International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Multi Objective-Trust Aware Coati Optimization Algorithm for Secure Cluster Head and Route Discovery in IoT-WSN

Shruthi Bennur Mallikarjuna[1,2]* **Channakrishna Raju[2]**

[1]*Department of Computer Science and Engineering,*
SJCE, JSS Science and Technological University, Mysuru, India
[2]*Department of Computer Science and Engineering,*
Sri Siddhartha Institute of Technology, SSAHE, Tumakuru, India
* Corresponding author's Email: shrubm@gmail.com

Abstract: Internet of Things (IoT) is a network of physical objects generally utilized for interconnecting and communicating with other devices via the Internet. Here, Wireless Sensor Network (WSN) is used as a medium to connect the IoT physics and information network. Security is considered as an important aspect in IoT-WSN due to the open deployment of sensors. In this research, a Multi Objective-Trust Aware Coati Optimization Algorithm (MO-TACOA) is proposed to perform secure and reliable data communication over the IoT-WSN under malicious attacks. Initially, the Secure Cluster Head (SCH) from the normal sensors are chosen by optimizing the MO-TACOA with trust, residual energy, interspace between sensors & SCH, interspace between SCH & BS, and node degree. Next, the secure path is identified by optimizing the MO-TACOA with residual energy and interspace between SCH & BS. Therefore, the proposed MO-TACOA improves the security against malicious attacks while also improving the data delivery. The MO-TACOA is evaluated using alive nodes, energy expenditure, lifecycle, throughput and Packet Loss Ratio (PLR). The existing methods namely, Taylor based Cat Salp Swarm Algorithm (Taylor C-SSA), Taylor-Spotted Hyena Optimization (TaylorSHO) and Beet swarm Induced Tunicate swarm Algorithm (BITA) are used for comparison. The MO-TACOA achieves the throughput of 16087 kbps which is higher than that of the TaylorSHO.

Keywords: Internet of things, Malicious attacks, Multi objective-trust aware coati optimization algorithm, Secure cluster head, Wireless sensor network.

1. Introduction

IoT is a 4th industrial revolution technology that connects a huge amount of people to internet via laptops, smartphones and other personal devices. Therefore, it simplifies data exchange among users through the utilization of objects or remaining items [1, 2]. IoT developed in modern wireless communications supports different types of physical devices with an internet protocol address for transferring and interacting with each other through the Internet [3, 4]. In the recent times, humans are live in a period where Internet devices are crucial in everyday lives, such as in environmental monitoring, real-time equipment monitoring, industrial safety production management and manufacturing supply chain management. The prediction states that for every person in 2050, there will be more than ten devices connected to the Internet [5]. IoT enhances various communication structures which are based on WSN for collecting data [6]. WSN contains many nodes which are positioned in the global environment to sense, compute, observe and transmit with the remaining networks. This WSN is used to observe the physical traits of the environment such as temperature, humidity, sound and so on [7].

WSN provides flexibility to the interlinked objects for sensing and controlling, alongside leading to the straight incorporation of computational model into the physical world. Next, the inter-link among the objects has the capacity for transferring data with least human interaction [8]. The integration of WSN with any object (Thing), internet and online application (i.e., mobile app, Cloud and so on) creates IoT [9]. WSN based IoT network has the benefit of appropriate deployment of network devices with better scalability at lesser costs [10]. The processing of information gathered from the sensors to ensure event monitoring is a key task of WSN. The data gathered by the sensors are transmitted to the Base Station (BS), also referred to as 'sink' in WSN [11, 12]. Smart devices have some restrictions by means of processing, computing, memory and energy resources. Additionally, one of critical issues of WSN is to establish reliability while preserving the data security in a susceptible environment against the malicious attacks [13-15].

The contributions of this research are enlisted as follows:

- MO-TACOA is used for selecting the SCHs from the sensors that avoids malicious attacks, and minimizes the energy expenditure of the nodes. The mitigation of malicious attacks leads to the avoidance of unwanted energy expenditure and packet loss over the IoT-WSN.
- Further, this MO-TACOA is used to discover a secure path in the network to ensure reliable data communication.

The remaining portions are sorted as follows: section 2 presents the related work. The proposed MO-TACOA is detailed in section 3 and outcomes are presented in section 4. The conclusion and future research directions are given in section 5.

2. Related work

The existing researches related to secure data transmission over the network are provided in this section.

Prakash [16] presented the Fractional Artificial Lion algorithm (FAL) for choosing CHs. The FAL was a hybridization of fractional calculus, lion optimization and the Artificial Bee Colony approaches, where it was optimized by using energy, distance, route life time and trust. Further, routing was done by using the energy and distance metrics. However, the developed FAL was required to consider the node degree for further reducing the node's energy.

