Trust-Based Energy-Efficient Routing Using Mud Ring Optimization in Wireless Sensor Network

Maradona N[1,*] and Jaya T[2]

[1]Dept. Information and Communication Engineering, Saveetha Engineering College in Chennai, Tamil Nadu
[2]Dept. Electronics and Communication Engineering, Saveetha Engineering College in Chennai, Tamil Nadu
Email: nmardona@gmail.com (M.N.); jayacsiramesh@gmail.com (J.T.)
[*]Corresponding author
Manuscript received April 29, 2024; revised May 10, 2024; accepted June 3, 2024; published June 24, 2024.

***Abstract*—One of the most challenging tasks in constructing a routing model for a Wireless Sensor Network (WSN) is ensuring energy efficiency. Various energy-efficient routing strategies are developed to guide data packets across Cluster Heads (CH) along secure paths. However, within the context of a WSN, achieving both network longevity and substantial scalability proves to be a formidable challenge. Traditional trust-based routing solutions are inadequate in offering security against attacks, and as a result, trust management remains a significant obstacle in routing. To address the need for routing data packets securely and efficiently to their intended receivers, a novel routing model is devised. This model employs the Trust Routing based on Mud Ring Optimization (TR-MRO) algorithm. By incorporating the principles of the TR-MRO algorithm, which takes into account recent trust, direct trust, indirect trust, and probability requirements, the proposed model guides the routing process through CHs. Through the TR-MRO algorithm, the most optimal and secure path for data transfer is determined based on fitness considerations. The performance of the proposed network is evaluated in terms of several key metrics, including network lifetime (3050 rounds), delay (0.03s), throughput (0.93kbps), trust (0.9), and packet delivery ratio (0.98). The evaluation is conducted in comparison to existing models, highlighting the effectiveness of the proposed approach.**

***Keywords*—WSN Routing, trust routing, mud ring optimization, energy efficiency and network lifetime**

I. Introduction

WSNs are self-organizing network domains that can accommodate many inexpensive nodes with wireless communication and data processing capabilities. The adaptable, low-cost emergent technology utilized for environmental monitoring is called WSN [1]. In order to perceive the network scenario for the purposes of data collection and communication, it is made up of a variety of small devices known as sensor nodes that are dispersed throughout the geographical region and have limited battery life, storage capacity, and computational complexity [2]. The sensor node was subject to a number of restrictions regarding its memory and storage capacity as well as its energy and computing resources. The main concerns in WSN are power consumption and security that invokes for greater attention. Due to the accessibility of sensor nodes' lower battery power levels, power optimization is a key performance parameter in WSNs [3, 4].

Attacks like a black hole and grey-hole denial of service, distributed denial of service assault (DDoS) [5], cross-site scripting, network sniffing, etc., pose a threat to MANET. There are two types of assaults that can be particularly damaging to cloud networks: black holes (false reports) and grey holes (packet drops) [6]. In a black hole attack, a malicious node advertises itself as having the shortest path to the destination and then absorbs all incoming traffic without forwarding it, essentially dropping all the packets. Gray-hole attacks are more sophisticated. It involves the intentional dropping of data packets at a predetermined rate, such as one every t seconds or every n packet end route to a specific target on the network [7]. Malicious nodes selectively drop packets rather than dropping all of them, making it harder to detect. This attack can be more difficult to mitigate as it subtly disrupts communication [8].

The researchers have also created a different set of protocols to protect WSNs from malicious assaults. Instead of using cryptosystems, these protocols rely on reputation- and trust-based systems to secure the data that the node transmits [9]. These protocols work by enabling the best use possible of the computational power that the sensor nodes have at their disposal. These methods are distinctive to ensure effectiveness against malicious assaults since their operational success depends on trust assessment [10]. These trust-based techniques are employed in the routing process to choose the subsequent forwarder node. This trust-based method's characteristic makes trust-based techniques particularly suited to be integrated with the WSN's routing protocol [11].

Lightweight Secure Routing (LSR) was suggested for WSNs by Pathak *et al.* [12] to deal with security, QoS, and energy efficiency issues. To solve the energy-hole issue, LSR uses Ant Colony Optimization (ACO), adaptive security and QoS models, and a hybrid deployment approach. The results of simulations show that LSR is superior to existing strategies in terms of energy consumption, trust convergence, network longevity, routing delay, and packet delivery. It also outperforms them in terms of network scalability and security risk assessments. Using clustering and routing, Sudha and Tharini [13] concentrated on energy-efficient WSN systems. The Lion Optimization Algorithm (LOA) is utilized for route selection, and the Dempster-Shafer Theory (DST) is used for node clustering. Elephant Herding Optimization (EHO) and Low Energy Adaptive Clustering Hierarchy (LEACH) routing were combined for improved security and performance by Veerapaulraj *et al.* [14] to overcome WSN problems. The average packet loss rate can be reduced by up to 35.42% with the proposed Trust EHO-based routing, increasing network longevity and efficiency.

