is the amount of energy consumed when transferring data packets. Figures 5 and 6 shown the energy consumption of M-TACSA with DEEC, LEACH, TDEEC, DDEEC, CLEACH. The comparison for 50nodes and 100 nodes are shown in that Figures 6 and 7. The M-TACSA consumes less energy than the DEEC, LEACH, TDEEC, DDEEC, CLEACH, according to the energy analysis. To reduce the energy consumption of M-TACSA the following strategies are used: 1. Identification of SCH and secure route with lesser transmission distance to the MS is utilized to minimize the usage of energy over the network, 2. CHBF is utilized to balanced clusters that helps to obtain energy balancing, 3. mitigation of malicious nodes using trust helps to avoid the unwanted energy depletion.

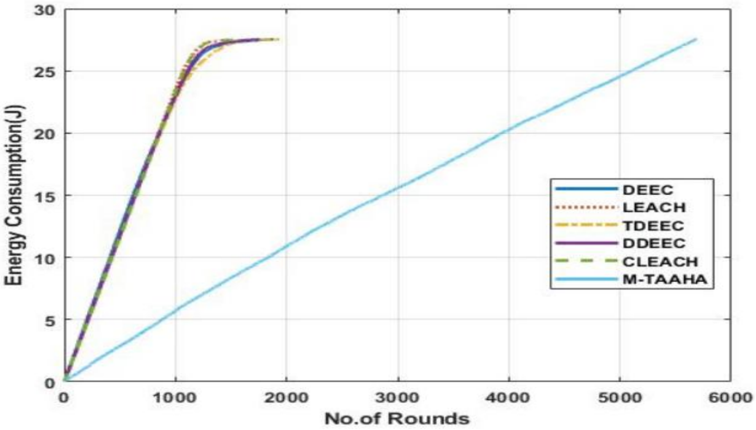

Figure 5. Energy usage evaluation for 50 nodes

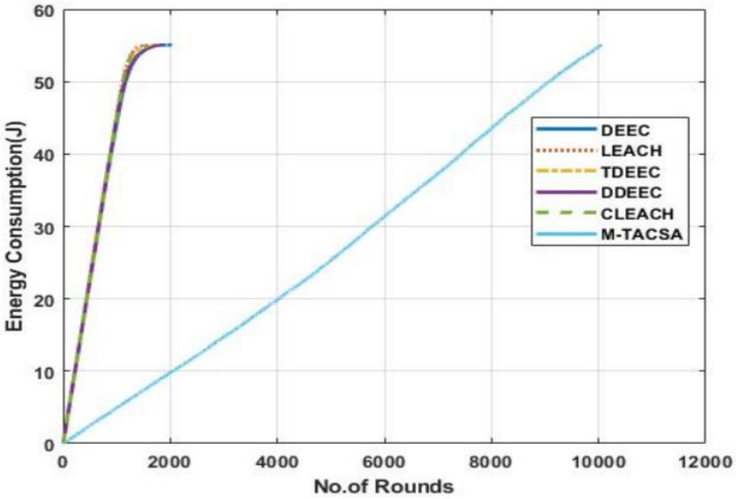

Figure 6. Energy usage evaluation for 100 nodes

4.1.3. Delay analysis

The time duration of data packets transmitting from source to destination is delay. The delay evaluation for 50 nodes and 100 nodes although number of malicious nodes are also varied for analysis are shown in Figures 7 and 8. The delay evaluation is made among DEEC, LEACH, TDEEC, DDEEC, CLEACH and M-TACSA. The results of the delay analysis showed that the delay of M-TACSA is less than the DEEC, LEACH, TDEEC, DDEEC, and CLEACH. To reduce delay, the M-TACSA is utilized to identify a secure routing path with a shorter broadcasting distance.