Gali and Nidumolu [17] developed the Chaotic Bumble Bees Mating Optimization (CBBMO) approach to perform secure data communication with Trust Sensing Model (TSM). In CBBMO, the concept of chaotic is incorporated into conventional bumble bees mating optimization for enhancing the convergence. The TSM included direct and indirect trust values for identifying the malicious node. Further, the developed CBBMO used the TSM for discovering an optimum secure path to enable data communication. However, the developed CBBMO-TSM did not consider the clustering which affected the energy expenditure of nodes.

Vinitha [18] implemented the Taylor based Cat Salp Swarm Algorithm (Taylor C-SSA) to ensure an effective routing in the network. Initially, the Low Energy Adaptive Clustering Hierarchy (LEACH) was employed to choose the CH. Next, the developed Taylor C-SSA was used to initialize the secure and energy aware multi hop routing according to the energy, delay, intra and inter cluster distance, distance, lifetime and trust. But, dynamic changes in the CH discovery of LEACH affected the data transmission.

Kalburgi and Manimozhi [19] developed the Taylor Spotted Hyena Optimization (TaylorSHO) which was the hybridization of taylor series with spotted hyena optimization for choosing the CHs. The different factors such as delay, energy and distance were considered while selecting the CHs. On the other hand, the modified k-Vertex Disjoint Path Routing considered throughput and link reliability for routing data over the network. The inappropriate selection of fitness measures led to affect the data broadcasting over the network.

Kumar and Kumar [20] presented the Beet swarm Induced Tunicate swarm Algorithm (BITA) for selecting the CHs in IoT-WSN. The BITA approach was a combination of beetle swarm optimization and tunicate swarm algorithm, which optimized by using the security, communication cost, throughput, inter-cluster distance, residual energy and Packet Delivery Ratio (PDR). Additionally, the minimal distance function was used to ensure multi-hop communication. Yet, the node degree was required to be considered in the BITA for further enhancing the energy expenditure of nodes.

Kusuma, P.D. and Dinimaharawati, A [21] developed Extended Stochastic Coati Optimizer (ESCO) which was enhanced version of COA. The enhancement was done by using the sequential phase, references in the guided foraging, amount of searches and shifting the fixed split to the stochastic split. Kusuma, P.D. and Hasibuan, F.C [22] presented the metaphor-free metaheuristic approach namely Attack-Leave Optimizer (ALO). The ALO was concentrated over the guided search that failed to enhance the current solution. Kusuma, P.D. and Prasasti, A.L [23] developed walk-spread algorithm that was the combination of direction based search and neighbourhood search approaches. The developed optimizations were required to be considered with multiple objectives for obtaining an effective solution.

