Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Clustering Tree Trusted Routing Algorithm Using Improved Coati Optimization Algorithm (Icoa) in Wireless Sensor Network (WSN)

K. Palaniyappan, Dr. D. Suresh

Assistant Professor, Department of Information Technology, Annamalai University, Annamalainagar, India.
Email: skpalaniyappan@gmail.com

Wireless Sensor Network (WSN) is made up of geographically dispersed sensors with the purpose is used to monitor environmental or physical variables. Since sensor nodes are energy-constrained devices, energy-efficient routing methods have developed into gradually more important in recent years. Hierarchical routing methods are suggested to extend network lifetime and reduce energy usage. This study, a clustering tree trusted routing algorithm with improved coati optimization algorithm (ICOA) namely CTTRIC is introduced for WSN. The proposed architecture aims to counter several routing attacks like the flooding attack (FA), wormhole attack (WH), sinkhole attack (SH), black hole attack (BH), and gray hole attack (GH) foe enhancing energy efficiency. Each recommendation's weight is established based on the recommender nodes' degree of trust as well as the difference among the estimated direct trust and the recommended trust. ICOA was implemented to provide reliable and trustworthy communication channels between the Base Station (BS) and Cluster Head (CH). Multi-objective fitness function is computed based on metrics like distance among each CH and its parent node, each CH energy, and its trust level are used to compute the ICOA. CTTRIC system performs well and effectively in terms of energy consumption, end-to-end delay (E2ED), packet delivery ratio (PDR), and Packet Loss Ratio (PLR).

Keywords: Trust routing, Improved Coati Optimization Algorithm (ICOA), Wireless Sensor Network (WSN), clustering tree trusted routing (CTTR) algorithm, and energy-efficient routing approaches.

1. Introduction

The design of the Internet of Things (IoT) requires the use of wireless sensor network (WSN). It uses sensor nodes to continuously monitor certain areas and wirelessly multi-hops the collected data to sink nodes. It has a wide range of potential applications [1,2]. Aim of this routing algorithm is to identify the optimal way from the sensor node to the sink node and accurately transmit monitoring data down the precise path in order to decrease energy consumption and increase network lifetime. Because of their resource limitations many typical wired routing technologies are make them very different from traditional wired networks.

Therefore, intelligent routing is a key and necessary phenomenon for increasing the Quality of Service (QoS) in a WSN-based IoT network [3, 4].

Finding energy-efficient data transmission channels, extending network lifetime, enhancing routing's robustness and dependability, facilitating data fusion and forwarding, and other objectives are the primary design goals of routing algorithms in WSN. Therefore, it is important to concern machine learning techniques, metaheuristic algorithms to limit the energy used by nodes in order to create successful routing decisions and improve network performance [5, 6].

Hierarchical cluster-based approaches were successful in addressing WSN energy consumption in terms of scalability and energy balancing. This routing is implemented by partitioning the network into many clusters [8–11]. Each clusters, CH collects packets from nodes and Cluster Member (CM), compiles it, and sends to the BS. However, in hierarchical cluster networks, security has received less attention. To protect against intruders, data security must be ensured at multiple levels. When nodes are placed in an unattended environment, they are susceptible to both internal and external attacks.

Therefore, in order to safeguard the data transmission process, current routing protocols in WSN must incorporate energy security measures. These systems intricate calculations are linked to their architecture, which results in significant memory and energy usage. This study, a cluster-tree-based trusted routing technique with the improved coati optimization algorithm (ICOA) known as CTTRIC is introduced for WSN. A distributed time-variant trust (TVT) model is incorporated into this routing scheme to examine sensor node behavior in relation to three trust criteria. The trust value of nodes in the WSN architecture is obtained using the decentralized time-variant trust model. An ICOA-based trusted routing tree (ICOTRT) is presented to create robust and secure communication channels between sensor nodes and the BS. It gathers data concerning each CH node, such as the trust level, remaining energy, and distance among CHs.

2. Literature Review

Qin et al. [12] proposed a Trust Sensing-based Secure Routing Mechanism (TSSRM) for WSN. This strategy uses a secure path selection technique that takes QoS criteria and trust value into account. TSSRM was implemented to stability of energy efficiency during the data transmission process and prevent routing attacks. TSSRM determine node trust and creates a secure routing process. This technique examines node behavior in terms of mobility and energy during the trust evaluation phase. This method then determines various routes between sensor nodes. TSSRM uses the trust of the found paths in the secure route selection procedure to decide the usually fashionable routes. Lastly, TSSRM applies the Semiring theory to combine the trust value and QoS.

Kavidha and Ananthakumaran [13] suggested Enhanced Fuzzy C Means and Adaptive Time Division Multiple Access Scheduling (ECATS) to improve communication within the network for the mobile sink to receive data packets on time. Neural elliptic galois (NEG) cryptography is presented for effective data protection. Location privacy (Threshold fault node detection) is introduced for enhancing the security of WSN model. The data aggregate among

several network nodes is managed via CH selection based on energy. TDMA-based Ant Lion Optimization (ACO) scheduling hybridization is introduced to pick the best CH while improving energy efficiency. Lastly, optimal WSN performance parameters such as PDR, throughput, minimal energy consumption, communication overhead, and E2ED can be used for ECATS. As a result, it is able to minimize energy usage and improve network reliability. Results are compared with a current routing protocols using MATrix LABoratory (MATLAB) simulation.