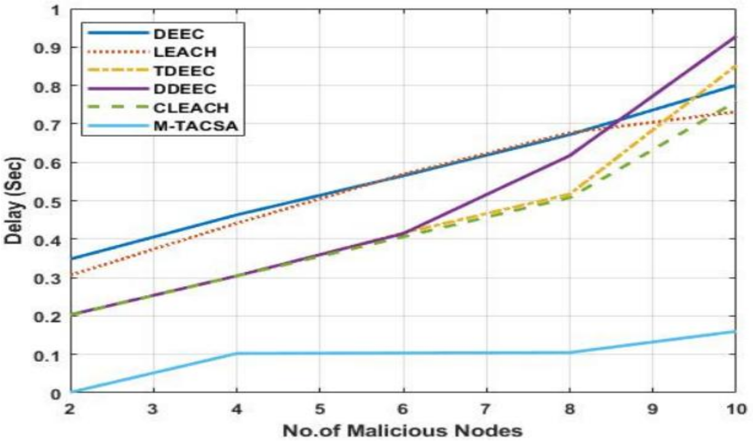

Figure 7. Delay evaluation for 50 nodes

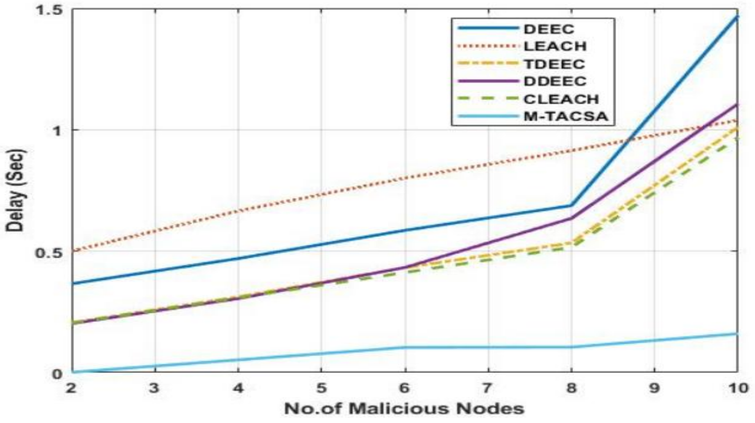

Figure 8. Delay evaluation for 100 nodes

4.1.4. Life expectancy analysis

In WSN life expectancy is the main parameter that indicates the network's operational period. In general, the network is expected to operate for as long as feasible, and the network's life expectancy is determined by the amount of energy present in the nodes. First Node Die (FND), Half Node Die (HND), and Last Node Die (LND) are the three-measure used to analyse the life expectancy. Half of the initialized nodes exhausts their energy is HND, the round number where the first node exhausts their energy is FND, and all the initialized nodes exhausts their energy is LND. The life expectancy comparison for 50 nodes and 100 nodes respectively are shown in Figures 9 and 10. The M-TACSA has a better life expectancy than the DEEC, LEACH, TDEEC, DDEEC, and CLEACH, according to their life expectancy analysis. By balancing energy utilization through optimal SCH and multi hop route selection without malicious node the M-TACSA nodes' available energy is maximised. So, compared to DEEC, LEACH, TDEEC, DDEEC, and CLEACH, M-TACSA has a high life expectancy.