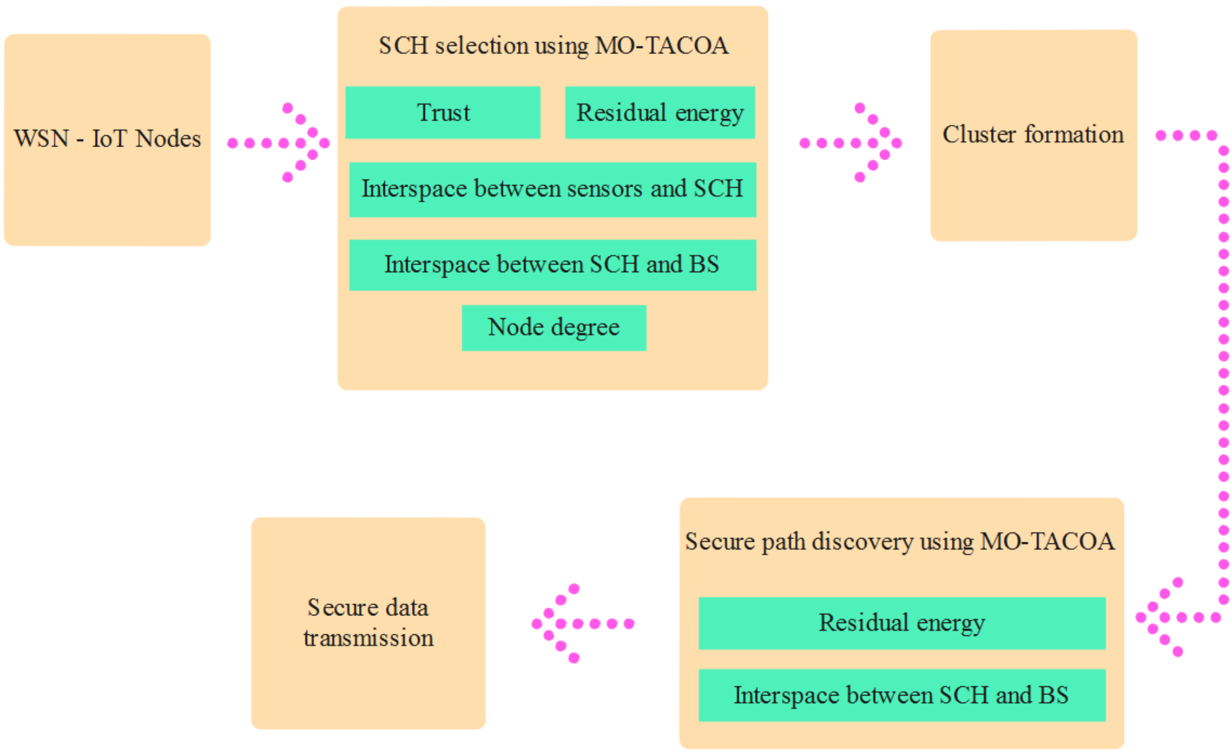

Figure. 1 Architecture of MO-TACOA based SCH and path discovery

3. Main title

The proposed MO-TACOA is used to perform secure data communication in the IoT-WSN. This MO-TACOA performs an effective SCH and secure path discovery. Initially, the malicious nodes are avoided while selecting the SCHs, which is used to gather the information from the Cluster Members (CMs). The collected information are transmitted to the BS based on the path discovered using MO-TACOA. Therefore, this MO-TACOA increases the robustness against the malicious attacks and enhances data delivery. The architecture of MO-TACOA based SCH and path discovery is shown in Fig. 1.

3.1 Network initialization

At first, the sensors are randomly deployed in the area of interest in IoT-WSN. From the normal sensors, the SCHs are identified using MO-TACOA, wherein the route via SCHs is also discovered using MO-TACOA.

3.2 SCH selection using MO-TACOA

In this stage, the SCHs from the network are chosen based on MO-TACOA. The typical COA approach is a population-based meta heuristic approach in which the coatis are considered to be population members. This COA is transformed into MO-TACOA by optimizing it with trust, residual energy, interspace between sensors & SCH, interspace between SCH & BS, and node degree. The SCH selection using MO-TACOA is detailed as follows:

3.2.1. Algorithm initialization process

Every coati's location in the search space discovers the values for the decision variables. Therefore, the coatis location in the MO-TACOA denotes a candidate solution to the issue. The solutions of coatis are initialized with the set of sensors that are required to chosen as SCHs. The node ID from 1 to S is randomly used to set the coatis population, where S defines the number of sensors. Let the ith coati is $X_i = \{x_{i,1}, x_{i,2}, \dots, x_{i,m}\}$, here m is the dimension i.e., number of SCHs.

The subsequent matrix X provided in Eq. (1) represents the coati-based populace.

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix}_{N\times m} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,j} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots & . & \vdots \\ x_{i,1} & \cdots & x_{i,j} & \cdots & x_{i,m} \\ \vdots & . & \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,j} & \cdots & x_{N,m} \end{bmatrix} \quad (1)$$

Where, position of coati i in the lookup field is denoted as X_i, evaluation of decision variable j is denoted as $x_{i,j}$, total amount of coatis is denoted as N, and amount of decision variables is denoted as m. The candidate solution's location in the decision variables leads to the estimation of various values for objective function of the issue. These parameters are shown in Eq. (2).

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_x \\ \vdots \\ F_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} F(X_1) \\ \vdots \\ F(X_x) \\ \vdots \\ F(X_N) \end{bmatrix}_{N\times 1} \quad (2)$$

Where, the obtained objective function is denoted as F and the objective function for coati i is denoted as F_i.

3.2.2. Exploration Phase (Predator Hunting and Attacking)

In this exploration, the coatis are separated into two different groups. The 1st group climbs tree for scaring the prey, while the 2nd group waits below the tree for the prey to fall out of fear. According to this movement pattern, the coati thoroughly forages the problem space. Here, the coatis prey is named as Iguana. The location of optimum individual of the population is considered to be the Iguana's location. The location of the 1st half of coatis climbing the tree is mathematically denoted as Eqs. (3) and (4) shows the randomized location of Iguana when it falls to the ground. Eq. (5) mathematically represents the movement of 2nd half of coatis which wait under the tree.

