[1]Dharma Teja M

[2]Srinivasan R

Multi-objective Trust-aware Dynamic Weight Pelican Optimization Algorithm for Secure Cluster Head and Routing Selection in WSN

Abstract: - Wireless Sensor Networks (WSN) is a group of Sensor Nodes (SNs) which are performed to intellect a normal singularity from an environment. The minimum resources and computational power of WSN creates vulnerable to number of security attacks. To addresses this problem, this paper proposes a Multi-objective Trust-aware Dynamic Weight Pelican Optimization Algorithm (M-TDWPOA)-based secure and energy aware multi-hop routing in WSN with the Base Station (BS). The proposed method comprises of two significant steps: Initially, dynamic energy-efficient Cluster Head (CH) selection by utilizing the multi-objective functions such as Distance between neighbor nodes, Distance between BS to CH, Energy, Centrality and Trust Threshold. Then, dynamic secure multi-hop routing is selected by the multi-objective functions such as Distance between BS to CH, Energy, Trust Threshold which is dynamically reducing the network overhead. Furthermore, a security aware multi-hop routing is employed through the different trust classes like direct, indirect, recent and authentication. The proposed M-TDWPOA approach is estimated with various performance metrics like alive nodes, dead nodes, energy consumption, Throughput and so on. The proposed M-TDWPOA achieves the minimum energy consumption of 0.4927J, 0.4851J, 0.4771J, 0.4693J and 0.4617J when compared to the existing methods like Fractional Artificial Lion (FAL).

Keywords: Base Station, Cluster Head Selection, Multi-hop routing, Multi-objective Dynamic Weight Pelican Optimization Algorithm, Secure and Energy aware routing and Wireless Sensor Networks.

I. INTRODUCTION

Wireless Sensor Networks (WSN) involves greater number of distributed Sensor Nodes (SN) and sink or Base Station (BS) which cooperates with an environment by sensing physical parameters [1]. WSN is utilized in dynamic network due to the simple installation and quick synchronization with other sensors [2]. WSN is significantly utilized for various real-time applications like smart cities, healthcare, transportation, smart agriculture, environmental monitoring and so on. These application uses the characteristics of communication, storage, sensing as well as processing the data in WSN [3][4]. The utilization of application-based WSN which might reduce the battery level because of the minimum energy consumption. As the WSN utilizes the non-rechargeable batteries as SN, an energy consumption becomes one of the significant problems for deploying the WSN [5]. The energy consumption happens when an energy flow among the two nodes. The clustering is a general routing approach performed to segment the whole network into small groups as well as selects the individual node from the cluster group is called Cluster Head (CH) selection [6][7]. The important aim of CH is to acquire the data from the Cluster Member (CM) as well as transform it to the sink node for further data processing. The WSN network lifetime can be enhanced by utilizing the two most significant approaches such as clustering and routing [8][9].

The clustering is the advantage of removes the redundant transmission of data, thus, it minimizes the communication overhead as well as it optimizes an energy consumption in a network [10][11]. The main problem in clustering is to identify an optimal CH configuration for efficient data transmission from SN. Different types of CH as well as energy-aware routing patterns are developed in a cluster-based routing frameworks [12]. Hence, an energy utilized for CH is a significant in cluster-dependent routing approaches [13]. In traditional WSN, the SNs are motorized through the batteries as well as energy tiredness in these batteries are predictable [14][15]. Hence, an energy-aware CH selection model is significant for a cluster-based routing approach to an enhancement of network lifetime of the WSN. Hence, meta-heuristic optimization-based algorithms are introduced for an efficient alternative selection of CH to extend a network lifetime [16]. However, these meta-heuristic face various

[1] * Corresponding author: 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, ORCID: 0000-0002-9201-2898

[2] Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai-62, Tamil Nadu, India.

challenges like fast convergence, local search concerns in the fitness function as well as cost [17][18]. The advantages of dynamic over the static node are data aggregation, in which essential nodes performs only in the transmission, hence remaining nodes can be conserved. Hence, the motivation of this research is to identify an optimal secure data transmissionusing efficient clustering to reduce an entire energy consumption to enhance the node's lifetime of the network. The novelty of this paperisenumerated as following:

- The Multi-objective Trust-aware Dynamic Weight Pelican Optimization Algorithm (M-TDWPOA) approach is proposed for the dynamic secure and energy-aware multi-hop routing selection in WSN.
- The proposed M-TDWPOA approach considers the number of fitness functions such as energy, trust, delay, distance between the BS to CH for the selection of secure multi-hop routing.
- Estimating the proposed M-TDWPOA approach's performance in contrast to routing protocols regarding network performance using different network size.

The remaining part of this research is arranged in a following way: In section 2, the literature survey is discussed. In section 3, the workflow and proposed methodology is provided. In section 4, the results and discussion are provided and in section, the conclusion is presented.

II.LITERATURE SURVEY

In this section, the literature survey of energy efficient a trusting routing protocols in WSN are discussed along with their advantages and limitations. Furthermore, the challenges of the previous works are considered for designing the protocol in WSN.

A. Vinitha *et al.* [19] presented the integration of Taylor series and Cat Salp Swarm Algorithm called Taylor C-SSAfor energy efficient multi hop routing in WSN. The Taylor C-SSA approach endure two stages for the accomplishment of multi hop routing, which involves CH selection as well as data transmission. Initially, Low Energy Adaptive Clustering Hierarchy (LEACH) protocolhad utilized to energy efficient CH selection for an efficient transmission of data with maximum energy. Secondly, the transmitted data over CH were forwarded to the BS by selected optimal hop. Furthermore, the security aware multi hop routing was employed through the development of trust model. The Taylor series ensured an accurate identification of general function. Besides, the suggested approach was incompetent to optimize efficient path selection.

Huaying Yin*et al.* [20] developed an AODV protocol and Multipath Routing approach-based Energy-Aware Trust algorithm (EATMR) for an enhancement of WSN security. Initially, the nodes were estimated according to Open-Source Development Model Algorithm (ODMA) and then, the clustering-based routing was substituted. In this approach, the process of routing followed an AODV protocol as well as multi-path routes model by the consideration of energy-aware trust. An optimal as well as secure route was examined by number of parameters like energy, trust, hop-count as well as multi-objective function. However, the EATMR approach was failed to examine the more objective function for achieving the efficient routing.