Ant Colony Optimization (ACO) based Quality of Service aware energy balancing secure routing (QEBSR) algorithm for WSN was proposed by Rathee et al. [14]. Improved heuristics are proposed to calculate the end-to-end transmission delay and the trust factor of the nodes on the routing path. Distributed energy-balanced routing and energy-efficient routing with node-compromise resistance are compared with the proposed approach. QEBSR algorithm is works better when compared to other algorithms.

Thangaramya et al. [15] introduced the Neuro-Fuzzy Rule Based Cluster Formation and Routing Protocol (FBCFP) for effective routing in IoT-based WSN. FBCFP is introduced in the network learning process based on the energy value, the distance between CHs and BS, the change in the cluster area and the degree of CH. FBCFP, a convolutional neural network (CNN) is used to learn the network environment and a fuzzy system to modify its initial weights. Proposed routing algorithm has improved network performance by the following metrics: energy consumption, PDR, latency, and network lifetime.

A trust-aware optimized compressed sensing-based data aggregation and routing algorithm for clustered WSN was proposed by Gilbert et al. [16]. Compressed sensing enables data aggregation from sensor nodes with reduced overhead. Several meta-heuristic algorithms, such as the Artificial Bee Colony (ABC), Ant Colony Optimization (ACO), Differential Evolution (DE), Firefly Algorithm (FA), and Particle Swarm Optimization (PSO) are used to validate the trust-aware routing process in WSN. Transmission distance, hop count, quantity of messages sent, and trustworthy path are all traded off. An objective function is presented that maximizes the path's trust while minimizing the distance travelled, hop count, and message count.

A novel protocol called Trust Based Secure and Energy Efficient Routing (TBSEER) was introduced by Hu et al. [17]. The entire trust value, which is impervious to hello flood, sinkhole, black hole, and selective forwarding attacks. It is determined by TBSEER using adaptive direct trust value, indirect trust value, and energy trust value. Furthermore, the adaptive punishment mechanism and volatilization factor are used to promptly identify the attack nodes. Only the direct trust value needs to be computed by the nodes; the indirect trust value is decided by the sink, greatly lowering the energy usage brought on by repeated calculations. Finally, comprehensive trust value is used to recognize the safest multi-hop paths and the CH actively prevents wormhole attacks. TBSEER decreases energy consumption, and highest malicious nodes identification.

Joshi and Raghuvanshi [18] presented a novel approach for determining the CH and the most effective path on IoT-WSN. Three objectives like energy, distance, and delay are taken into account by the multi-objective Rider Optimization Algorithm (ROA), which is used to choose the CH. Multi-objective sailfish optimization method (SFO) is introduced for routing by

choosing effective and ideal routes. Proposed model performs better with respect to execution time, energy reduction, network delay, throughput, PDR, no. of alive nodes in the network, and no. of dead nodes.

A clustering approach with a trust model with the purpose of uses energy and data-trust towards recognize an untrusted node was proposed by Hriez et al. [19]. Additionally, the suggested clustering methodology extends the network's lifespan by utilizing the positive aspects of stochastic fractal search optimization. Energy trust and data trust are the two trust variables taken into account by this trust model. Furthermore, the clustering procedure is carried out by this approach using stochastic fractal search optimization. In order to maximize network lifetime and enhance network security, CHs are selected from the trustworthy nodes using the clustering approach and fitness function. In order to choose the cluster-heads from among the trusted nodes, a new fitness function is finally presented. According to evaluation results, this approach is superior to current protocols.

A Trust-Aware Routing Mechanism (TARM) was introduced by Saleh et al. [20]. It gathers information from ideal nodes by utilizing an edge node with a mobility function. The edge node divides the difficult and abnormal nodes from the regular nodes using a trust evaluation technique. In TARM, the clusters on deployed sensor nodes are formed using a modified version of Grey Wolf Optimization (GWO). After the clusters are created, the trust levels for each cluster are determined, and the edge node begins gathering data only from reliable nodes through the appropriate CH. The best routing route between the reliable nodes and the mobile edge node is carried out via the ABC algorithm. When compared to alternative approaches, simulations demonstrate that the suggested strategy ensures good security.

Hosseinzadeh et al. [21] presented a cluster-tree-based trustworthy routing technique named CTTRG, which makes use of the Grasshopper Optimization Algorithm (GOA) for WSN. TVT model is incorporated into this routing architecture to examine sensor node behavior with three trust criteria. CTTRG, a GOA-based trustworthy routing tree (GTRT) is introduced to create safe and reliable communication channels between sensor nodes and BS. As far as the speed at which malicious nodes, PLR, and E2ED are detected, CTTRG performs well.

3. Proposed Methodology

CTTRIC, a clustering tree trusted routing algorithm for WSN that uses the improved coati optimization algorithm (ICOA). The suggested architecture aims to counter several routing attacks, particularly the FA, WH, SH, BH, and GH against energy efficiency. Each recommendation weight is established based on the recommender nodes degree of trust as well as the discrepancy among the estimated direct trust and the recommended trust. ICOA is introduced to give reliable channels of communication among the BS and the CHs. The multi-objective fitness function is calculated for CH selection and routing. Lastly, ICOTRT message that contains the CHs position in the routing tree, BS updates the status of CHs in ICOTRT.

3.1 SYSTEM MODEL

Aim of this communication is to check data packets from source to destination and remove all the packets. The threat model, energy consumption mechanism, and network parameters are major steps of proposed model.

3.1.1 Network settings

In CTTRIC, sensor nodes have been randomly allocated to WSN model and it has been illustrated in Figure 1. Furthermore, the nodes are divided into several clusters, and CHs are chosen randomly from WSN model. Let us consider the parameters used in CTTRIC protocol,

- The BS and network nodes are static.
- BS uses a limitless supply of energy.
- Because they share a common energy source, network nodes are homogeneous.
- Positioning devices and radio communication modules are among the equipment mounted on sensor nodes.
- Every SN_ihas a unique identifier.