$$X_i^{P1}: x_{i,j}^{P1} = x_{i,j} + r.\left(\text{Iguana}_j - I.x_{i,j}\right) \quad \text{for} \quad i = 1,2,\dots,\left\lfloor\frac{N}{2}\right\rfloor \text{ and } j = 1,2,\dots,m \quad (3)$$

$$\text{Iguana}^G: \text{Iguana}_i^G = lb_j + r.(ub_j - lb_j) \quad (4)$$

$$X_i^{P1}: x_{i,j}^{P1} = \begin{cases} x_{i,j} + r.\left(\text{Iguana } a_j^G - I.x_{i,j}\right), & F_{\text{Iguana}} < F_i \\ x_{i,j} + r.\left(x_{i,j} - \text{Iguana}_j^G\right), & else \end{cases}$$
$$for\ i = \left\lfloor\frac{N}{2}\right\rfloor + 1, \left\lfloor\frac{N}{2}\right\rfloor + 2, \dots N\ and\ j = 1,2,\dots,m \quad (5)$$

Where, new location computed for coati i is represented as X_i^{P1}, $x_{i,j}^{P1}$ is the new coati's dimension j, I is the integer value that is either 0 or 2, and location of prey is denoted as Iguana, Iguana_j is its dimension j, prey's location in ground is denoted as Iguana^G and its jth dimension is denoted as Iguana_j^G, the fitness value of Iguana^G is denoted as F_{Iguana}, floor function is denoted as $\lfloor.\rfloor$, ub_j and lb_j are respectively the upper and lower values of the jth decision variable, while the random variable among [0,1] is denoted as r. The X_i^{P1} is defined as an optimum individual when the X_i^{P1} of coati i obtains an improved fitness than the X_i; otherwise, the old location is preserved based on Eq. (6).

$$X_i = \begin{cases} X_i^{P1}, & F_i^{P1} < F_i \\ X_i, & else \end{cases} \quad (6)$$

Where, the fitness of the new location is denoted as F_i^{P1}.

3.2.3. Exploitation phase (escaping from the predators)

The coati randomly moves near to its location based on Eqs. (7) and (8) when the coatis is attacked by the predator. The new location is considered as optimum when it improves the fitness according to Eq. (9).

$$lb_j^{local} = \frac{lb_j}{t},\ ub_j^{local} = \frac{ub_j}{t}, t = 1,2,,\dots,T \quad (7)$$

$$X_i^{P2}: x_{i,j}^{P2} = x_{i,j} + (1-2r).\left(lb_j^{local} + r.\left(ub_j^{local} - lb_j^{local}\right)\right)$$
$$i = 1,2,\dots,N,\ j = 1,2,\dots,m \quad (8)$$

$$X_i = \begin{cases} X_i^{P2}, & F_i^{P2} < F_i \\ X_i, & else \end{cases} \quad (9)$$

Where, $P2$ represents the location and fitness of coati in the 2nd phase, while the local upper and lower bounds of j th decision variable are denoted as ub_j^{local} and lb_j^{local}, respectively.

3.3 Objective function for selecting SCH

The developed MO-TACOA considers the following multiple objective values for choosing the SCH.

- **Trust (f_1)**

The MO-TACOA considers the trust as an important objective measure, wherein it incorporates three parameters namely, direct, indirect and recent trust values. Direct trust (DT) is the proportion among the received and transmitted data packets which is expressed in Eq. (10). Indirect trust (IDT) is

Received: February 4, 2024. Revised: April 16, 2024.

calculated according to the DT from the target node which is represented in Eq. (11). Next, the recent trust (RT) is measured using the DT and IDT according to the target node as represented numerically in Eq. (12). The overall trust value of the node is expressed in Eq. (13).

$$DT = \frac{Received\ packets_{a,b}(t)}{Sent\ packets_{a,b}(t)} \tag{10}$$

$$IDT = \frac{1}{NN}\sum_{u=1}^{NN} DT_{u,a} \tag{11}$$

$$RT = (\tau \times DT) + \big((1-\tau) \times IDT\big) \tag{12}$$

$$f_1 = DT + IDT + RT \tag{13}$$

Where, the nodes are denoted as a & b, time is denoted as t, the amount of neighboring nodes are denoted as NN and τ is constant which is equal to 0.3.

- **Residual energy (f_2)**

Network lifespan is mainly based on the energy expenditure, hence it is essential to reduce the energy usage. Moreover, the energy expenditure of SCH is important due to the accomplishment of different tasks such as data collection, aggregation and dissemination through the network. Eq. (14) numerically expresses the node's residual energy.

$$f_2 = \sum_{i=1}^{m} \frac{1}{E_{SCH_i}} \tag{14}$$

Where, the remaining energy of ith SCH is denoted as E_{SCH_i}.