Shivaraj Sharanabasappa Kalburgi and M. Manimozhi [21] implemented the integration of Taylor series and Spotted Hyena Optimization called (Taylor-SHO) for CH selection and network lifetime enhancement in WSN. Initially, the suggested approach was utilized for the efficient CH selection by the utilization of fitness estimation based on energy, distance as well as delay. After, the data routing was employed through modified k-Vertex Disjoint Path Routing (mod-kVDPR) approach, which was acquired from the parameters namely trust and throughput. Finally, the route controlling was involved to perceive the delivery operation of the data packets as well as report for connectiondisaster. However, the suggested approach was failed to determine an analysis of computation overhead.

R. Renuga Devi and T. Sethukarasi [22] introduced a Trust Based Energy Based Routing (TBEBR) approach for minimization of energy consumption, enhancement of network lifetime and security level. The suggested approach was aimed to identified energy-efficient shortest path routing selection, which made easy transmission with minimum energy exhaustion. For the selection of next hop in routing pat, the TBEBR considered the parameters like initial energy, residual energy, reliabilities and trust value. Mixed Integer Linear Programming (MILP) approach was chosen to make the less energy-consumption WSN approach. The TBEBR based WSN routing had minimum resource accessibility, partial communication as well as minimum energy constraints.

Perumalla Suman PrakashYin*et al.* [23] developed the Fractional Artificial Lion (FAL) approach for an efficient and secure optimal path selection during routing in WSN. The FAL was developed by the integration of Fractional Calculus, Lion Optimization Algorithm (LOA) as well as Artificial Bee Colony (ABC). CH selection and routing were efficiently achieved through the FAL approach. The fitness function with maximum value was measured as an optimal route for data packets transmission and after simulated WSN was utilized for the route maintenance. The FAL had achieved better scalability, besides maximum death nodes were not examined for clustering to acquire efficacy of the model.

Some limitation had been identified in this section such as incompetent to optimize efficient path selection, failed to examine the more objective function for achieving the efficient routing, failed to estimate the computation overhead and death nodes were not examined for clustering to acquire efficacy of the model. These limitations have been addressed in this research based on dynamic secure and energy-efficient CH and routing selection.

III.PROPOSED METHODOLOGY

The M-TDWPOA approach has multiple significant phases: trust-based clustering, optimal CH selection as well as trust-aware energy efficient routing. As begin, the nodes with similar energy are deployed arbitrarily in the network region. The dynamic routing mechanism ensures the secure distribution of the data packets by utilizing trust-based approaches. Figure 1 shows the network model of WSN.

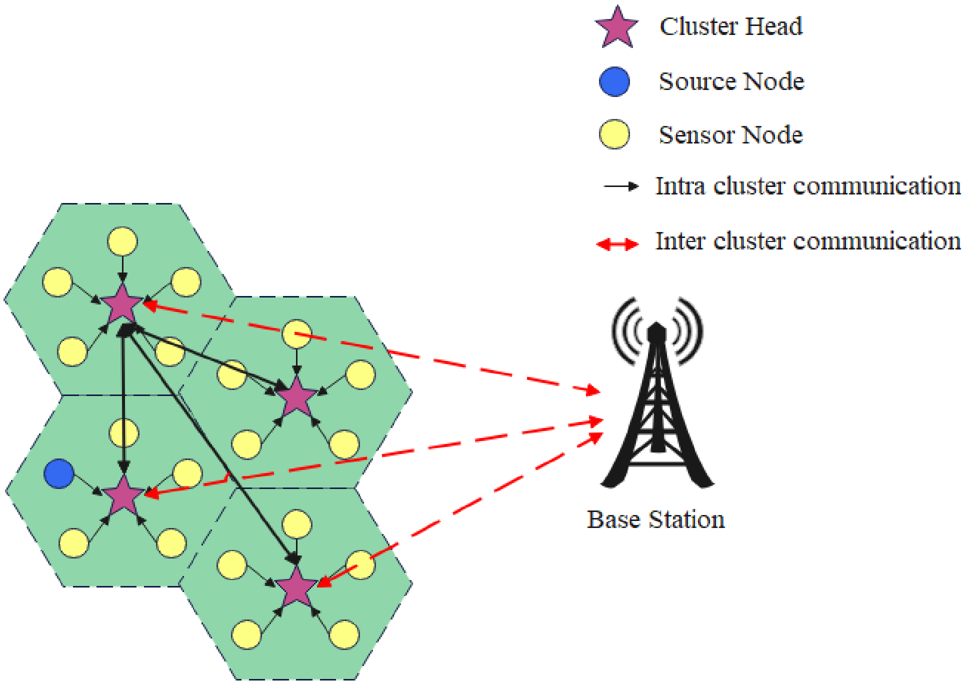


Figure. 1. Network model of WSN

3.1 System Model

As in Figure 1, the nodes in WSN are gatheredfrom various clusters and every CH is associated to an individual sink or BS. The wireless connection between the SN denoted the direct interaction within transmission boundary. Each node has communication boundary and SNs are consistently dispersed in the dimension of U_v and V_v meters. Every node has unique ID, hence the SNs are gathered to create clusters in WSN. Sink is utilized to obtain data packets from SN by CH. Now, every direct rate of U_i and V_i represents the individual SN. Once the cluster is created, the nodes communicate the bytes by utilizing their consistent CH.

3.2 Network Model

In WSN, the goal of the clustering is to reducean energy consumption through grouping the sensors into clusters. the general nodes often investigate a background as well as transmit the sensory data to the CH. The predominant aim of CH is to collect data from every cluster node as well as transforms it to the BS. The grouping process aids in ignoring the direct communication among the sensors as well as receivers.