With an emphasis on improved security and information management, Abualkishik *et al.* [15] presented Trust Aware Aquila Optimizer based Secure Data Transmission for

Information Management (TAAO-SDTIM) in WSNs. The proposed technique chooses the most secure node for data transmission by optimizing paths to a base station while taking into account characteristics like trust level, distance, and residual energy. In order to identify the best cluster head (CH), Suman Prakash *et al.* [16] developed a secure routing strategy for Wireless Sensor Networks (WSNs) using the Fractional Artificial Lion algorithm (FAL). To improve CH determination based on factors such latency, energy, distance, and connection lifetime, FAL blends fractional calculus, the LOA), and Artificial Bee Colony (ABC) approaches. To improve WSN performance, the TE-MHOA technique, which combines energy- and trust-based multi-objective hybrid optimization algorithms (APSO-MBO), is introduced [17]. The suggested method uses multipath routes, intra-cluster, and inter-cluster transmission to increase metrics like throughput (1089.97 Kbps), latency (0.014 ms), and other performance indicators.

Nodes in WSNs gather data from various surroundings and use swarm connectivity to transport data. Routers make data transmission more effective. Traditional methods priorities routing that is energy-efficient but have security issues. Convolutional neural networks (CNNs) are used to pick reliable cluster heads, strengthening security by recognizing and rejecting hostile nodes, and enhancing overall data transmission reliability. Kavitha and Ganapathy [18] pioneered this novel method. By merging Blockchain-based routing with a Deep Generative Adversarial Neural Network (DGANN) that has been upgraded by the Jellyfish Search Optimizer algorithm (JSOA), Raja and Periasamy [19] presented a novel method to address security and efficiency issues in WSNs. The suggested method optimizes DGANN weight parameters with JSOA for better network performance, mitigating malicious attacks and the black hole issue during data transfer. Sensor nodes in WSNs have limited computing power, energy, and battery replacement options. The topology of the network is altered when certain nodes run out of power. There may even be a point where the network system becomes paralyzed and unable to function correctly due to an excessive number of dead nodes. Designing energy-balanced and energy-efficient routing protocols is therefore crucial for WSNs in order to extend the network lifetime.

The development and application of a trust-based, energy-efficient routing model for WSNs is the main contribution of this study. Through the use of CHs, this approach addresses the problem of maximizing network longevity and scalability. The contributions are as follows,

- To introduce the Trust Routing based on Mud Ring Optimization (TR-MRO) algorithm, which dynamically chooses CHs based on recent trust, direct trust, indirect trust, and probability values. As a result, data transmission follows an ideal and secure path.
- Integrating energy economy and trust management, the suggested model enhances the network's resistance to attacks and ensures dependable communication by optimizing routing patterns while taking trustworthiness into account.
- To demonstrate the efficiency of the proposed model through a comprehensive performance evaluation. The analysis includes metrics such as network lifetime, low delay, high throughput, trustworthy routing, and excellent PDR.
- The study conducts a thorough comparison with existing models as T-EHO, DST-LOA, TE-MHOA and LSR-ACO, showcasing the superior performance and benefits of the proposed TR-MRO algorithm in terms of energy efficiency, trust-based routing, and network reliability.

The remainder of the article is structured as Section II describes the energy model and routing constraints. Section III explains the process of proposed routing algorithm. Section IV describes the analysis of proposed system results and finally, Section V concludes the proposed model.

II. Proposed System

A. Network Model

A WSN consists of m sensor nodes and a base station (BS), which serves as the sink node. The wireless links serve as a representation of the direct communication between sensor nodes. Each node in the network is uniformly distributed and has its unique ID, allowing the nodes to be divided into clusters [20]. The sink node is positioned as closely as possible to where it will receive data bytes from other network nodes that are normally connected. The routing system based on CH is used to transmit data from each sensor node to the base station. There are G clusters divided up into the network. After the network has formed cluster groups, each node can send data packets to its associated CH so that CH can gather data packets from cluster members. CH forwards the data packets it has collected to BS. Fig. 1 shows the structure of proposed methodology.

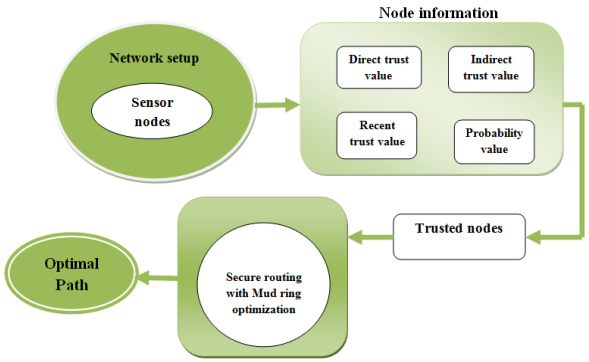

Fig. 1. Architecture of proposed methodology.