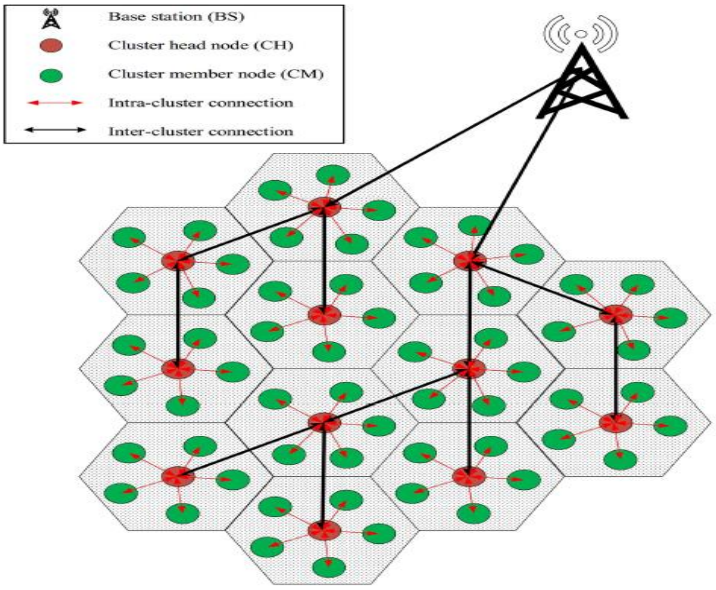

FIGURE 1. NETWORK MODEL IN CTTRIC

3.1.2 Energy consumption mechanism

Free space and multi-path are the two modes in which the energy model is described in CTTRG. To transfer k bits to SN_j, the energy used by $SN_i$is obtained from equation (1),

$$E_{TX}(k,d) = \begin{cases} E_{elec} \times k + E_{fs} \times k + d^2, d < d_0 \\ E_{elec} \times k + E_{mp} \times k + d^4, d \geq d_0 \end{cases} \quad (1)$$

Furthermore, equation (2) is utilized to determine how much energy SN_j needs to receive this packet.

$$E_{RX}(k,d) = E_{elec} \times k \quad (2)$$

$d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$ is denoted as the distance among SN_i and SN_j by spatial coordinates (x_i, y_i) and (x_j, y_j) correspondingly. E_{elec} is denoted as the electrical energy. Furthermore, E_{fs} and E_{mp} is denoted as the energy required by free space and the multi-path. $d_0 = \sqrt{\frac{E_{fs}}{E_{mp}}}$ is denoted as the transfer distance threshold.

3.1.3 Attack model

In WSN, security threats resulting from wireless connectivity, dynamic topology, deployment in dangerous settings, and the absence of a central controller must be avoided or minimized. An essential element of cyber security is trust [22]. Since security risks can compromise privacy, alter or remove data, and serve as a foundation for additional cybersecurity attacks, a security system actually aims to dynamically recognize trustworthy nodes and lower security risks.

3.2 CTTRIC METHOD

This section, CTTRIC routing algorithm is introduced for WSN. The ICOA-based trusted routing tree (ICOTRT) and the TVT model are the two primary mechanisms in this approach. Figure 2 shows a diagram of the proposed approach.

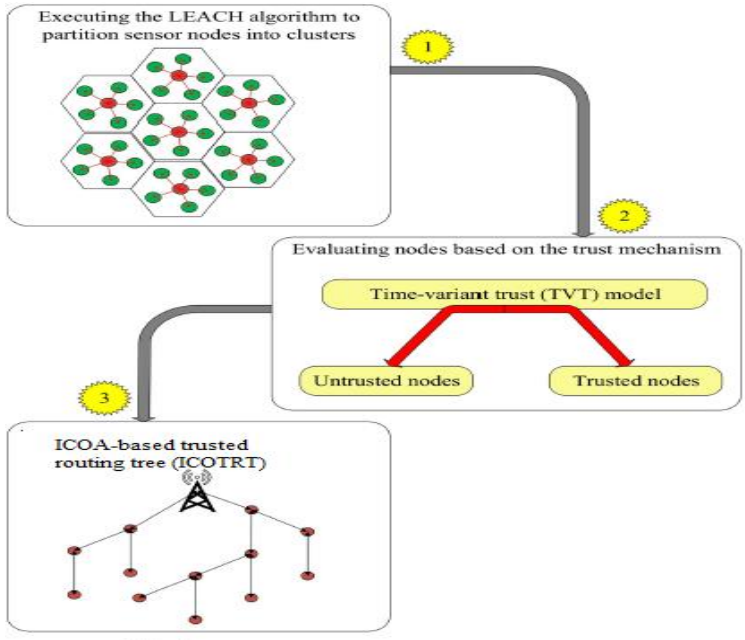

FIGURE 2. DIAGRAM OF CTTRIC MODEL

3.2.1 Time-Variant Trust (TVT) model

The trust value remains constant throughout each period, even though the nodes trust is periodically renewed in traditional trust architecture. Time-variant weight coefficient is taken into account for the trust parameters. Time-Variant Direct Trust (TVDT), Recommended Trust

(RT), and time-variant final trust (TVFT) are the three parts of TVT.

TVDT component: In CTTRG, the TVDT part includes an initial value and a dynamic coefficient. It is generated based on the trust parameters like the BH, SH, and GH probability (pr_{SBG}), the WH probability (pr_{WH}), and the FA probability (pr_{FA}).