3.3 Energy Model

Here, an initial order communication node is utilized for energy organization in SN. The energy node is directly proportional to the propagation distance n when a threshold distance $n_0$surpassesa value of n. A total energy utilized through every node to communicatea$b$-bit data packet is expressed in eqn. (1) and (2) as follows:

$$E_{T_x} = b \times E_{elec} + b \times \varepsilon_{amp} \times d^{\lambda} \qquad (1)$$

$$\varepsilon_{amp} = \begin{cases} \varepsilon_f \times n^2, when\ n \leq n_0 \\ \varepsilon_p \times n, when\ n > n_0 \end{cases} \qquad (2)$$

The packet involves b bits is communicated among transmitter T_x and Receiver R_x at the distance of d meters according to an energy E_{T_x}. Where, E_{T_x} – total energy required to transfer the data; E_{elec} – dissipation of energy per bit; ε_f – energy utilized for amplification in free space model; b – number of bits; λ – route drop constant. The λvalue is identifiedaccording to transmission distance $d$which is similar to the threshold distance d_0, which is basically expressed in eqn. (3) as:

$$d_0 = \sqrt{\varepsilon_{fs}/\varepsilon_{mp}} \qquad (3)$$

Furthermore, an energy consumption of the receiver is expressed in eqn. (4) and (5) as:

$$E_{rx} = E_{elec} \times b \qquad (4)$$

$$E_{sum} = E_{elec} + E_{T_x} \qquad (5)$$

Where, E_{rx} – total energy required for received data; E_{sum} – total energy loss for WSN. The process of above discussed data communication is repeated until the SNs are dead. Hence, the nodes become departed when the energy of the corresponding node exhausted to less than 0 respectively.

3.4 Secure CH and secure route discovery using MDWPOA

Pelican Optimization Algorithm (POA) [24][25] is a metaheuristic algorithm and which is inspired through the pelican's hunting behavior as well as strategy. The POA explores as well as exploits agreatest point of an objective function through replicating a pelican behavior. The Pelican's strategy is classified into two phases in a searching process such as moving towards prey (exploration) as well as winging on water surface (exploitation). Figure 2 shows the block diagram of M-TDWPOA.

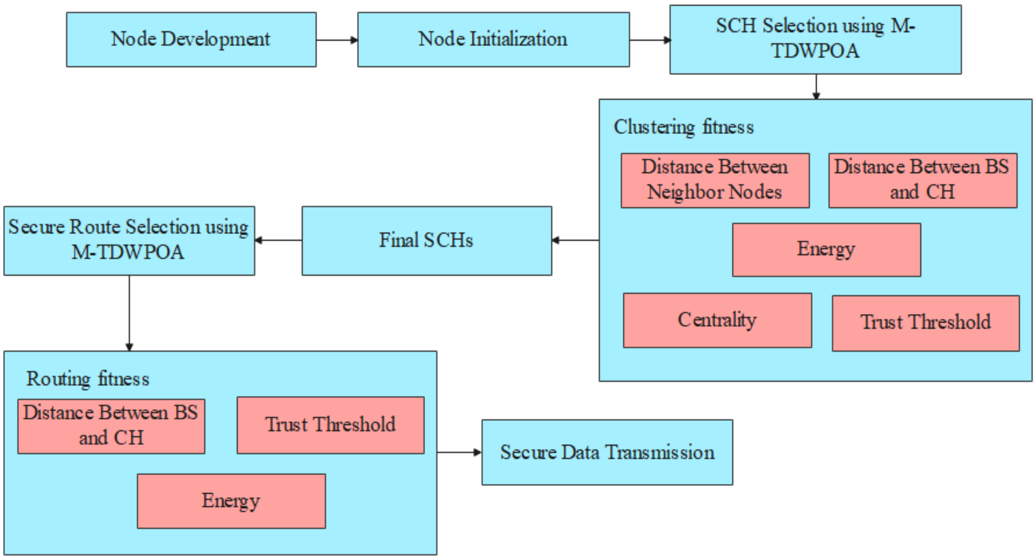


Figure 2. Block diagram of the proposed M-TDWPOA

a. Moving towards prey (exploration)

In an initial phase, pelican determines a prey position and moves in the direction of determined position. The strategy of the pelican allows the scanning of the search space as well as enhances the exploration capability of POA in determining the various positions of the search space. This process enhances a pelican's capability to explore the space for efficient search problem solving. The perception as well as pelican's strategy of moving towards the prey is expressed in expressed in eqn. (5) as follows:

$$P_{im}^{t+1} = \begin{cases} P_{im}^{t} + rand.(S_m^t - \lambda.P_{im}^t), & F(P_s) < F(P_i) \\ P_{im}^{t} + rand.(P_m^t - S_m^t), & F(P_s) \geq F(P_i) \end{cases} \qquad (5)$$

Where, t – current iteration number; P_{im}^t and S_m^t – position of ith pelican and prey's position in mth dimension; λ – arbitrarily equal to 1 or 2; $F(P_s)$ –objective function value; $F(P_i)$ – value of fitness function of ith pelican in mth dimension.

b. winging on water surface (exploitation)

In this stage, after the pelicans reaches the water surface, the pelicans feast their wings above the water to push the fish out before gathering their prey in gorge pouch. This plan has resulted in number of fish is wedged through the pelicans in areas under the attack. From the aspect of mathematical view, the approach must determine the points close to the position of the pelican to converge on the better solution. During hunting, the pelican's behavior is expressed in eqn. (6) as follows:

$$P_{im}^{t+1} = P_{im}^{t} + \gamma.\left(\frac{T-t}{T}\right).(2.random - 1).P_{im}^{t} \qquad (6)$$

Where, T – maximum iteration number; $.\left(\frac{T-t}{T}\right)$ – neighborhood radius of P_{im}^t; $random$ – random number among the range of 0 and 1. After enhancing the actual POA approach, an optimization efficiency must be enhanced. The particular enhancement strategy is provided below. The dynamic weight factor θ plan is utilized to enhance the standard POA position in the initialization as well as moving towards the prey. Here, dynamic weight factor θ supports the pelican to update its position. At the starting of this iteration, θ has maximum value, and the pelican is capable to employ the best global search at the end of an iteration θ adaptively. An enhanced version of this process in expressed in eqn. (7) as follows:

$$P_{im}^{t+1} = \begin{cases} \theta = \dfrac{e^{2(1-{t}/{T})} - e^{-2(1-{t}/{T})}}{e^{2(1-{t}/{T})} + e^{-2(1-{t}/{T})}} \\ P_{im}^{t} + rand.(S_m^t - \lambda.P_{im}^t).\theta, & F(P_s) < F(P_i) \\ P_{im}^{t} + rand.(P_m^t - S_m^t).\theta, & F(P_s) \geq F(P_i) \end{cases} \qquad (7)$$

Where, θ – dynamic weight factor; Here, the pelican is capable to employ the better local search while enhancing the convergence speed. The way of pelican's prey hunting behavior is discussed. The dynamic adjustment of these weights enhances the POA ability, ensures the secure CH selection and intersecting the energy limits of WSN. The fitness function of the secure and energy-aware CH selection and routing is discussed in the following section.