- **Interspace between sensors & SCH (f_3), and Interspace between SCH & BS (f_4)**

The energy expenditure of the nodes mainly depends on the broadcasting distance over the network. The SCH with lesser distance is preferred for minimizing the energy expenditure. The interspace between the sensors & SCH, and the interspace between SCH & BS are expressed in Eqs. (15) and (16), correspondingly.

$$f_3 = \sum_{j=1}^{m}\left(\sum_{i=1}^{CM_j} dis(S_i, SCH_j)/CM_j\right) \tag{15}$$

$$f_4 = \sum_{i=1}^{m} dis(SCH_i, BS) \tag{16}$$

Where, CM_j represents the cluster members of the jth cluster, distance among sensor i and SCH j is denoted as $dis(S_i, SCH_j)$, distance among ith SCH and BS is denoted as $dis(SCH_i, BS)$ and sensor i is denoted as S_i.

- **Node degree (f_5)**

The amount of sensors connected to the next hop is denoted as node degree that is specified in Eq. (17).

$$f_5 = \sum_{i=1}^{m} CM_i \tag{17}$$

The weighted coefficient (μ_i) is allocated to every objective for transforming the multiple objective values into a single purpose function (F) according to Eq. (18).

$$F = \mu_1 \times f_1 + \mu_2 \times f_2 + \mu_3 \times f_3 + \mu_4 \times f_4 + \mu_5 \times f_5\,, \quad Where, \sum_{i=1}^{5} \mu_i = 1, \mu_i \in (0,1) \tag{18}$$

The trust value considered in the MO-TACOA based SCH discovery helps to avoid the malicious attacks, thereby preventing unwanted energy expenditure and packet loss. The remaining energy is used to discover the failure node which helps to ensure a reliable communication. The interspace is considered to minimize the energy expenditure by lessening the broadcasting distance. Further, the node degree is considered for minimizing the energy expenditure by performing load balancing over the network.

3.4 Clustering stage

After selecting the SCHs using MO-TACOA, an ID of SCH is transmitted by BS throughout the network, while weight coefficient for clustering (SCH_{weight}) is computed as per Eq. (19) for each SCH. The CMs joined with the CH have high weight coefficient that further helps to form clusters.

$$SCH_{weight} = \frac{E_{SCH}}{dis(S,SCH) \times dis(SCH,BS)} \tag{19}$$

3.5 Secure path discovery using MO-TACOA

The secure path discovery stage is initialized once the clusters are generated in the network. There are two different routing paths, single hop and multi hop path, considered in this MO-TACOA for minimizing the energy expenditure. The single hop routing is directly initialized when the transmitted SCH is near to the BS; otherwise, the multi hop path is discovered among the SCH and BS based on MO-TACOA. The multi hop path discovery is detailed in the below steps:

Table 1. Simulation parameters

Parameter	Value
Network size	200m × 200m
Location of BS	(70,70)
Number of nodes	50 and 100
Size of packet	4000 bits
Initial energy	0.5J
ε_{mp}	$0.0013pJ/bit/m^2$
ε_{fs}	$10pJ/bit/m^2$
E_{elec}	$50nJ/bit/m^2$