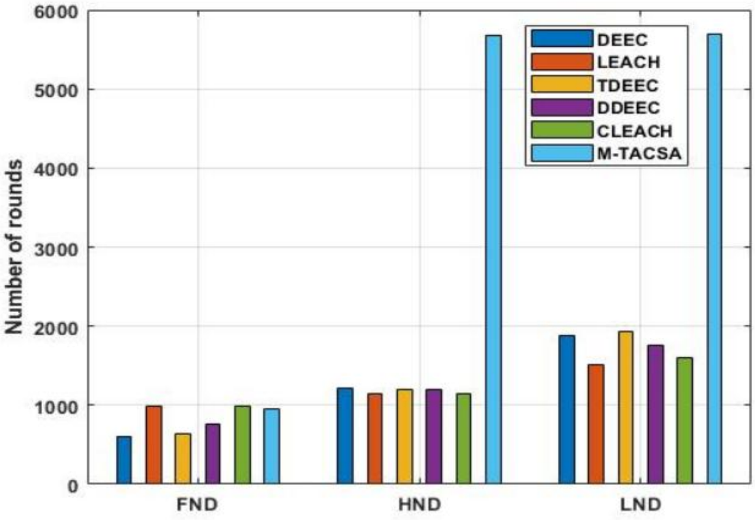

Figure 9. Life expectancy evaluation for 50 nodes

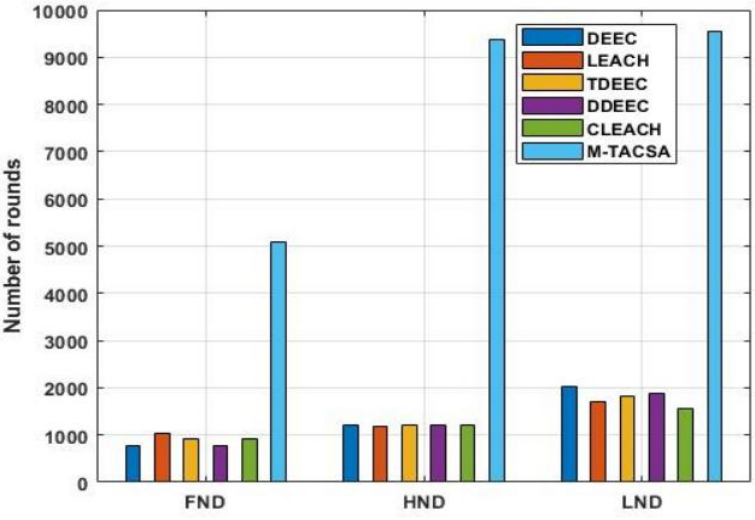

Figure 10. Life expectancy evaluation for 100 nodes

4.1.5. Dead nodes

The evaluation of the dead nodes is the most important performance metric for any WSN routing method. In this case, the CH is select based on the SNs ideal value, and using multiple hop communication, the information of the CH is then broadcast to all nodes in the network and low energy nodes are less likely to be selected as CH. The dead nodes comparison for 50 nodes and 100 nodes respectively are shown in Figures 11 and 12. The M-TACSA has fewer dead nodes than the DEEC, LEACH, TDEEC, DDEEC, and CLEACH, according to their dead node analysis. The M-TACSA increases the network's lifespan by reducing the occurrence of sudden death of node because of low energy levels.