3.5 Fitness Function for secure CH selection

In this section, the multi-objective fitness function is estimated for obtaining the best solution. The five fitness functions are considered for both secure CH selection and routing discovery. An estimated solution of this best fitness value is assumed as an optimal solution.

1. Distance between neighbor nodes

Begin, each CH identifies the neighbor CH. After the node is selected, it transmits the ACK message with the distance of BS, node degree. The distance between the neighbor node is expressed in eqn. (8) as:

$$f1 = \sum_{i=1}^{n} f(XCH_i) \qquad \forall i \in N \qquad (8)$$

2. Distance between BS to CH

The energy consumption of the nodes is based on the distance towards the transmission path. Transmitting the data from BS to CH when the distance among the two devices remains less. The distance between BS to CH is expressed in eqn. (9) as:

$$f2 = \sum_{i=1}^{n} min\left(dist(XCH_1, BS)\right) \qquad (9)$$

3. Energy

The fitness function of the energy is formulated in eqn. (10). The complete CH is cumulative involves high CH count and energy. The total energy is based on the consumed energy through the nodes during transmission, reception as well as sensing.

$$f3 = \frac{fc_{(ac)}^{egy}}{f_{(bc)}^{egy}} \qquad (10)$$

4. Centrality

The node's distance from its neighbors is determined by node centrality, which is expressed in eqn. (11) as:

$$f4 = \sum_{i=1}^{R} \frac{\sqrt{\frac{\sum_{j\in m} S^2(i,j)}{n(i))}}}{Network\ Dimensions} \qquad (11)$$

where $n(i)$ - number of neighboring SNs.

5. Trust Threshold

In M-TDWPOA, the hierarchical trust values are utilized to manage the dynamic trust behavior. The trust threshold distributes the security in the proposed approach in the clustering and routing process. At this time, every hop in WSN delivers maximum trust degrees for estimating a trust level between the hops as well as neighboring hop. The trust model is estimated by for parameters such as direct, indirect, recent and authentication. The Direct trust (DT_j) score is determined by the interactions of the two nodes. As an outcome, every node in the network may estimate of its neighbour nodes. The Indirect Trust (IT_j) is determined by a node interacts with its neighbors and is calculated using the information in the neighbor table. The recent trust (RT) is estimated through DT and IDT along with significant validity as well as confesses the sink. The DT_j, IT_j, RT and AT are expressed in eqn. (12-15) as:

$$DT_j = \beta.\frac{ar_j}{nr_j} + (1-\beta).\frac{at_j}{nt_j} \qquad (12)$$

$$IT_j = \frac{\sum_{i=1}^{r} k\in nn_j[T_k + T_k^j]}{|nn_j|} \qquad (13)$$

$$T_{i,j}^{recent}(t) = \alpha * T_{i,j}^{direct}(t) + (1-\alpha) \times T_{i,j}^{indirect}(t) \qquad (14)$$

$$AT = \frac{Pfd_a}{Prd_a} \qquad (15)$$

where nr_j - total number of received packets, ar_j - number of byline packets received through$j$th node. β impact coefficient among packets transmits and received to calculateshortest score. T_k^j - recommended trust to s_j by s_k and T_k - trust score s_k; nn_j and $|nn_j|$ - set of neighbouring nodes and their number. $Prd_a$and Pfd_a- sum of packets received and forwarded through node 'a'.

3.6 Clustering Stage

After the selection of secure and energy aware CH using M-TACSA, the actual sensors are allocated to the appropriate clusters. Energy and distance measurements are taken consider by using the potential function S_i, which is expressed in equation (16),

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

After this clustering stage, to discovery the path for data transmission SCH to BS, the discovery of the routing discovery using M-TACSA is discussed below.

3.7 Secure Routing Discovery

The M-TACSA based secure multi hop discovery between CH and BS is performed by using Distance between BS to CH, Energy, Trust Threshold. The secure routing discovery is performed by two steps: initialization and route selection.

1. In routing, every MDWPOA represents the data transmitting path between CH and BS. The transmission route from source node to BS is updated by every pelican and the quantity of CH in the appropriate transmission is similar to the measurement for every pelican.
2. To determine the data transmission path, the MDWPOA utilizes the indistinguishable fitness value. The route request message is transmitted from source node to the neighbor node to modify the route discovery path. At this stage, the further node with greater fitness rating transmits the message return to the CH by reverse path. The transmission of data is initiated by the network after the routing path is developed.

IV.EXPERIMENTAL RESULTS AND DISCUSSION

In this section, the proposed MIPOA approach is estimated through performing the simulations over the previous works. The performance is estimated according to the expectations that SN are static when organized nodes are incapable to change their positions. The demonstration of the proposed method is stimulated on MATLAB tool with windows 10 OS, intel core i7 processor system configuration, 16GB RAM. Table 1 shows the simulation parameter of the proposed method.

Table 1. Simulation parameters

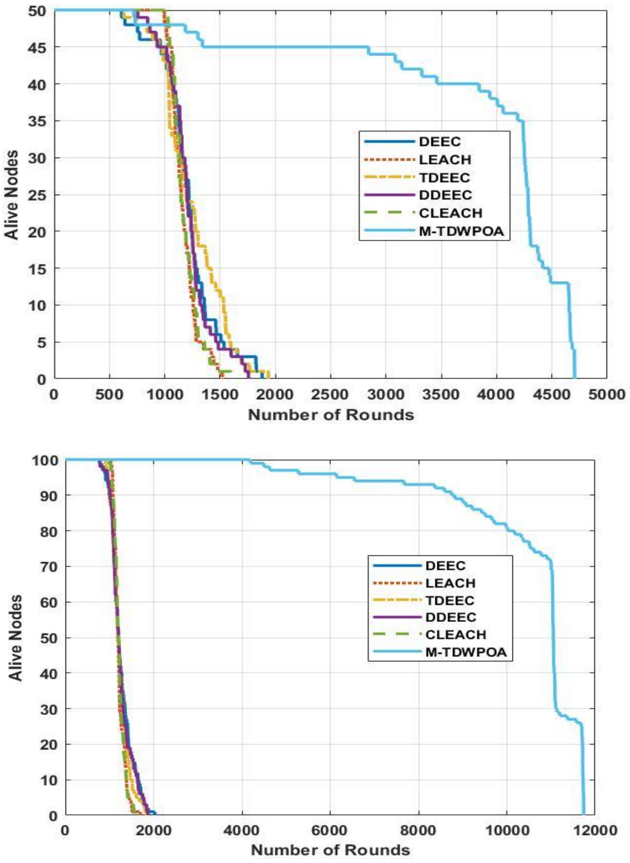
Parameter	**Value**
Number of nodes	50, 100
Network size	$200m \times 200m$
Initial energy	0.55J
E_{elec}	$50nJ/bit/m^2$
ε_{fs}	$10pJ/bit/m^2$
ε_{mp}	$0.0013pJ/bit/m^2$
Size of packet	4000 bits