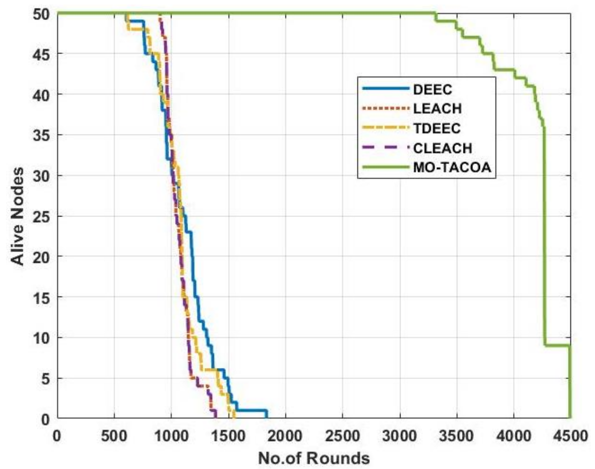

Figure. 2 Alive node analysis for 50 nodes

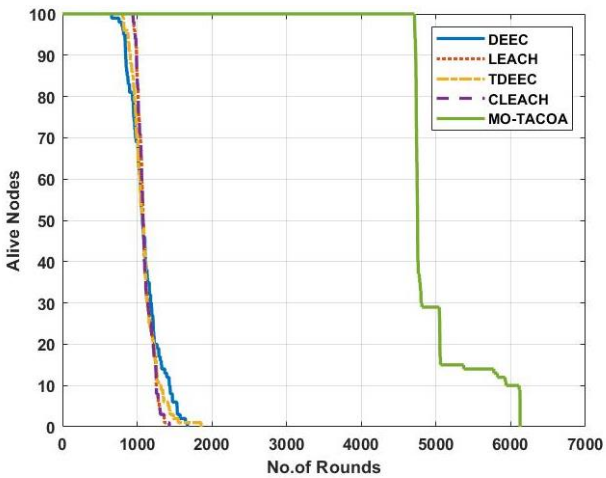

Figure 3 Alive node analysis for 100 nodes

1. Initially, the solutions of MO-TACOA are initialized with the possible paths, where the solution dimension is equal to the number of relay SCHs in the route.
2. For path discovery, the location update is identical to the previous section, for which Eq. (20) is used as a routing objective (RF).

$$RF = \delta_1 \times \sum_{i=1}^{m} E_{SCH_i} + \delta_2 \times \sum_{i=1}^{m} dis(SCH_i, BS)$$
$$Where, \sum_{i=1}^{2} \delta_i = 1, \delta_i \in (0,1) \quad (20)$$

Where, routing weighted coefficient (δ_i) is used in routing phase for transforming the multiple objective values into a single purpose function (RF). The derived objectives are used to discover the optimum secure shortest route which facilitates reliable data transmission. Moreover, the energy expenditure of the nodes is balanced by performing CH rotation. Therefore, the developed MO-TACOA is used to perform a secure data communication over IoT-WSN which aids in minimizing the packet loss.

4. Experimental results and discussions

The MO-TACOA is suggested to choose secure SCHs, and the path from the IoT-WSN. The clear examination of the experimental results is provided in the below sections.

4.1 Experimental setup and evaluation metrics

For this MO-TACOA method, the analysis is performed using MATLABR 2020b software with i7 processor, Windows 10 operating system and 16GB RAM. The parameters used during the simulation are shown in Table 1. The MO-TACOA is evaluated based on the alive nodes, energy expenditure, lifecycle, throughput and PLR.

4.2 Comparison of results with classical methods

Initially, the MO-TACOA is analyzed with the classical methods that include DEEC, LEACH, TDEEC and CLEACH. Here, the DEEC, LEACH, TDEEC and CLEACH are also developed for the specifications given in the Table 1.

4.2.1. Alive nodes analysis

Alive nodes are the amount of nodes with enough energy for broadcasting information over the network. The simulation graphs in the Figs. 2 and 3 depict the alive node analysis for 50 and 100 nodes, respectively. The MO-TACOA has higher alive nodes than the classical methods. The minimization in energy expenditure increases the alive nodes of MO-TACOA. The mitigation of malicious attacks by MO-TACOA avoids unwanted energy expenditure in the IoT-WSN. Moreover, load balancing among the clusters and optimum shortest path discovery further leads to a reduction in energy expenditure.

Received: February 4, 2024. Revised: April 16, 2024.