RT component: In this section, RT is denoted as with the purpose of SN_i not simply depends on its interactions is used to compute the trust of SN_j, but also makes advantage of the trust values that the recommended nodes (RN_k). In TVT, $RN_k$is a common node between SN_i and SN_j, and $R = \{RN_1, RN_2, \ldots, RN_k, \ldots, RN_{|R|}\}$ is a set with the purpose of includes all RN_k nodes. In TVT, SN_iconsiders a weight coefficient $CT_{ik}(t-1)$ for evaluating the trust recommended by RN_k.

TVFT component: Currently, known with the purpose of TVDT is a time-variant function.

3.2.2 ICOA-based trusted routing tree (ICOTRT)

In CTTRIC, an ICOTRT tree is based on the network to start consistent association among CHs and BS. ICOA algorithm is used by BS to build an ICOTRT tree. Furthermore, it puts all CHs $TR = \{CH_1, CH_2, \ldots, CH_q, \ldots, CH_Q\}$ (Q is the no. of CHs in the WSN). Each Coati establishes the routing path among each CH and BS. ICOA is to simulate coati behavior in order to pick CH in WSN. It is used to repeat the natural behaviors of two coatis like exploration (hunting and attacking iguanas) and exploration (avoiding predators) [23]. During the initialization phase, the expression in equation (3) is used to randomly create the coatis' location in search space.

$$X_i: x_{i,j} = b_j^L + rand(0,1).\left(b_j^U - b_j^L\right), i = 1, \ldots., N, j = 1, \ldots, m \quad (3)$$

Equation (3), X_i is denoted as the location of the i^{th} coati, $x_{i,j}$ is denoted as the value of the j^{th} CH. b_j^L and b_j^U is denoted as the lower and lower ranges of the nodes. N is denoted as the coatis' number, m is the denoted as the optimal selection of CH based on the variables.

Phase 1: Exploration Phase

Coati's position update approach throughout the exploration phase primarily mimics the way Coati hunts and attacks iguanas. Coati's behavior can be broken down into two phases, such as hunting and iguana assault. To finish hunting and fighting the iguana, Coati's activity is split into two phases. (1) Fright. A group of Coatis scale a tree to get close to and frighten an iguana. (2) Under the tree, a number of additional Coatis wait for the terrified iguana to fall to the ground. Once it does, they finish the attack and pursue it. COA method assumes that the iguana is the population's best member because of its location. Consequently, position can be expressed mathematically as follows,

$$X_i^{P1}: x_{i,j}^{P1} = x_{i,j} + rand(0,1).\left(G_j - Ix_{i,j}\right), i = 1,2, \ldots., \left[\frac{N}{2}\right], j = 1, \ldots, m \quad (4)$$

where $X_{i,j}^{P1}$ is denoted as the new position of the i^{th} Coati in the j^{th} CH, $r \in [0,1]$ is denoted as the random number, $G_j$is the iguana's location in the j^{th} CH, $I \in \{1,2\}$ is denoted as the random number from the set, N is denoted as the no. of Coati. The iguana is dropped to the ground and then randomly positioned inside the search area. Two formulas are used to model this step,

$$G^g: G_j^g = b_j^L + \text{rand}(0,1)(b_j^U - b_j^L) \tag{5}$$

where G_j^g is the location of the iguana on the ground in the j^{th} CH.

$$X_i^{P1}: x_{i,j}^{P1} = \begin{cases} x_{i,j} + \text{rand}(0,1).\left(G_j^g - Ix_{i,j}\right), F_{G,j}^g \le F_{i,j}, i = [N/2]+1, \ldots, N\ j = 1, \ldots, m \\ x_{i,j} + \text{rand}(0,1).\left(x_{i,j} - G_j^g\right), \text{else} \end{cases} \tag{6}$$

where $F_{G,j}^g$ is denoted as the fitness function of the j^{th} iguana subsequent to it falls to the G, $F_{i,j}$ is the fitness function of the i^{th} Coati in j^{th} CH. Else, kept as same and it is described as follows,

$$X_i = \begin{cases} X_i^{P1}, F_i^{P1} \le F_i \\ X_i, \text{other} \end{cases} \tag{7}$$

where F_1^{P1} is the fitness function of the i^{th} Coati at the new CH location, F_i is the fitness function of the i^{th} Coati at the recent CH position.

Phase 2: Exploitation phase

Coati's location-updating approach during the exploitation phase is to replicate its natural behavior when it comes to encountering and escaping from predators. When a predator attacks Coati during the exploitation phase, Coati defends its place. By using this tactic, Coati was able to secure a position near its present location. This illustrates how COA algorithms are exploited in local search. A random site is created close to each Coati's location using the following equation (8) in order to replicate this behavior,

$$b_{j,L}^{loc} = \frac{b_j^L}{t}, b_{j,U}^{loc} = \frac{b_j^U}{t}, t = 1, \ldots, T \tag{8}$$

where $b_{j,L}^{loc} \& b_{j,U}^{loc}$ is denoted as the local lower & upper bound of the j^{th} CH, t is the total number of iterations, T is the greatest number of iterations. It is described by equation (9),

$$X_i^{P2} = x_{i,j} + (1-2r)\left(b_{j,L}^{loc} + r\left(b_{j,U}^{loc} - b_{j,L}^{loc}\right)\right) \tag{9}$$

where $X_{i,j}^{P2}$ is the new CH location of the i^{th} Coati in the j^{th} CH.

$$X_i = \begin{cases} X_i^{P2}, F_i^{P2} \le F_i \\ X_i, \text{else} \end{cases} \tag{10}$$