4.1 Performance Analysis

The proposed M-TDWOA performance is estimated with the various performance metrices like alive nodes, dead nodes, energy consumption First Node Dead (FND), Half Node Dead (HND), Last Node Dead (LND), Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR) and Throughput. The proposed M-TDWOA analyzed with the previous approaches like Distributed Energy-Efficient Clustering (DEEC), LEACH, Threshold DEEC (TDEEC), Developed DEEC (DDEEC) and Centralized LEACH (CLEACH). Table 1 shows the implementation of previous approaches using similar specifications.

4.1.1 Alive Nodes

Alive nodes are utilized for originating the transmission in WSN.Figure 3 (a) and 3 (b) represents the performance analysis of alive nodes with 50 and 100 nodes. The proposed M-TDWOA is estimated with the various number of rounds like from 0 to 5000 respectively. If the number of rounds is increases, alive nodes are decreases. The alive nodes of proposed M-TDWOA are verified with the previous approaches like DEEC, LEACH, TDEEC, DDEEC and CLEACH. As a result, the proposed M-TDWOA approach attains the maximum the number of alive nodes in both the 50 and 100 nodes as compared to DEEC, LEACH, TDEEC, DDEEC and CLEACH.

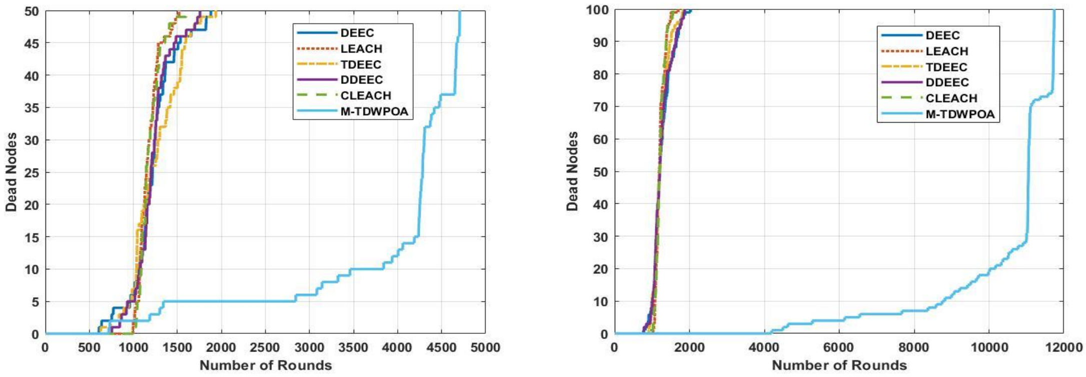


(a) (b)

Figure 3. Alive nodes analysis (a) 50 nodes and (b) 100 nodes

4.1.2 Dead Node

The estimation of the dead nodes is the significant performance metric for an efficient routing selection in WSN. Figure 4 (a) and 4 (b) represents the performance analysis of dead nodes with 50 and 100 nodes. The proposed M-TDWOA is estimated with the various number of rounds like from 0 to 5000 respectively. If the number of rounds is increases, the dead nodes are increases. The dead nodes of proposed M-TDWOA are verified with the previous approaches like DEEC, LEACH, TDEEC, DDEEC and CLEACH. As an outcome, the proposed M-TDWOA approach attains the minimum the number of dead nodes in both 50 and 100 nodes as compared to DEEC, LEACH, TDEEC, DDEEC and CLEACH.

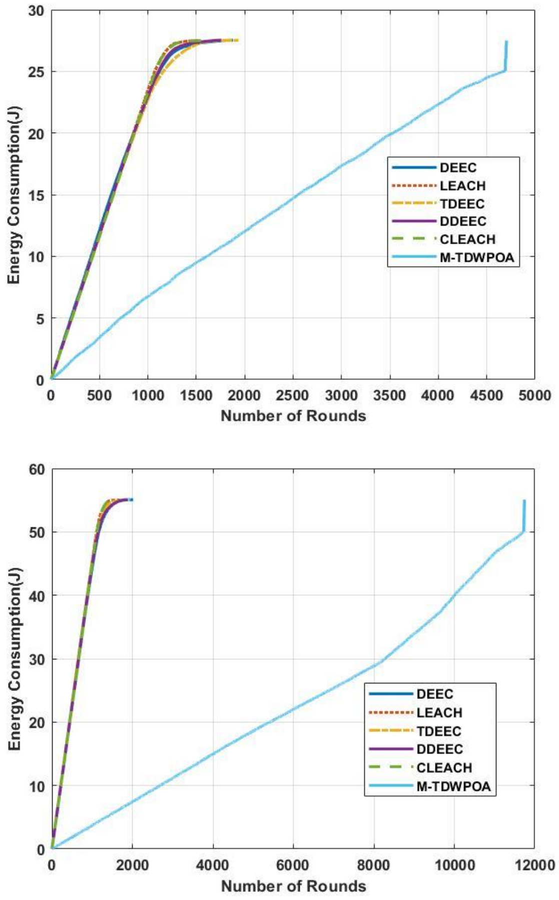


(a) (b)

Figure. 4, Dead nodes analysis (a) 50 nodes and (b) 100 nodes

4.1.3 Energy Consumption

The data transmission among the nodes in WSN utilizes an energy, hence, the node having maximum energy is selected for an estimation.Figure 5 (a) and 5 (b) represents the performance analysis of energy consumption with 50 and 100 nodes. The proposed M-TDWOA is estimated with the various number of rounds like from 0 to 5000 respectively. If the number of rounds is increases, the consumption of an energy are increases. The energy consumption of proposed M-TDWOA is verified with the previous approaches like DEEC, LEACH, TDEEC, DDEEC and CLEACH. Figure 5 shows the proposed M-TDWOA approach attains minimum energy consumption as compared to DEEC, LEACH, TDEEC, DDEEC and CLEACH.