B. Energy Model

The protocol and energy dissipation are required for network communication, which is made possible by the presence of radio electronics and a power amplifier available in the transmitter. Thus, it is evident that the distance and nature of the node are factors in how the energy disperses during the time of transmission. The model for energy consumption is based on Eq. (1) whenever a typical sensor node sends a p-bit data packet.

$$H_t(p) = H_e(p) + H_a(p,d) \quad (1)$$

where, consumed energy, transmitted energy and consumed energy when the node receives are represented as H_a, H_t ,

and H_e , respectively. Then the data bits and communication distance are denoted as p and d , respectively.

The energy used by the sensor nodes to receive the p bits of data are specified as,

$$H_r(p) = p \times H_e \tag{2}$$

where the received energy is denoted as $H_r(p)$. Then the total energy is computed by sum of transmitted and received energy.

C. Trust Model

By enabling effective and safe routing in WSN, the trust model offers security. To determine the collection of trusted nodes, the trust factor of each node is assessed. As a result, T provides a model of the trust factor that is tailored for identifying the trusted nodes present in the Zth path. This model is based on three factors: indirect trust, direct trust, and recent trust. Eq. (3) uses the trust values to get the trust factor.

$$Trust = T_D + T_I + T_R \tag{3}$$

where, T_R , T_I and T_D refers to the recent trust, indirect trust and direct trust, respectively.

The three WSN properties that make up the trust value metric are used to determine if a node is likely to be malicious (M_{node}). By accounting for the number of data packets missed throughout the WSN's data transmission process, the likelihood of a sensor node being compromised or otherwise impacted is assessed. As seen below, the likelihood is calculated.

$$M_{node} = (1 - R_F) - R_{delay} \tag{4}$$

Here, R_F stands for the ratio of ineffective forwarding of packets, divided by the number of packets sent to a node calculated by Eq. (5)

$$R_F = \frac{P_n}{P_s} \tag{5}$$

$$R_{delay} = \frac{N_{delay}}{P_s} \tag{6}$$

where, number of packets declined by the node is P_n , number of packets directed towards the same node is P_s and slowed down number of packets by a node is N_{delay} .

D. Direct Trust

In the case of two nearby nodes, direct trust is the outcome of independent or local trust assessment. The forwarding ratio is used to compute the node trust since it is simple to utilize and has less overhead. The number of appropriately forwarded packets divided by the number of unforwarded packets is known as the forwarding ratio. Based on Eq. (7), the direct trust depending on the forwarding ratio is computed

$$T_D^{(x,y)}(t) = \frac{B^{x,y}(t)}{C^{x,y}(t)} \tag{7}$$

where, $C^{x,y}(t)$ denotes the count of packets effectively received by the node y from the node x and $B^{x,y}(t)$ denotes the correctly forwarded packets by the node y to the node x at time t .

E. Indirect trust

The indirect trust is established based on suggestions and is calculated from the knowledge of other agents in the system that has used target nodes to make operational decisions. The opinions of other nodes are considered when evaluating it. The node starts off by asking other nodes for recommendations regarding the target node. The assessed node compiles the suggestions made by other nodes. The node x obtained the following indirect trust from node y ,

$$T_I^{x,y}(t) = \frac{1}{u}\sum_{k=1}^{u} T_D^{x,y}(t) \tag{8}$$

where, u indicates the neighbors of a node x such that $1 \le k \le u$.

F. Recent Trust

Recent trust, which takes into account a weighted combination of both direct and indirect trust, duplicates the most recent behaviors. Since there are more interactions between the computing agent and the targeted agent in this case, the direct trust is given more weight. Furthermore, the evaluation turns out to be more confident about the event than the alluring advice from others. Assume that $T_R^{x,y}$ represents the most recent instance of the node x having faith in the node y .

$$T_R^{x,y} = \beta \times T_D^{x,y} + (1-\beta) \times T_I^{x,y} \tag{9}$$

where, the weight of direct trust β is computed by Eq. (10),

$$\beta = \frac{P_1^{x,y}}{P^{x,y} + K^{x,y}} \tag{10}$$

where, $P_1^{x,y}$ indicates the count of interaction agent u in tth interval, and $K^{x,y}$ indicate the mean number of interactions that other agents have conducted with the agent u . The suggested approach makes use of a threshold-based trust rating model to compute qualitative trusted nodes in order to achieve encrypted communications through routing choices. The trust rating system is employed in this case to rank the top and lowest trust values produced by the computing procedure. This approach aids in providing trusted nodes to provide secure communication.