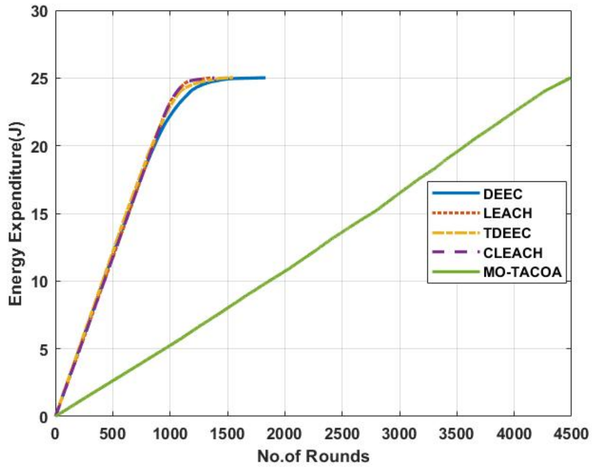

Figure. 4 Energy expenditure analysis for 50 nodes

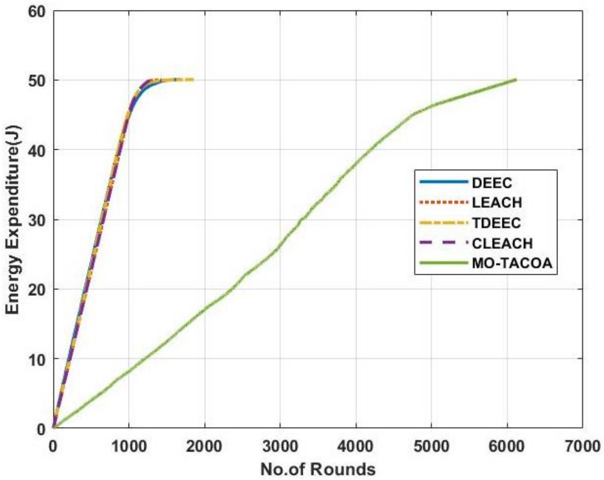

Figure. 5 Energy expenditure analysis for 100 nodes

4.2.2. Energy expenditure

Energy expenditure is the energy consumed while broadcasting and receiving information. The simulation graphs in the Figs. 4 and 5 illustrate the energy expenditure analysis for 50 and 100 nodes, respectively. These figures depict that the MO-TACOA has lesser energy consumption than the classical methods. The developed SCH and secure path discovery using MO-TACOA prevents unwanted energy usage in the network. Furthermore, load balancing among the clusters, and the discovery of the shortest path contribute to minimized energy expenditure.

4.2.3. Network lifecycle

The lifecycle of network is defined as the time period between initialization and the exhaustion of all nodes in the network. It is computed by using three parameters: First Node Expiration (FNE), Half Node Expiration (HNE) and Last Node Expiration (LNE).

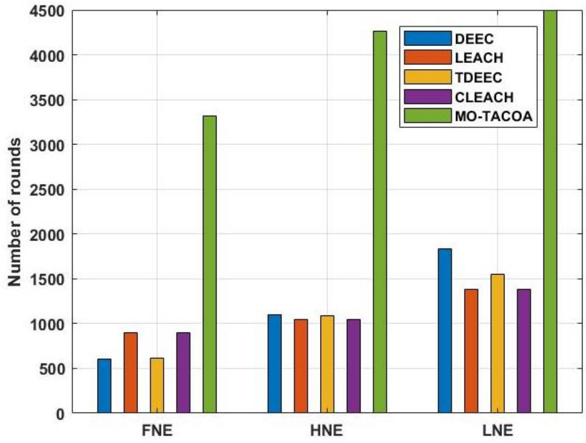

Figure. 6 Lifecycle analysis for 50 nodes

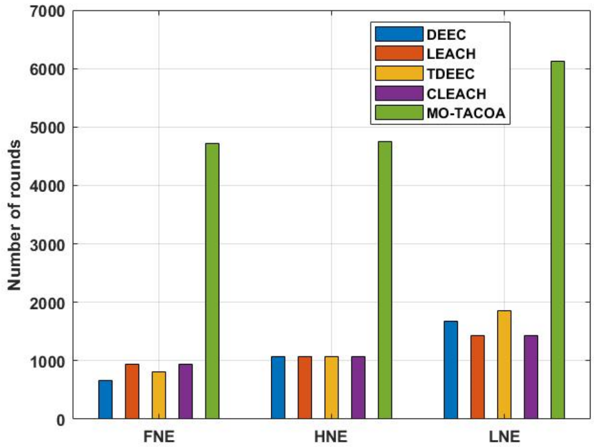

Figure. 7 Lifecycle analysis for 100 nodes

FNE is the round where the first node exhausts its energy, HNE is the round where half of the nodes exhaust their energy, while LNE is the round where all of the nodes exhaust their energy. The simulation graphs in Figs. 6 and 7 illustrate the lifecycle analysis for 50 and 100 nodes, correspondingly. These graphs further depict that the MO-TACOA has higher lifecycle than the classical methods. The minimization in energy expenditure increases the lifecycle of MO-TACOA. Moreover, the mitigation of malicious attacks based on the trust incorporated in MO-TACOA avoids unwanted energy expenditure. Further, as noted before, the load balancing among the clusters as well as the shortest path discovery minimize the energy expenditure.

4.2.4. Throughput and PLR

The amount of packets that successfully collect the BS is denoted as throughput, whereas PLR is the ratio between the lost packets and transmitted packets over the network. The simulation graphs in the Figs.

Received: February 4, 2024. Revised: April 16, 2024.