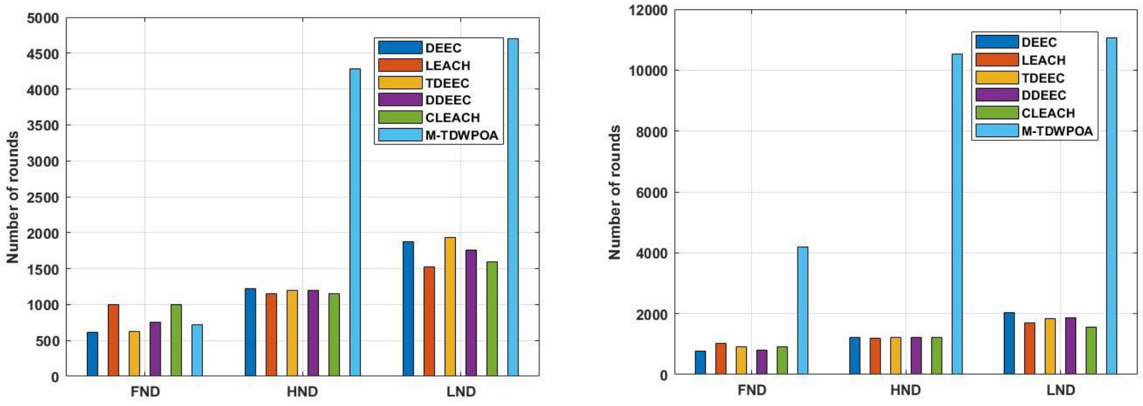


(a) (b)

Figure. 5. Energy consumption analysis (a) 50 nodes and (b) 100 nodes

4.1.4 FND, HND, LND

Figure 6 (a) and 6 (b) represents the performance analysis of FND, HND and LND with 50 and 100 number of nodes. The proposed M-TDWOA is estimated with the various number of rounds like from 0 to 5000 respectively. The FND, HND and LND of proposed M-TDWOA is verified with the previous approaches like DEEC, LEACH, TDEEC, DDEEC and CLEACH. Figure 5 shows the proposed M-TDWOA approach attains high FND, HND and LND as compared to DEEC, LEACH, TDEEC, DDEEC and CLEACH.



(a) (b)

Figure 6. FND, HND, LND analysis (a) 50 nodes and (b) 100 nodes

4.1.5 Packet Delivery Ratio

PDR postulates the percentage of data packets which are effectively distributed to BS by SN range. Figure 7 represents the performance analysis of PDR for both 50 and 100 number of nodes. The PDR of proposed M-TDWOA is verified with the previous approaches like DEEC, LEACH, TDEEC, DDEEC and CLEACH. Figure 5 shows the proposed M-TDWOA approach attains more PDR as compared to DEEC, LEACH, TDEEC, DDEEC and CLEACH. The proposed M-TDWOA attains the 98% of PDR in both 50 and 100 nodes.

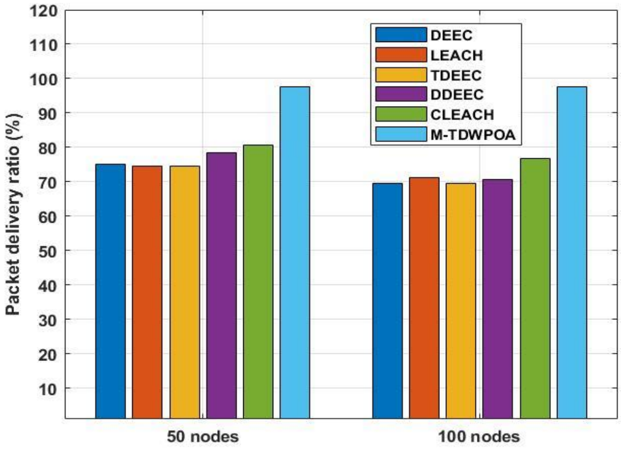


Figure. 7. Performance analysis of Packet Delivery Ratio with 50 and 100 nodes

4.1.6 Packet Loss Ratio

PLR depicts the ratio of lost packets numbers to the total transmitted packets number. Figure 7 represents the performance analysis of PLR for both 50 and 100 number of nodes. The PDR of proposed M-TDWOA is verified with the previous approaches like DEEC, LEACH, TDEEC, DDEEC and CLEACH. Figure 5 shows the proposed M-TDWOA approach attains less PLR as compared to DEEC, LEACH, TDEEC, DDEEC and CLEACH. The proposed M-TDWOA attains the 2% of PLR in both 50 and 100 nodes.

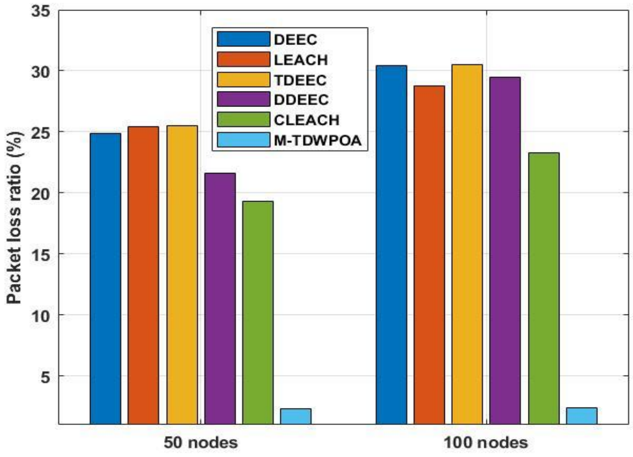


Figure. 8. Performance analysis of Packet Loss Ratio with 50 and 100 nodes

4.1.7 Throughput

Throughput expresses an amount of data packets transmission by the channel regarding specific time intervals. It is measured by bits per second. Figure 9 shows the throughput analysis of proposed M-TDWOA with DEEC, LEACH, TDEEC, DDEEC and CLEACH. The proposed M-TDWOA attains the high throughput when compared to the previous methods like DEEC, LEACH, TDEEC, DDEEC and CLEACH.