Based on the trust values with respect to Eq. (3), the nodes will be categorized into five categories which are formulated as, $T = \{T1, T2, T3, T4, T5\}$ where, $T1$ indicates no trust which is considered in the range $0 \le T1 \le 0.25$, T2 indicates poor trust, which is considered in the range $0.26 \le T2 \le 0.5$, T3 indicates fair trust which is considered in the range $0.51 \le T3 \le 0.75$, T4 indicates good trust, which is considered in the range $0.76 \le T4 \le 0.9$, and T5 indicates complete trust, which is considered in the range $0.91 \le T5 \le 1$.

G. Probability Computation

The proposed clustering technique involves selecting Cluster Heads (CH) based on node energy parameters. Nodes generate random numbers between 0 and 1, comparing them to a threshold function to determine if they become CH for a round. The threshold function considers CH selection probability, initial energy, round number, and residual energy. The goal is to pick energy-efficient CH nodes each round to prolong network lifespan, promoting efficient energy usage. Nodes not chosen as CH in one round have chances in subsequent rounds. This approach optimizes CH selection, enhancing network longevity. The threshold functions for normal and advance nodes are represented by Tnorm(n) and Tadvan(n).

The advance and normal nodes threshold functions are represented as N_n and A_n, respectively. The normal node threshold is computed by Eq. (11),

$$T(N_n) = \begin{cases} \dfrac{P_n}{1 - P_n\left[\left(r \bmod \dfrac{1}{P_n}\right)\right]} \times \dfrac{H_{ini}}{H_{res}}, & if\ n \in G \\ 0, & otherwise \end{cases} \quad (11)$$

where, nodes remaining energy is H_{res}, initial energy is H_{ini}, rounds is r and non CH group is denoted as G.

Probability of normal nodes for becoming CH P_n is computed by Eq. (12),

$$P_n = \frac{P_{opt}}{1 + a(m)} \quad (12)$$

The threshold function for advance node is computed by Eq. (13),

$$T(A_n) = \begin{cases} \dfrac{P_A}{1 - P_A\left[\left(r \bmod \dfrac{1}{P_A}\right)\right]} \times \dfrac{H_{ini}}{H_{res}}, & if\ n \in G \\ 0, & otherwise \end{cases} \quad (13)$$

The probability of advance nodes for becoming CH (P_A) is computed by Eq. (14)

$$P_A = \frac{P_{opt} \times (1 + a)}{1 + a(m)} \quad (14)$$

If the node satisfies the threshold function conditions, it gets selected as CH otherwise the process of clustering phase is repeated for the other node for becoming CH.

III. Proposed TR-MRO Algorithm for Energy Efficient Routing

Secure transmission between nodes is provided by the proposed method, called TR-MRO. The TR-MRO that is being developed combines the MRO with trust model to determine the most effective method for data transmission between nodes. For selecting an ideal path, the suggested TR-MRO makes use of a recently developed fitness function. The fitness function is designed to find a secure path using criteria like energy, distance, and trust. With direct trust, indirect trust, recent trust, and a probability model, the trust factor is calculated. The nodes are divided into five categories based on the trust factor's value: no trust, low trust, fair trust, good trust, and total trust. For the routing operation, the nodes with complete and good trust are utilized. Thus, the proposed TR-MRO algorithm utilizes a newly devised fitness function, which involved energy, trust, and distance for choosing the optimal path to accomplish secured transmission. The parameters, like energy, and trust, must be larger and the distance must be reduced to detect the best path.

Consider E and F to be the source and target nodes, respectively, and i to provide the number of trusted nodes required going from the source node to the destination. The paths picked from i nodes to begin transmission between the source and target nodes are shown in the solution vector. Here, g indicates the index of nodes, which lies in $1 \le g \le i$.

A. Objective Function

To choose the best solution from a set of possible solutions, the fitness function is computed. Energy, distance, trust, and likelihood are used to assess the proposed TR-MRO's fitness. To maximize the fitness value for a given solution, where objective function is defined as the weighted sum of trust, energy, and distance (D) of nodes for routing, Eq. (15) expressed the objective function,.

$$obj = w_1 E_x + w_2 D_x + w_3 T_x \quad (15)$$

where, distance, trust value and energy of x^{th} node is represented as D_x, T_x and E_x, respectively. The weights w1, w2, and w3 can be used to adjust the importance of trust, energy, and distance in the overall fitness function according to the routing.

Mud Ring Algorithm (MRA) models this bottlenose dolphin foraging behavior, beginning with the echolocation-based swarm hunt for prey and concluding with the formation of a mud ring for feeding [21].