Coati on the periphery of the group will promptly relocate to the safe region to improve their position. Coatis, the central Coati will haphazardly roam about the group. It is described as follows,

$$x_{i,j}^{P2} = \begin{cases} G_j + \beta.\left|x_{i,j}^{P2} - G_j\right|, & \text{if } f_i > f_g \\ x_{i,j}^{P2} + K\left(\dfrac{\left|x_{i,j}^{t} - G_j\right|}{(f_i - f_W) + \varepsilon}\right), & \text{if } f_i = f_g \end{cases} \tag{11}$$

where G is denoted as the present global best CH location. ε is a constant, β is denoted as the

step control parameter with a normal distribution as zero mean 0 and one standard variance. The step size and Coati's travel direction are indicated by $K \in [-1,1]$. f_i is the existing Coati individual fitness value. The best and worst global fitness levels are denoted by $f_g$and f_w respectively. To prevent zeros in the denominator, ε is a constant. A multi-objective fitness function is computed when evaluating ICOTRT trees in construction. In each iteration, Coati's locations will then be modified in accordance with this fitness function. Changing the CH locations in the routing tree and creating the best ICOTRT tree are the goals of this upgrade procedure. ICOTRT tree is constructed according to three criteria: the trust level of the CH, the distance with the CH and its parent node, and the CH remaining energy. In this context, equation (12) evaluates ICOTRT trees based on the fitness function,

$$F_{fitness} = \beta f_1 + (1-\beta) f_2 \tag{12}$$

where $\beta \in [0,1]$ is a fixed number which finds the result of $f_1$and $f_2$on $F_{fitness}$. From this BS finds the best response ($\widehat{T_d}$) in the population. The BS searches for a tree in the ICOTRT algorithm where each CH has a minimal distance to its parent. Therefore, $f_1$is determined by equation (13),

$$f_1 = \frac{1}{\sum_{i=1}^{Q} d(CH_i, Parent_i)} \tag{13}$$

where $d(CH_i, Parent_i) = \sqrt{(x_i - x_p)^2 + (y_i - y_p)^2}$. Also, (x_i, y_i) and (x_p, y_p) is denoted as the coordinates of CH_i and its parent ($Parent_i$). However, as CH's energy decreases after performing multiple data transmission operations, and it has important impact on network performance. Consequently, f_2 is used to find the direct of CHs in ICOTRT depending on energy and trust by equation (14),

$$f_2 = \sum_{D=1}^{[\log Q]} \frac{1}{D} \sum_{x=1}^{2^D} \left(\partial \left(\frac{E_{res,t}^{x} - Emin}{E_{ini} - Emin} \right) + (1-\partial) \left(\frac{TVFT_x(t) - \min\limits_{CH_k \in TR} \{TVFT_k(t)\}}{\max\limits_{CH_k \in TR} \{TVFT_k(t)\} - \min\limits_{CH_k \in TR} \{TVFT_k(t)\}} \right) \right) \tag{14}$$

where the residual energy of CH_x is represented by $E_{res,t}^{x}$, $Emin = 15\% E_{ini}$.The primary energy of the network nodes is represented by E_{ini}, which is also the lowest energy threshold. In addition, D represents the tree depth, $\partial \in [0,1]$ is a fixed number, and $TVFT_x(t)$ is the trust of CH_x. This step establishes the ICOTRT algorithm's halting condition, allowing the process to proceed through 300 iterations and discover the optimal GTRT at the last one. Lastly, by sending an ICOTRT message that contains the CHs' placement in the routing tree, BS updates the status of CHs in ICOTRT.

4 Simulation and Results

Network Simulator (NS2) is used to evaluate performance and the experimental outcomes of CTTRIC is compared with other methods like TBSEER [17], TSSRM [12], and CTTRG [21]. Totally there are 100 number of sensor nodes with simulation area of 100x100m^2. Every node starts by a trust level of 0.5 and it maximum energy of 1J. Moreover, the trust threshold is 0.35. Table 1 describes the simulation parameter of WSN model.

TABLE 1. SIMULATION SETTINGS OF WSN MODEL

SCALE	VALUE
Area	100×100 m^2
Nodes	100
Maximum energy	1 J
Initial trust of nodes	0.5 J
Trust Threshold	0.35
Control packet size	400 bits
Data Packet Size	4000 bits