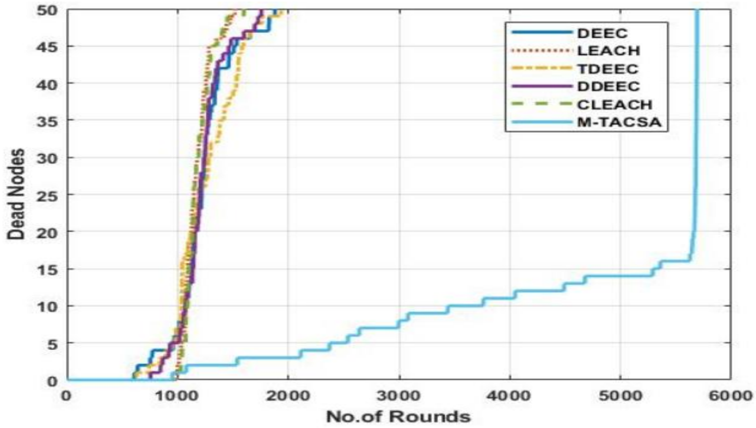

Figure 11. Death nodes evaluation for 50 nodes

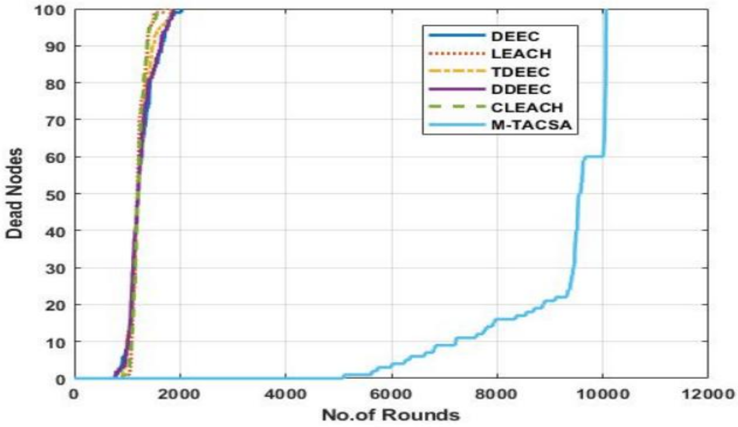

Figure 12. Death nodes evaluation for 100 nodes

4.1.6. Residual Energy

As it is directly related to energy, the amount of energy left behind is an important parameter to assess in addition to increasing network lifetime. During data aggregation, the residual network energy is used to compute the node energy utilization for each round. It can be observed that M-TACSA had the highest residual energy than DEEC, LEACH, TDEEC, DDEEC, and CLEACH. This shows that the network's nodes have a substantially higher amount of energy remaining, which could result in longer network lifetime. The residual energy comparison for 50 nodes and 100 nodes respectively are shown in Figures 13 and 14.

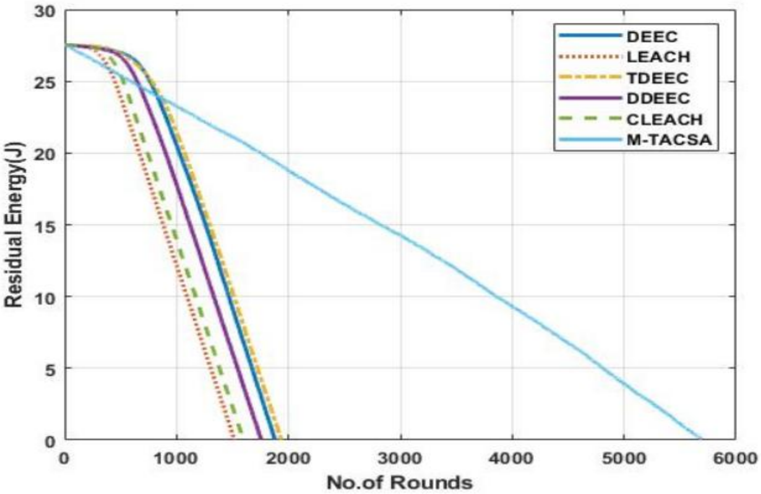

Figure 13. Residual energy evaluation for 50 nodes

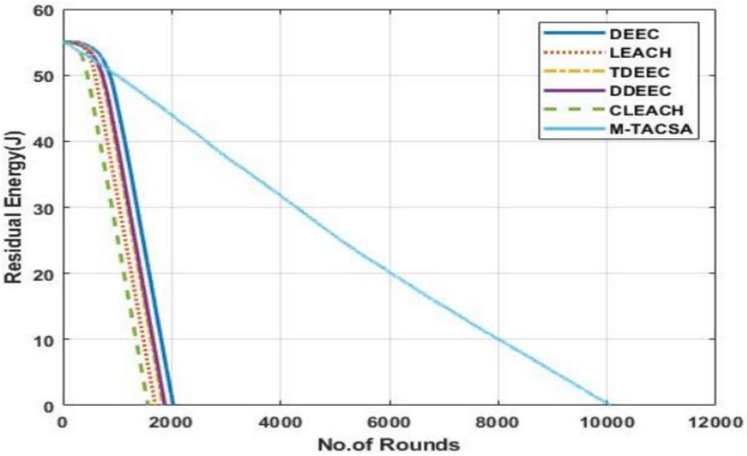

Figure 14. Residual energy evaluation for 100 nodes

4.2. Comparative analysis

In the aforementioned scenarios, scenario 1 is for Taylor-SHO [18] and scenario 2 is for TBEBR [19], comparison with M-TACSA. For the specifications mentioned in the Table 2, the M-TACSA is configured for evaluating the performances. Tables 2, and 3 shows the comparison of M-TACSA with Taylor-SHO [18] and TBEBR [19] respectively. In this scenario, Taylor-SHO [18] consists of 100 Nodes (N), and TBEBR [19] consists of 100 Nodes (N), 100, 100 Areas in (x, y) meters, and 2 Initial_energy in joules are utilized.