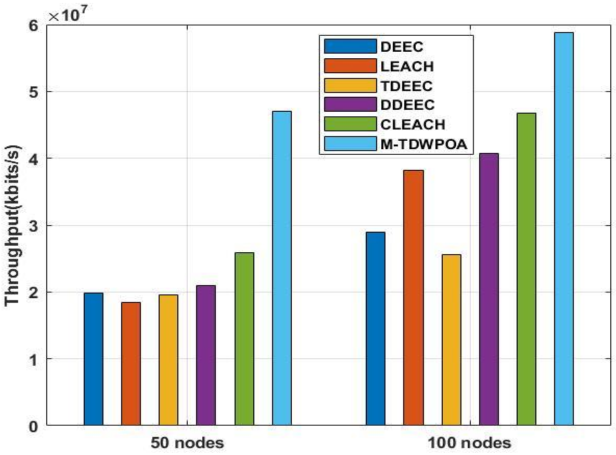


Figure. 9. Performance analysis of Throughput with 50 and 100 nodes

4.2 Comparative Analysis

Table 2 represents the outcomes of previous works with proposed method based on the various metrics. The efficiency of the proposed method is compared with the previous works like Taylor C-SSA [19], TBEBR [22] and FAL [23] based on various number of nodes 50 and 100 respectively. The outcomes in maximum metrics with various number of nodes shows the better performance in proposed method. Hence, the proposed method is an efficient model to enhance the energy and trust aware routing in WSN.

Table 2 shows the simulation parameters of the different scenarios. The different scenarios like 1, 2, and 3 are depicted as Taylor C-SSA [19], TBEBR [22] and FAL [23] respectively. These different scenarios are compared with the proposed M-TDWPOA for estimating the efficacy of the model. Table 3, 4, and 5 shows the comparison of proposed -TDWPOA with Taylor C-SSA [19], TBEBR [22] and FAL [23]. The proposed M-TDWPOA performance results is compared with Taylor C-SSA [19] and FAL [23] using the number of rounds of 200, 400, 600, 800 and 1000 respectively. The proposed M-TDWPOA performance results is compared with TBEBR [22] using the number of rounds of 20, 40, 60, 80 and 100 respectively. The justification of the malicious nodes utilizing trust metric in M-TDEPOA supports to eliminate the unnecessary energy utilization.

Table 2. Simulation parameter with the different scenarios

Parameters	Scenarios		
	1	2	3
Area	$100 \times 100m$	$100 \times 100m$	$100 \times 100m$
No. of nodes	50,100	20, 40, 60, 80, 100	100, 150, 200
Initial energy	0.55J	2J	0.5

Table 3. Comparison of proposed M-TDWPOA with Taylor C-SSA [19]

Scenario	Method	Performance	Number of nodes	Number of rounds				
				200	400	600	800	1000
1	Taylor C-SSA [19]	Number of alive nodes	50	50	50	48	43	32
			100	100	92	86	69	65
		Delay (Sec)	50	0.32	0.38	0.39	0.41	0.42
			100	0.31	0.37	0.38	0.40	0.41
		Residual Energy (J)	50	0.53	0.45	0.38	0.33	0.30
			100	0.52	0.42	0.36	0.28	0.24
		Throughput	50	1	1	1	1	1
			100	1	1	1	1	1
	ProposedM-TDWPOA	Number of alive nodes	50	50	50	49	48	48
			100	100	100	100	100	100
		Delay (Sec)	50	0.0004	0.004	0.06	0.1	0.15
			100	0.004	0.08	0.12	0.19	0.26
		Residual Energy (J)	50	0.543	0.482	0.455	0.402	0.387
			100	0.535	0.48	0.47	0.462	0.448
		Throughput (ratio)	50	1	1	1	1	1
			100	1	1	1	1	1

Table 4. Comparison of proposed M-TDWPOA with TBEBR [22]

Scenario	Method	Performance	Number of nodes	Number of rounds				
				200	400	600	800	1000
2	TBEBR [22]	Residual Energy (%)	20	90	85	76	75	70
			40	92	89	80	79	72
			60	95	88	87	81	75
			80	95	90	89	82	79
			100	98	91	89	80	72
	Proposed M-TDWPOA	Residual Energy (%)	20	99.1	93.97	90.43	85.87	80.21
			40	99.02	96.54	92.42	90.13	86.21
			60	98.21	95.32	90.32	88.43	83.21
			80	97.43	95.23	90.322	87.64	84
			100	99.12	97.21	96.98	96.05	95.21

Table 5. Comparison of proposed M-TDWPOA with FAL [23]

Scenario	Method	Performance	Number of nodes	Number of rounds				
				200	400	600	800	1000
3	FAL [23]	Alive Nodes	100	98	82	65	43	33
		Energy Consumption (J)		0.39	0.28	0.20	0.16	0.14
		Throughput (%)		96.5	95.7	95	93.8	91.5
	Proposed	Alive Nodes	100	100	100	100	100	100

	M-TDWPOA	Energy consumption (J)		0.4927	0.4851	0.4771	0.4693	0.4617
		Throughput (%)		97.43	96.26	96.01	95.14	93.75

4.3 Discussion

The limitations of the existing approaches andthe advantages of the proposed algorithm in secure CH and routing selection are described. The Taylor C-SSA [19] had incompetent to optimize efficient path selection. EATMAR [20] failed to examine the more objective function for achieving the efficient routing. Taylor-SHO [21] failed to determine an analysis of computation overhead. TBEBR [22] had minimum resource accessibility, partial communication as well as minimum energy constraints. FAL [23] near-death nodes were not examined for clustering to acquire efficient system performance. The proposed M-TDWPOA method tackle these limitations by utilizing the secure and energy-aware clustering and routing selection in WSN by updating the dynamic weight in the prey of POA. Inproposed M-TDWPOA achievedminimum delay because of the development of minimum path and utilization ofthe control packet in route path selection.

V.CONCLUSION

Since security in WSN is interesting because of the existence of malicious nodes. However, trust-aware routing plans provides the efficient security with minimum complexity. In this research, the M-TDWPOA approach is proposed for the dynamic secure and EEC and routing discovery in WSN. Moreover, M-TDWPOA approach utilizes the clustering-based routing approach to enhance the energy consumption as well as network lifetime. The optimal route path selection is identified by multi-objective functions such as Distance between neighbor nodes, Distance between BS to CH, Energy, Centrality and Trust Threshold. The secure selection of CH and routing discovery is attained effectively by the M-TDWPOA. The value with best fitness function is taken an optimal route for the transmissionof data and the routing discovery is performed through simulated WSN. The experimental results shows that the proposed method attains efficient results in overall performance metrices. The proposed M-TDWPOA achieves the minimum energy consumption of 0.4927J, 0.4851J, 0.4771J 0.4693J and 0.4617J. In future, the proposed method will expand to the security model based on clustering and routing protocol is implemented for enhancing security.