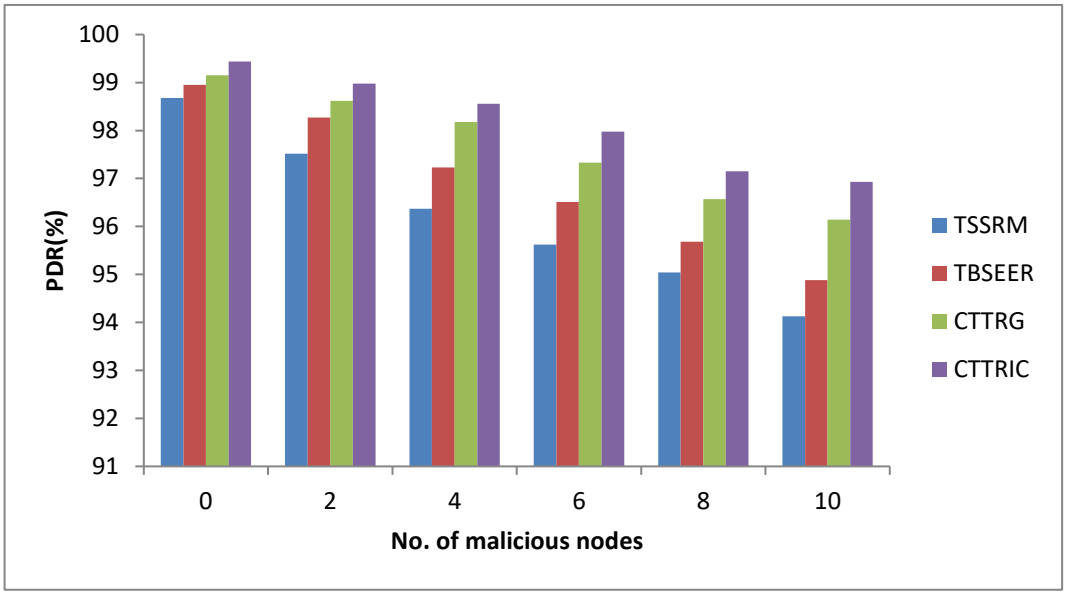

FIGURE 3. PDR COMPARISON AMONG DIFFERENT SCHEMES

PDR is denoted as the ratio of the no. of packets that successfully arrive at the BS to each and every one packets sent to the BS. Figure 3 CTTRIC has the highest PLR of 96.93%; other methods have 94.13%, 94.88%, and 96.14% for TSSRM, TBSEER, and CTTRG among malicious nodes (10) respectively. This is because to CTTRIC robust security mechanism, which swiftly detects malicious nodes. Additionally, it will lessen the quantity of lost data packets and stop the impact of malicious nodes.

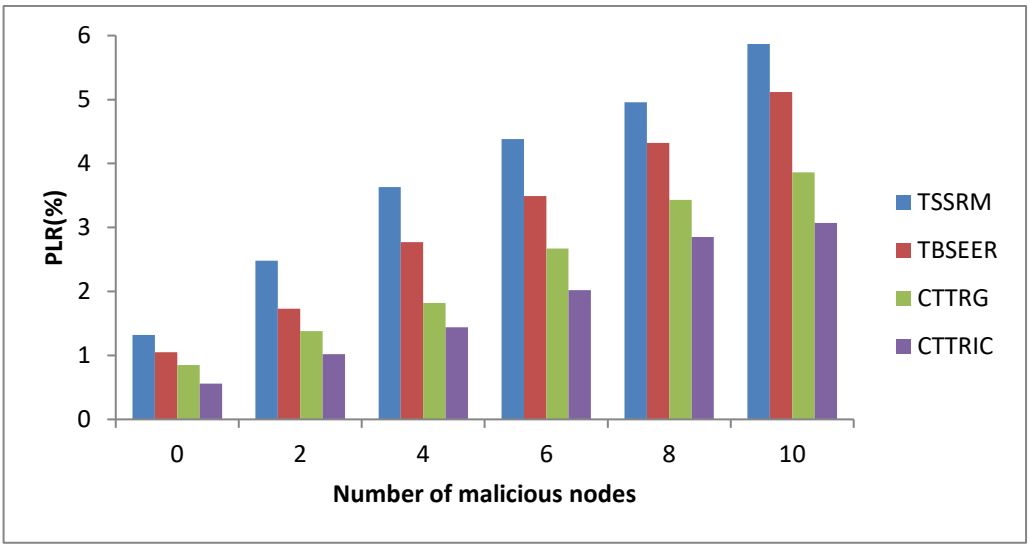

FIGURE 4. PLR COMPARISON AMONG DIFFERENT SCHEMES

PLR is denoted as the ratio of the no. of packets that don't arrive at the BS to all packets sent to the BS. Figure 4, CTTRIC has the lowest PLR of 2.07%, other methods have the highest PLR of 5.87%, 5.12%, and 3.86% for TSSRM, TBSEER, and CTTRG among malicious nodes (10) respectively. When creating a GTRT tree, three parameters like the energy of the network nodes, their trust level, and the distance among each CH and its parent. As a result, a secure and robust tree is formed between CHs.

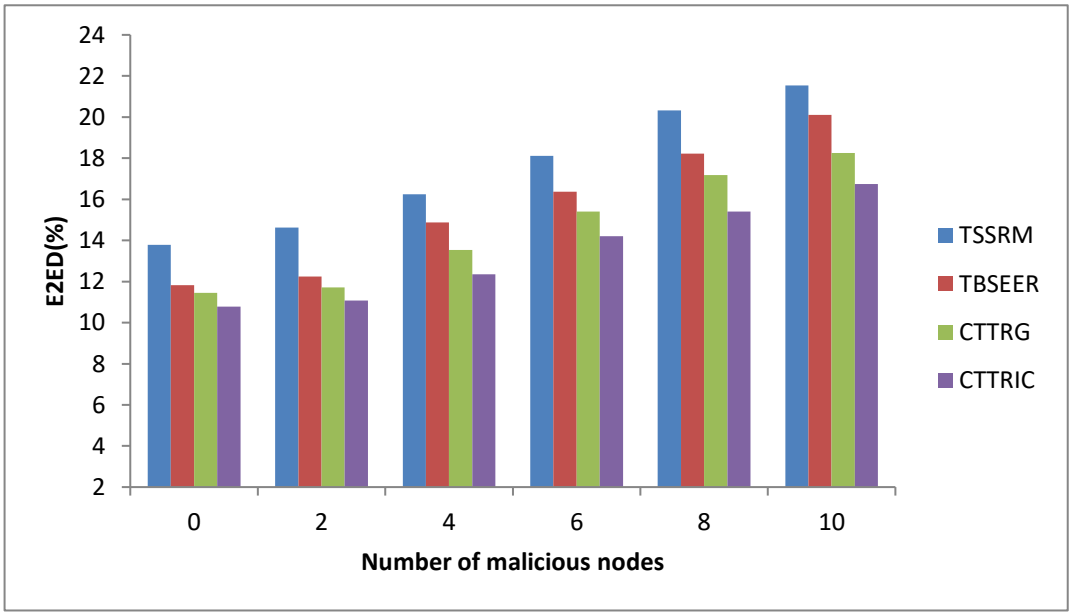

FIGURE 5. E2ED COMPARISON AMONG DIFFERENT SCHEMES

The average time needed to transmit a packet from the source to the destination known as