This comparative analysis revealed that the M-TACSA outperforms well when compared to the existing techniques. Compare to the existing methods of Taylor-SHO [18] and TBEBR [19], the mitigation of malicious nodes using trust metric in the M-TACSA helps to avoid unwanted energy usage and avoids the packet loss over the WSN. The energy balancing among the clusters is achieved by using CHBF in M-TACSA that results in lesser energy usage. Therefore, the alive nodes of the M-TACSA are increased while minimizing the packet drop over the WSN.

Table 2. Comparison of M-TACSA with Taylor-SHO

Performance	**Methods**	**Number of rounds**				
		200	**400**	**600**	**800**	**1000**
Delay(s)	Taylor-SHO [18]	0.4×10^{-3}	0.5×10^{-3}	0.7×10^{-3}	0.9×10^{-3}	1×10^{-3}
	M-TACSA	0.123×10^{-3}	0.267×10^{-3}	0.49×10^{-3}	0.74×10^{-3}	0.935×10^{-3}
Energy consumption(mJ)	Taylor-SHO [18]	0.2×10^{-3}	0.3×10^{-3}	0.4×10^{-3}	0.5×10^{-3}	0.9×10^{-3}
	M-TACSA	0.098×10^{-3}	0.123×10^{-3}	0.2876×10^{-3}	0.432×10^{-3}	0.689×10^{-3}

Table 3. Comparison of M-TACSA with TBEBR

Performance	**Methods**	**Number of Rounds**				
		20	**40**	**60**	**80**	**100**
Delay(s)	TBEBR [19]	2.2	2.4	3	3.9	4.2
	M-TACSA	0.027×10^{-3}	0.048×10^{-3}	0.071×10^{-3}	0.094×10^{-3}	0.104×10^{-3}
Energy consumption(mJ)	TBEBR [19]	25	40	40	60	64
	M-TACSA	21.1	34.3	34.6	45.9	55.4
Packet Deliver Ratio (%)	TBEBR [19]	97	92	89	84	80
	M-TACSA	99.1	98.99	98.95	98.90	98.89

5. CONCLUSION

Nodes in the WSN broadcast monitored data utilizing multi hop routing in terms of their collaboration with one another. Because of the collaboration among the nodes, it is subject to malicious attacks. In this paper, the energy and secure based routing is implemented by M-TACSA method for WSN with BS. The normal node is chosen as the CH using the M-TACSA, which also selects the CH with the equal cluster balancing, shortest transmission distance, and highest energy. To increase the energy present in the nodes in the WSN, cluster balancing is performed. After, the M-TACSA is used to determine the secure route from SCH to BS. To prevent packet loss and improves the life expectancy, the malicious nodes are therefore avoided when choosing the SCH and secure path. The comparison of M-TACSA shows it has higher performance than the existing method of TBEBR and Taylor-SHO.

REFERENCE

[1] Xue, X., Shanmugam, R., Palanisamy, S., Khalaf, O.I., Selvaraj, D. and Abdulsahib, G.M., 2023. A hybrid cross layer with harris-hawk-optimization-based efficient routing for wireless sensor networks. Symmetry, 15(2), p.438.

[2] Nasirian, S., Pierleoni, P., Belli, A., Mercuri, M. and Palma, L., 2023. Pizzza: A Joint Sector Shape and Minimum Spanning Tree-based Clustering Scheme for Energy Efficient Routing in Wireless Sensor Networks. IEEE Access.

[3] Narayan, V., Daniel, A.K. and Chaturvedi, P., 2023. E-FEERP: Enhanced Fuzzy based Energy Efficient Routing Protocol for Wireless Sensor Network. Wireless Personal Communications, pp.1-28.

[4] Wen, J., Yang, J., Wang, T., Li, Y. and Lv, Z., 2023. Energy-efficient task allocation for reliable parallel computation of cluster-based wireless sensor network in edge computing. Digital Communications and Networks, 9(2), pp.473-482.

[5] Vellaichamy, J., Basheer, S., Bai, P.S.M., Khan, M., Kumar Mathivanan, S., Jayagopal, P. and Babu, J.C., 2023. Wireless sensor networks based on multi-criteria clustering and optimal bio-inspired algorithm for energy-efficient routing. Applied Sciences, 13(5), p.2801.