B. Searching For Prey - Exploration Phase

When looking for prey, dolphins swim randomly while employing velocities $\vec{v}$ at places $\vec{X}$ with a sound loudness $\vec{L}$. All dolphins use echolocation to detect distance. While the loudness may change in a variety of ways, we assume that it changes depending on the time step and the pulse rate r, [0, 1], where 0 indicates no emission pulses and 1 indicates the highest pulse emission rate. All dolphins are able to automatically adjust the loudness of their produced sounds based on how close their prey is. The computation of the vector $\vec{L}$ is,

$$\vec{L} = 2\vec{b} \times \vec{r} - \vec{b} \quad (16)$$

$$\vec{b} = 2\left(1 - \frac{t}{\max_{iter}}\right) \quad (17)$$

The workability $\vec{X}^t$ based on the velocity at time step t is provided in Eq. (18),

$$\vec{X}^t = \vec{X}^{t-1} + \vec{v}^t \quad (18)$$

where, $\vec{r}$ represnts the random number in [0, 1] and v is initialized as a random vector.

C. Mud Ring Feeding- Exploitation Phase

Dolphins can locate and encircle their prey after detecting it. The optimal design's location in the search space is unknown a priori, hence the MRA technique considers the target prey (or a solution that is close to it) as the best option at the moment. Once the best search agent has been identified, the other dolphins will seek to update their positions in accordance with that dolphin. This behavior can be described by Eqs. (19) and (20),

$$\vec{Z} = |\vec{C}\vec{X}^{t-1} - \vec{X}^{t-1}| \quad (19)$$

$$\overrightarrow{X^{t}} = \vec{X}^{t-1} \times \sin(2\pi l) - \vec{L}\vec{Z} \quad (20)$$

Here, $\vec{L}$ and $\vec{C}$ re the coefficient vectors, dolphin position vector and best position is represented as $\overrightarrow{X^{t}}$ and $\vec{X}^{t-1}$. The optimization process is validated to have ended when the end criterion is met. The end criterion, which includes the maximum number of iterations, the improvement percentage, and the execution duration, is established to ensure that the algorithm converges more effectively.

IV. Result and Discussion

To compare the effectiveness of the suggested method to other similar protocols in the literature, simulations are done using MATLAB. Utilizing MATLAB simulation environment allowed for greater analysis in terms of average findings and comparison analysis. The proposed method is assessed in terms of network longevity, delay, trust, PDR, and throughput to demonstrate the network's effectiveness. The simulation parameters are shown in Table 1.

Table 1. Simulation parameters

Parameters	Values
Area	500×500m
Total number of nodes	100
Malicious nodes	50
Initial nodes energy	0.5J
Threshold energy	0.2J
Trust value initial	1

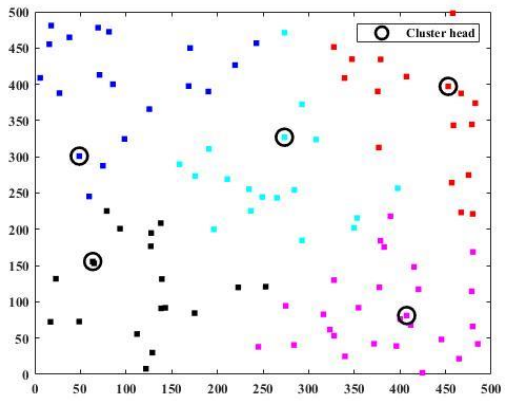

Fig. 2. Cluster head selection.

In clustering-based networks, nodes are grouped into clusters to improve network efficiency and reduce energy consumption. Each cluster typically has one node called the "cluster head" responsible for managing and coordinating the cluster. Fig. 2 shows the cluster head selection with the choice of 5 cluster heads. In this context, 5 heads chosen, it likely refers to the selection of a specific number of cluster heads from a group of nodes or devices within the network. In this process, a subset of sensor nodes is chosen to act as cluster heads, responsible for managing and aggregating data from other nodes within their clusters. This selection is often based on various criteria like node energy, connectivity, or location. Choosing five cluster heads can help distribute the network's management tasks effectively. These cluster heads play a vital role in data routing, and resource allocation, ultimately improving the network's efficiency, energy consumption, and overall performance. Proper cluster head selection is essential for prolonging network lifespan and maintaining reliable communication in resource-constrained environments.

A. Network Lifetime

Network lifetime is the period of time from the deployment of nodes until the first node fails due to energy depletion. Energy usage has an adverse relationship with network longevity. The comparative analysis of network lifetime is shown in Fig. 3.