E2ED. Figure 5 shows the E2ED comparison of CTTRIC is lesser of 16.74 ms, other methods has highest E2ED of 21.54 ms, 20.11 ms, and 18.25 ms to TSSRM, TBSEER, and CTTRG among malicious nodes (10) respectively. Data packets are transferred through the optimized tree in CTTRIC, which reduces routing process latency. Since E2ED is directly correlated by number of hostile nodes in the network, all routing techniques encounter a delay in data transfer when there are a lot of these nodes. Since a huge number of malicious nodes on the network are difficult for security systems to detect.

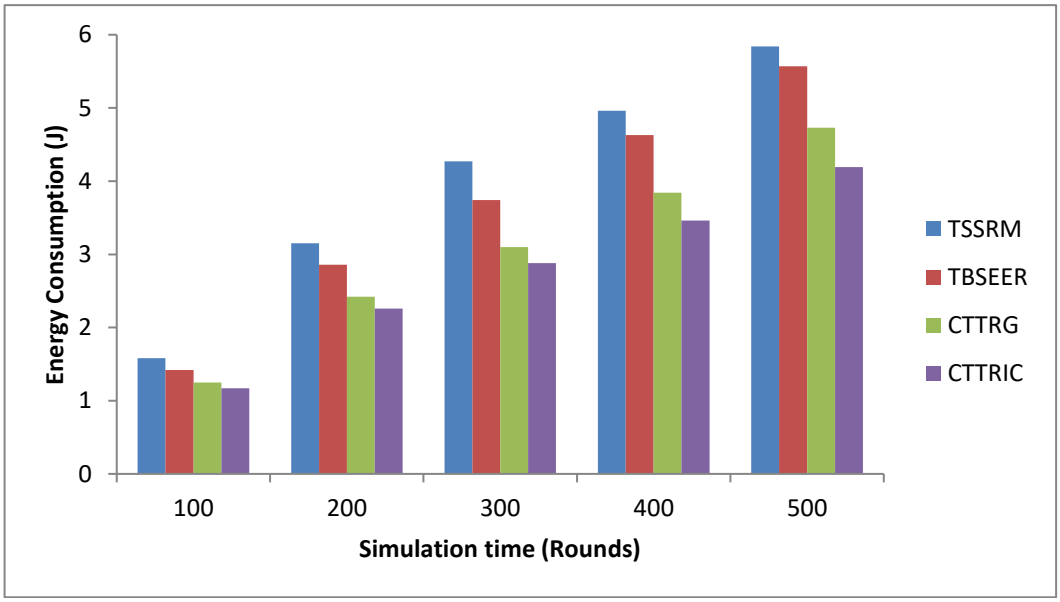

FIGURE 6. ENERGY CONSUMPTION COMPARISON AMONG DIFFERENT SCHEMES

Figure 5 shows the E2ED comparison of CTTRIC is lowest of 4.19 J, other methods has highest energy consumption of 5.84 J, 5.57 J, and 4.73 J for TSSRM, TBSEER, and CTTRG among simulation time (500 rounds) respectively. It shows that the proposed system has 28.25%, 24.77% and 11.41% lowest energy usage when compared to TSSRM, TBSEER, and CTTRG methods respectively. The tree-cluster architecture used in the proposed system significantly improves energy consumption efficiency.

5 Conclusion and Future Work

This paper, clustering tree trusted routing algorithm with improved coati optimization algorithm (ICOA) namely CTTRIC is introduced for WSN. The ICOTRT and the TVT model are the two primary mechanisms in this approach. Decentralized time-variant trust model is suggested to determine the trust of nodes in CTTRIC. TVDT, RT, and TVFT are the three parts of TVT. To create dependable connections between CH and BS, CTTRIC creates an ICOTRT tree on the network. ICOA is a metaheuristic algorithm that imitates coati behavior for the best CH selection in WSN. The primary function of the COA is to replicate the normal behaviors of two coatis, including as exploration and two activities. Modeling the coatis'

approach to attacking iguanas serves as the basis for the initial stage of updating the coatis population in the CH selection process. The primary function of Coati's location-updating approach during the exploitation phase is to replicate its natural behavior when it comes to encountering and escaping from predators. A multi-objective approach is considered in the ICOTRT tree construction algorithm, which builds the ICOTRT tree according to three criteria: the trust level of the CH, the distance among the CH and its parent node, and the CH remaining energy. CTTRIC performance is evaluated against TSSRM, TBSEER, and CTTRG with PDR, PLR, E2ED, and energy efficiency. To find the best tree in the WSN model, the ICOTRT tree has also been built utilizing several nature-based techniques.