[6] Rami Reddy, M., Ravi Chandra, M.L., Venkatramana, P. and Dilli, R., 2023. Energy-efficient cluster head selection in wireless sensor networks using an improved grey wolf optimization algorithm. Computers, 12(2), p.35.

[7] Abraham, R. and Vadivel, M., 2023. An Energy Efficient Wireless Sensor Network with Flamingo Search Algorithm Based Cluster Head Selection. Wireless Personal Communications, 130(3), pp.1503-1525.

[8] Manikandan, A., Venkataramanan, C. and Dhanapal, R., 2023. A score based link delay aware routing protocol to improve energy optimization in wireless sensor network. Journal of Engineering Research, p.100115.

[9] Shah, S.L., Abbas, Z.H., Abbas, G., Muhammad, F., Hussien, A. and Baker, T., 2023. An Innovative Clustering Hierarchical Protocol for Data Collection from Remote Wireless Sensor Networks Based Internet of Things Applications. Sensors, 23(12), p.5728.

[10] Al-Otaibi, S., Cherappa, V., Thangarajan, T., Shanmugam, R., Ananth, P. and Arulswamy, S., 2023. Hybrid K-Medoids with Energy-Efficient Sunflower Optimization Algorithm for Wireless Sensor Networks. Sustainability, 15(7), p.5759.

[11] Prakash, P.S., Kavitha, D. and Reddy, P.C., 2022. Delay-aware relay node selection for cluster-based wireless sensor networks. Measurement: Sensors, 24, p.100403.

[12] Cherappa, V., Thangarajan, T., Meenakshi Sundaram, S.S., Hajjej, F., Munusamy, A.K. and Shanmugam, R., 2023. Energy-Efficient Clustering and Routing Using ASFO and a Cross-Layer-Based Expedient Routing Protocol for Wireless Sensor Networks. Sensors, 23(5), p.2788.

[13] Al-Sadoon, M.E., Jedidi, A. and Al-Raweshidy, H., 2023. Dual-Tier Cluster-Based Routing in Mobile Wireless Sensor Network for IoT Application. IEEE Access, 11, pp.4079-4094.

[14] Sathish, K., Hamdi, M., Chinthaginjala, R., Pau, G., Ksibi, A., Anbazhagan, R., Abbas, M. and Usman, M., 2023. Reliable Data Transmission in Underwater Wireless Sensor Networks Using a Cluster-Based Routing Protocol Endorsed by Member Nodes. Electronics, 12(6), p.1287.

[15] Chaurasia, S. and Kumar, K., 2023. MOORP: Metaheuristic Based Optimized Opportunistic Routing Protocol for Wireless Sensor Network. Wireless Personal Communications, pp.1-32.

[16] Kranthikumar, B. and Leela Velusamy, R., 2023. Trust aware secured energy efficient fuzzy clustering-based protocol in wireless sensor networks. Soft Computing, pp.1-12.

[17] Lipi George S.Vinoth Kumar , Detecting Guilty Party Using Dynamic Agents in Data Leakage, International Journal of Scientific and Engineering Research, Vol-3,Issue-7,2012.

[18] D.Prabakar S.Vinoth Kumar, M.Kavitha, Mitigating Selective Forwarding TCP Attacks by Combining MAITH with a Channel-Aware Approach in MANET, International Journal of Computer Science & Technology, Vol-3,Issue-1,2012.

[19] B.Maheswari S.Vinoth Kumar , Delay Restricted Dynamic Multicast Routing Algorithm for Wide Area Network, International Journal of Electronics & Communication Technology,Vol-3,Issue-1,2012.

[20] Aruna.R. et al, Efficient Packet Flow Path Allocation Using Node Proclivity Tracing Algorithm, Lecture Notes in Networks and Systems, 2023, 600, pp. 603–614

[21] Angel, M.A. and Jaya, T., 2022. An Enhanced Emperor Penguin Optimization Algorithm for Secure Energy Efficient Load Balancing in Wireless Sensor Networks. Wireless Personal Communications, 125(3), pp.2101-2127.