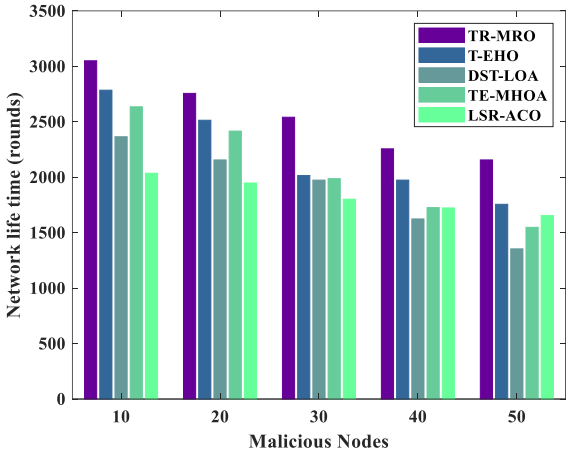

Fig. 3. Network lifetime vs malicious nodes.

This evaluation takes into account the existence of 50 malicious nodes and measures the network lifetime in terms of rounds. This comparison focuses on how well the TR-MRO strategy performs when compared to a number of current networks, including T-EHO [14], DST-LOA [13], TE-MHOA [11], and LSR-ACO [12]. A negative scenario is introduced by 50 malicious nodes, which may affect the network's overall performance, effectiveness, and dependability. In order to show the superiority of our suggested strategy in sustaining a longer network lifetime despite the existence of malicious nodes, we will contrast the TR-MRO methodology against these existing networks.

B. Trust Analysis

If a node is trustworthy for routing the data bytes depends on the trust factor. The ability of the node to transfer data reliably and securely is implied by a higher trust value. Analyses of trustworthy vs. malicious nodes are presented in Fig. 4. While taking into account the presence of a predetermined number of malicious nodes (50), this comparison focuses on the variance in trust levels (ranging

from 0.78 to 0.9). Examining how various routing strategies fare when dealing with nodes that have differing degrees of trustworthiness is the goal. The study's goal is to demonstrate the effectiveness of the suggested TR-MRO technique in maintaining reliable routing, even in the presence of malicious nodes, when compared to the other available strategies by analyzing the comparison's results (T-EHO, DST-LOA, TE-MHOA, and LSR-ACO). The focus on trust levels gives the evaluation a crucial new dimension because it reflects real-world situations where nodes may display different levels of dependability and security.

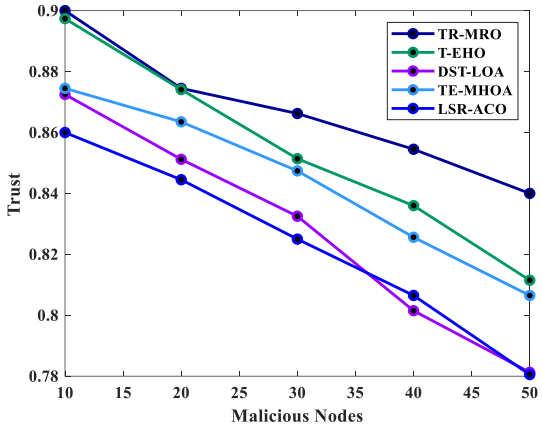

Fig. 4. Trust (0.78 to 0.9) vs malicious nodes (50).

C. Throughput Analysis

Throughput values, which provide the total amount of data packets received at a moment and identify the packet delivery, are used to calculate how the approaches would behave. According to Fig. 5, the throughput value marginally decreases as the number of malicious nodes rises. The suggested technique achieves (0.93kbps) at 10 malicious nodes, which is faster than the current methods T-EHO (0.90), DST-LOA (0.89), TE-MHOA (0.865), and LSR-ACO (0.875).

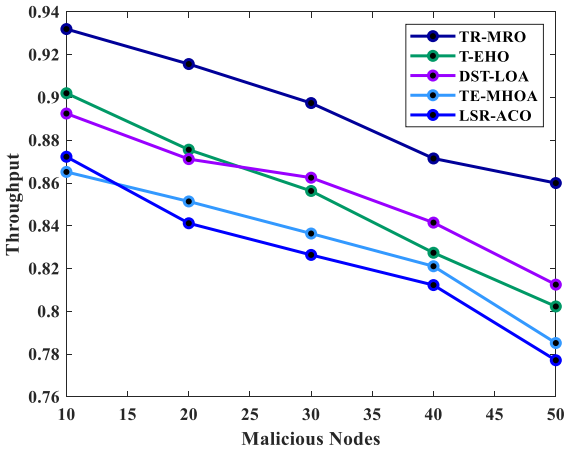

Fig. 5. Analysis of Throughput vs malicious nodes.

D. End-to-End Delay

Average end-to-end delay represents the average time taken by the packets to reach its actual destination. It is determined by taking the packet's origination time and subtracting the time at which it arrives at its destination. Only for successfully transmitted data packets is the End-to-End delay measured. As in the cases of T-EHO, DST-LOA, TE-MHOA, and LSR-ACO, high overhead and complex protocols lead to high-end to end delays. Low delays are achieved in Fig. 6 using TR-MRO, which has lower overhead during calculation. Energy efficiency is the main factor that matters in unattended implementation settings. The most important network tasks, including packet transmissions, receptions, and sending-receiving acknowledgment, will be completed during the routing time, which has an effect on the network's overall energy usage.