REFERENCES

[1] 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.

[2] Refaee, E.A. and Shamsudheen, S., 2022. Trust-and energy-aware cluster head selection in a UAV-based wireless sensor network using Fit-FCM. *The Journal of Supercomputing*, pp.1-16.

[3] Bangotra, D.K., Singh, Y., Selwal, A., Kumar, N. and Singh, P.K., 2022. A trust based secure intelligent opportunistic routing protocol for wireless sensor networks. *Wireless Personal Communications*, *127*(2), pp.1045-1066.

[4] Nirmaladevi, K. and Prabha, K., 2023. A selfish node trust aware with optimized clustering for reliable routing protocol in manet. *Measurement: Sensors*, *26*, p.100680.

[5] Natesan, G., Konda, S., de Prado, R.P. and Wozniak, M., 2022. A hybrid mayfly-Aquila optimization algorithm-based energy-efficient clustering routing protocol for wireless sensor networks. *Sensors*, *22*(17), p.6405.

[6] Nagaraju, R., Goyal, S.B., Verma, C., Safirescu, C.O. and Mihaltan, T.C., 2022. Secure routing-based energy optimization for IOT application with heterogeneous wireless sensor networks. *Energies*, *15*(13), p.4777.

[7] Renuga Devi, R. and Sethukarasi, T., 2022. Develop Trust-Based Energy Routing Protocol for Energy Efficient with Secure Transmission. *Wireless Personal Communications*, pp.1-28.

[8] Pathak, A., Al-Anbagi, I. and Hamilton, H.J., 2022. An adaptive QoS and trust-based lightweight secure routing algorithm for WSNs. *IEEE Internet of Things Journal*, *9*(23), pp.23826-23840.

[9] Hosseinzadeh, M., Yoo, J., Ali, S., Lansky, J., Mildeova, S., Yousefpoor, M.S., Ahmed, O.H., Rahmani, A.M. and Tightiz, L., 2023. A cluster-based trusted routing method using fire hawk optimizer (FHO) in wireless sensor networks (WSNs). *Scientific Reports*, *13*(1), p.13046.

[10] Dinesh, K. and Svn, S.K., 2024. GWO-SMSLO: Grey wolf optimization-based clustering with secured modified Sea Lion optimization routing algorithm in wireless sensor networks. *Peer-to-Peer Networking and Applications*, pp.1-27.

[11] 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*, *11*(4), pp.404-413.

[12] Sudha, G. and Tharini, C., 2023. Trust-based clustering and best route selection strategy for energy efficient wireless sensor networks. *Automatika*, *64*(3), pp.634-641.

[13] Veerabadrappa, K. and Lingareddy, S.C., 2022. Trust and Energy Based Multi-Objective Hybrid Optimization Algorithm for Wireless Sensor Network. *International Journal of Intelligent Engineering & Systems*, *15*(5).

[14] Sajan, R.I., Christopher, V.B., Kavitha, M.J. and Akhila, T.S., 2022. An energy aware secure three-level weighted trust evaluation and grey wolf optimization-based routing in wireless ad hoc sensor network. *Wireless Networks*, *28*(4), pp.1439-1455.

[15] Dinesh, K. and Santhosh Kumar, S.V.N., 2023. Energy-efficient trust-aware secured neuro-fuzzy clustering with sparrow search optimization in wireless sensor network. *International Journal of Information Security*, pp.1-25.

[16] Han, Y., Hu, H. and Guo, Y., 2022. Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm. *IEEE Access*, *10*, pp.11538-11550.

[17] Nagarajan, M.K., Janakiraman, N. and Balasubramanian, C., 2022. A new routing protocol for WSN using limit-based Jaya sail fish optimization-based multi-objective LEACH protocol: an energy-efficient clustering strategy. *Wireless Networks*, *28*(5), pp.2131-2153.

[18] Fang, W., Zhang, W., Yang, W., Li, Z., Gao, W. and Yang, Y., 2021. Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. *Digital Communications and Networks*, *7*(4), pp.470-478.

[19] Vinitha, A. and Rukmini, M.S.S., 2022. Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm. *Journal of King Saud University-Computer and Information Sciences*, *34*(5), pp.1857-1868.

[20] Yin, H., Yang, H. and Shahmoradi, S., 2022. EATMR: an energy-aware trust algorithm based the AODV protocol and multi-path routing approach in wireless sensor networks. *Telecommunication Systems*, *81*(1), pp.1-19.

[21] R. Aruna; M. Shyamala Devi; S. Vinoth Kumar.,2023. Efficient Packet Flow Path Allocation Using Node Proclivity Tracing Algorithm. *Lecture Notes in Networks and Systems book series (LNNS,volume 600)*

[22] Kalburgi, S.S. and Manimozhi, M., 2022. Taylor-spotted hyena optimization algorithm for reliable and energy-efficient cluster head selection based secure data routing and failure tolerance in WSN. *Multimedia Tools and Applications*, *81*(11), pp.15815-15839.

[23] Renuga Devi, R. and Sethukarasi, T., 2022. Develop Trust-Based Energy Routing Protocol for Energy Efficient with Secure Transmission. *Wireless Personal Communications*, pp.1-28.

[24] Suman Prakash, P., Kavitha, D. and Chenna Reddy, P., 2022. Safe and secured routing using multi-objective fractional artificial lion algorithm in WSN. *Concurrency and Computation: Practice and Experience*, *34*(21), p.e7098.

[25] Wang, Z., Duan, J., Xu, H., Song, X. and Yang, Y., 2023. Enhanced pelican optimization algorithm for cluster head selection in heterogeneous wireless sensor networks. *Sensors*, *23*(18), p.7711.

[26] Alamir, N., Kamel, S., Megahed, T.F., Hori, M. and Abdelkader, S.M., 2023. Developing hybrid demand response technique for energy management in microgrid based on pelican optimization algorithm. *Electric Power Systems Research*, *214*, p.108905.