References

1. Zhang D., L. Quan, C. Lin, et al., Multi-layer based multi-path routing algorithm for maximizing spectrum availability, Wirel. Netw. (2018) 1–13.
2. Al-Ariki H.D., M.N. Swamy, A survey and analysis of multipath routing protocols in wireless multimedia sensor networks, Wirel. Netw. 23 (6) (2017) 1823–1835.
3. Jothimuneeswari S., S. Ganapathy, A Kannan, Intelligent data gathering and energy efficient routing algorithm for mobile wireless sensor networks, Asian J. Inf. Technol. 15 (2016) 921–927.
4. Selvi, M., Velvizhy, P., Ganapathy, S., Nehemiah, H.K. and Kannan, A., 2019. A rule based delay constrained energy efficient routing technique for wireless sensor networks. Cluster Computing, 22, pp.10839-10848.
5. Rahmani A.M., Ali S., Malik M.H., Yousefpoor E., Yousefpoor M.S., Mousavi A., et al. 2022. An energyaware and Q-learning-based area coverage for oil pipeline monitoring systems using sensors and Internet of Things. Scientific Reports, 12(1), pp.1-17.
6. Gulati K., Boddu R.S.K., Kapila D., Bangare S.L., Chandnani N. and Saravanan G., 2022. A review paper on wireless sensor network techniques in Internet of Things (IoT). Materials Today: Proceedings, 51, pp.161–165.
7. Alawad, F. and Kraemer, F.A., 2022. Value of information in wireless sensor network applications and the IoT: A review. IEEE Sensors Journal, pp.1-18.
8. Selvakumar K., L. Sairamesh, A. Kannan, ‘‘An intelligent energy aware secured algorithm for routing in wireless sensor networks,’’Wireless Pers, Commun. Now. 96 (3) (Oct. 2017) 47814798. [11] Z. Hong, R. Wang, X. Li, A clustering-tree topology control based on the energy forecast for heterogeneous wireless sensor networks, IEEE/CAA Journal of Automatica Sinica 3 (1) (2016) 68–77.
9. Aliady W.A., S.A. Al-Ahmadi, ‘‘Energy preserving secure measure againstwormhole attack in wireless sensor networks,’’, IEEE Access 7 (2019) 84132–84141.
10. Selvi M., K. Thangaramya, S. Ganapathy, K. Kulothungan, H.K. Nehemiah, A. Kannan, ‘‘An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks,’’ Wireless Pers, Commun. Now. 105 (4) (Feb. 2019) 1475–1490.
11. Mathapati M., T.S. Kumaran, A. Muruganandham, M. Mathivanan, ‘‘Secure Routing Scheme with Multi-Dimensional Trust Evaluation for Wireless Sensor Network, J. Ambient Intell. Humanized Comput., Jun. 2020, https://doi.org/ 10.1007/s12652-020-02169-7.
12. Qin D., Yang S., Jia S., Zhang Y., Ma J. and Ding Q., 2017. Research on trust sensing based secure routing mechanism for wireless sensor network. IEEE Access, 5, pp.9599–9609.
13. Kavidha V. and Ananthakumaran S., 2019. Novel energy-efficient secure routing protocol for wireless sensor networks with Mobile sink. Peer-to-Peer Networking and Applications, 12, pp.881–892.

14. Rathee M., Kumar S., Gandomi A.H., Dilip K., Balusamy B. and Patan R., 2019. Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks. IEEE Transactions on Engineering Management, 68(1), pp.170–182.
15. Thangaramya K., Kulothungan K., Logambigai R., Selvi M., Ganapathy S. and Kannan A., 2019. Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT. Computer Networks, 151, pp.211–223.
16. Gilbert E.P.K., Baskaran K., Rajsingh E.B., Lydia M. and Selvakumar A.I. (2019) 'Trust aware nature inspired optimized routing in clustered wireless sensor networks', Int. J. Bio-Inspired Computation, Vol. 14, No. 2, pp.103–113.
17. Hu H., Han Y., Yao M. and Song X., 2021. Trust based secure and energy efficient routing protocol for wireless sensor networks. IEEE Access, 10, pp.10585–10596.
18. Joshi P. and Raghuvanshi A.S., 2021. A Multi-Objective Metaheuristic Approach Based Adaptive Clustering and Path Selection in IoT Enabled Wireless Sensor Networks. International Journal of Computer Networks and Applications, 8(5), pp.566–584.
19. Hriez S., Almajali S., Elgala H., Ayyash M. and Salameh H.B., 2021. A novel trust-aware and energyaware clustering method that uses stochastic fractal search in IoT-enabled wireless sensor networks. IEEE Systems Journal, 16(2), pp.2693–2704.
20. Saleh, A., Joshi, P., Rathore, R.S. and Sengar, S.S., 2022. Trust-aware routing mechanism through an edge node for IoT-enabled sensor networks. Sensors, 22(20), pp.1-22.
21. Hosseinzadeh, M., Ahmed, O.H., Lansky, J., Mildeova, S., Yousefpoor, M.S., Yousefpoor, E., Yoo, J., Tightiz, L. and Rahmani, A.M., 2023. A cluster-tree-based trusted routing algorithm using Grasshopper Optimization Algorithm (GOA) in Wireless Sensor Networks (WSNs). Plos one, 18(9), pp.1-31.
22. Goyal, S.B., Bedi, P., Rajawat, A.S. and Shrivastava, D.P., 2022. Secure Authentication in Wireless Sensor Networks Using Blockchain Technology. In AI-Enabled Agile Internet of Things for Sustainable FinTech Ecosystems (pp. 93–105). IGI Global.
23. Qi, Z., Yingjie, D., Shan, Y., Xu, L., Dongcheng, H. and Guoqi, X., 2024. An improved Coati Optimization Algorithm with multiple strategies for engineering design optimization problems. Scientific Reports, 14(1), pp.1-44.