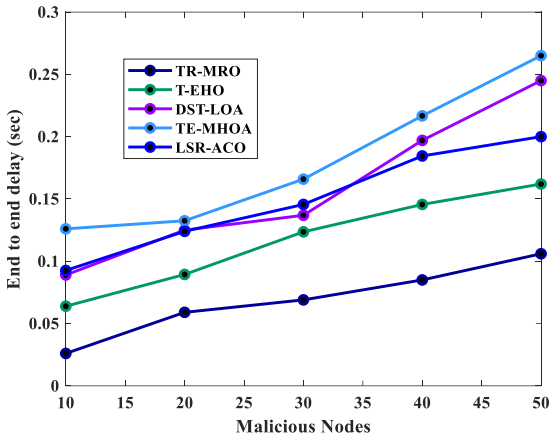

Fig. 6. Analysis of Delay.

E. Packet Delivery Ratio

Utilizing the PDR measure, the ratio of data packets transmitted and received is assessed to determine the routing efficiency. Fig. 7 displays the PDR for each protocol with a varying number of malicious nodes in the network. Given that both protocols can thwart black-hole and grey-hole attacks, the proposed TR-MRO's delivery ratio is practically comparable. All malicious nodes are kept out of the neighbor's list of source nodes by these protocols, and they are all discarded. Due to their inability to effectively handle the growing number of malicious nodes, T-EHO, DST-LOA, TE-MHOA, and LSR-ACO experience substantially reduced packet delivery rates.

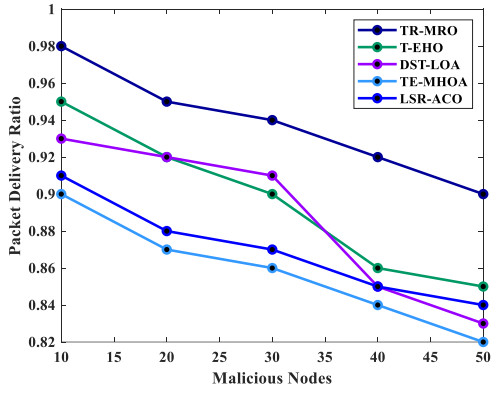

Fig. 7. Analysis of PDR vs malicious nodes.

The PDR decreases with an increase in malicious nodes in a network because malicious nodes intentionally disrupt the communication by dropping or manipulating packets. When there are more malicious nodes, a higher percentage of packets are deliberately discarded or tampered with, leading to a lower PDR. This reduces the overall reliability and efficiency of data transmission in the network, as fewer packets reach their intended destinations successfully.

V. Conclusion

This study addresses the significant challenges of energy efficiency and trust management in designing routing models for WSNs. An energy-efficient and trust-based routing model of TR-MRO algorithm is proposed for optimal path selection. This model efficiently routes data packets through CHs, leveraging the TR-MRO algorithm's selection process based on recent trust, direct trust, indirect trust, and probability values. The TR-MRO algorithm further computes optimal and secure routes for data transfer based on fitness measures. The proposed network's efficiency is validated through a comprehensive performance analysis. Notable achievements include a network lifetime of 3050 rounds, minimal delay of 0.03 seconds, throughput at 0.93 kbps, a high trust level of 0.9, and an exceptional PDR of 0.98. This evaluation demonstrates that the proposed TR-MRO algorithm outperforms existing models, highlighting its effectiveness in achieving energy-efficient, secure, and trustworthy routing in WSNs.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Author Contributions

Maradona.N and Jaya.T jointly conceived the study, designed and conducted the experiments, analyzed the data, and wrote the manuscript. Both authors contributed equally to this work.

References

[1] Z. Wang, H. Ding, B. Li, L. Bao and Z. Yang, "An energy efficient routing protocol based on improved artificial bee colony algorithm for wireless sensor networks," IEEE access, vol. 8, pp. 133577-133596, 2020.

[2] D. Rajesh, and T. Jaya, "Energy competent cluster‐based secured CH routing EC2SR protocol for mobile wireless sensor network," Concurrency and Computation: Practice and Experience, vol. 34, no. 1, pp. e6525, 2022.

[3] K. J. Singh, A. Nayyar, D. S. Kapoor, N. Mittal, S. Mahajan, A. K. Pandit and M. Masud, "Adaptive flower pollination algorithm-based energy efficient routing protocol for multi-robot systems," IEEE Access, vol. 9, pp. 82417-82434, 2021.

[4] D. Rajesh, and T. Jaya, "ECIGC-MWSN: Energy capable information gathering in clustered secured CH based routing in MWSN," Materials Today: Proceedings, vol. 43, pp. 3457-3462, 2021.

[5] M. Kurtkoti, B. S. Premananda, and K. Vishwavardhan Reddy, "Performance analysis of machine learning algorithms in detecting and mitigating black and gray hole attacks," In Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2021, Singapore: Springer Nature Singapore, pp. 945-961, 2022.

[6] S. Venkatasubramanian, A. Suhasini, and S. Hariprasath, "Detection of Black and Grey Hole Attacks Using Hybrid Cat with PSO-Based Deep Learning Algorithm in MANET," International Journal of Computer Networks and Applications (IJCNA), pp. 724-735, 2022.

[7] R. Swami, M. Dave, and V. Ranga, "DDoS attacks and defense mechanisms using machine learning techniques for SDN," In Research Anthology on Combating Denial-of-Service Attacks, IGI Global, pp. 248-264, 2021.

[8] M. M. Hamdi, A. F. Flaih, M. L. Jameel, A. S. Mustafa, A. J. Abdulelah, M. A. Jubair, and A. J. Ahmed, "A study review on Gray and Black Hole in Mobile Ad Hoc Networks (MANETs)," In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), IEEE, pp. 1-6, 2022.

[9] D. Rajesh, and T. Jaya, "A mathematical model for energy efficient secured CH clustering protocol for mobile wireless sensor network," Wireless Personal Communications, vol. 112, no. 1, pp. 421-438, 2020.

[10] D. K. Bangotra, Y. Singh, A. Selwal, N. Kumar and P. K. Singh, "A trust based secure intelligent opportunistic routing protocol for wireless sensor networks," Wireless Personal Communications, vol. 127, no. 2, pp. 1045-1066, 2022.

[11] P. P. Jadhav, and S. D. Joshi, "Atom search sunflower optimization for trust-based routing in internet of things. International Journal of Numerical Modelling," Electronic Networks, Devices and Fields, vol. 34, no. 3, pp. e2845, 2021.

[12] A. Pathak, I. Al-Anbagi, and H. J. Hamilton, "An adaptive QoS and trust-based lightweight secure routing algorithm for WSNs," IEEE Internet of Things Journal, vol. 9, no. 23, pp. 23826-23840, 2022.

[13] G. Sudha, and C. Tharini, "Trust-based clustering and best route selection strategy for energy efficient wireless sensor networks," Automatika, vol. 64, no. 3, pp. 634-641, 2023.

[14] S. Veerapaulraj, M. Karthikeyan, S. Sasipriya, and A. S. Shanthi, "An Optimized Novel Trust-Based Security Mechanism Using Elephant Herd Optimization," Computer Systems Science & Engineering, vol. 44, no. 3, 2023.

[15] A. Z. Abualkishik, and A. A. Alwan, "Trust aware aquila optimizer based secure data transmission for information management in wireless sensor networks," Journal of Cybersecurity and Information Management, vol. 9, no. 1, pp. 40-51, 2022.

[16] P. Suman Prakash, D. Kavitha and P. Chenna Reddy, "Safe and secured routing using multi-objective fractional artificial lion algorithm in WSN," Concurrency and Computation: Practice and Experience, vol. 34, no. 21, pp. e7098, 2022.

[17] K. Veerabadrappa, and S. C. Lingareddy, "Trust and Energy Based Multi-Objective Hybrid Optimization Algorithm for Wireless Sensor Network," International Journal of Intelligent Engineering & Systems, vol. 15, no. 5, 2022.

[18] V. Kavitha, and K. Ganapathy, "Galactic swarm optimized convolute network and cluster head elected energy-efficient routing protocol in WSN," Sustainable Energy Technologies and Assessments, vol. 52, pp. 102154, 2022.

[19] L. Raja, and P. S. Periasamy, "A Trusted distributed routing scheme for wireless sensor networks using block chain and jelly fish search optimizer based deep generative adversarial neural network (Deep-GANN) technique," Wireless personal communications, vol. 126, no. 2, pp. 1101-1128, 2022.

[20] D. Rajesh, and T. Jaya, "Enhancement of network lifetime by fuzzy based secure CH clustered routing protocol for mobile wireless sensor network," Journal of Ambient Intelligence and Humanized Computing, vol. 13, no. 5, pp. 2795-2805, 2022.

[21] A. S. Desuky, M. A. Cifci, S. Kausar, S. Hussain, and L. M. El Bakrawy, "Mud Ring Algorithm: A new meta-heuristic optimization algorithm for solving mathematical and engineering challenges," IEEE Access, vol. 10, pp. 50448-50466, 2022.