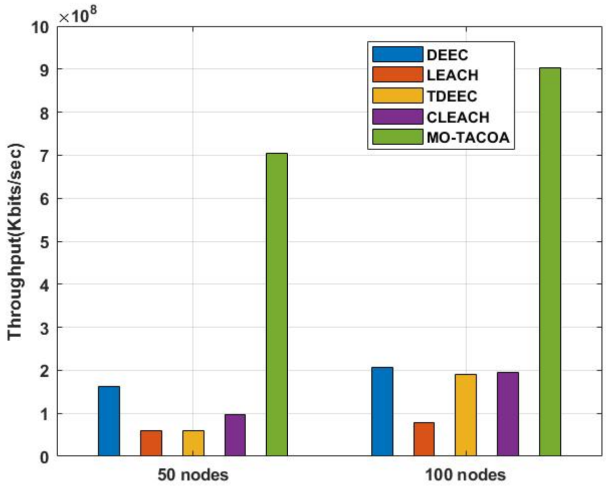

Figure. 8 Throughput analysis

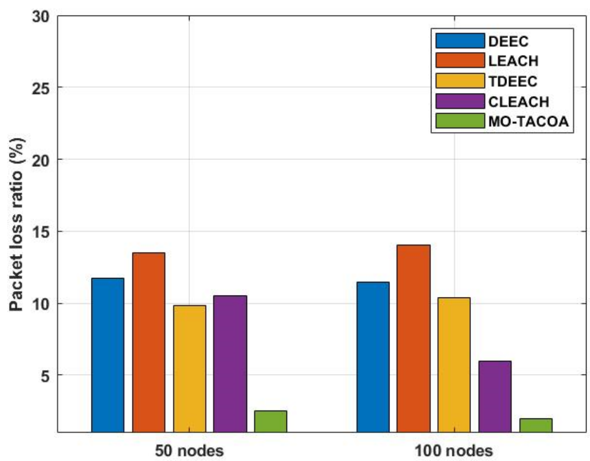

Figure. 9 PLR analysis

8 and 9 simultaneously depict the throughput and PLR analysis. These graphs represent that MO-TACOA has improved data delivery than the classical methods. The malicious attacks avoided by performing the SCH and secure route discovery in MO-TACOA avoid packet loss. Moreover, the node failure avoided during SCH selection is additionally utilized for enhancing data delivery.

4.3 Comparison of results with existing methods

The proposed MO-TACOA is compared with, Taylor C-SSA [18], TaylorSHO [19] and BITA [20] to evaluate its efficiency, as given in table 2. The network scenario is considered for simulation according to their respective existing researches.

The results given in the Tables 3 and 4 present the comparison of MO-TACOA with TaylorSHO [19] and Taylor C-SSA [18] & BITA [20], simultaneously. These tables prove that the MO-TACOA has improved performances than the Taylor C-SSA [18], TaylorSHO [19] and BITA [20]. The trust value considered by the MO-TACOA eliminates the malicious attacks, therefore preventing unwanted energy expenditure and packet loss over the IoT-WSN. Moreover, load balancing in the network also facilitates reduction in the energy expenditure of MO-TACOA.

Table 2. Comparative scenario

Parameters	Values
Nodes	100
Area	$100m \times 100m$
BS location	(50, 50)

Table 3. Comparison of MO-TACOA with TaylorSHO

Number of rounds	Throughput (kbps)	
	TaylorSHO [19]	MO-TACOA
200	2900	4255
400	5600	6751
600	9200	11094
800	12600	13579
1000	12900	16087

Table 4. Comparison of MO-TACOA with Taylor C-SSA and BITA

Number of rounds	Alive nodes		
	Taylor C-SSA [18]	BITA [20]	MO-TACOA
250	99	100	100
500	87	100	100
750	76	100	100
1000	68	100	100
1250	52	100	100
1500	44	95	100
1750	37	52	100
2000	31	24	100

5. Conclusion

In this research, secure cluster head and path identification using MO-TACOA are performed for ensuring a secure and reliable communication over the IoT-WSN. The MO-TACOA avoids malicious attacks while selecting the SCH, as well as is used to minimize the energy expenditure of the nodes, alongside performing load balancing over the nodes. Next, a secure shortest path via the CHs to BS is discovered by using the MO-TACOA. The combination of both single hop and multi hop routing is done in MO-TACOA to lessen the energy expenditure of the nodes. Therefore, the developed MO-TACOA is used to enhance security against malicious attacks and improves data delivery. The

 DOI: 10.22266/ijies2024.0831.07

Received: February 4, 2024. Revised: April 16, 2024.

simulation results represent that the MO-TACOA achieves superior performance than the Taylor C-SSA, TaylorSHO and BITA. The MO-TACOA accomplishes a throughput of 16087 kbps, resulting in being higher than the TaylorSHO, therefore preferable.

Notation List

Parameter	Description
S	Number of sensors
X_i	ith coati
m	Dimension i.e., number of SCHs
$x_{i,j}$	Evaluation of decision variable j
N	Total amount of coatis
F	Objective function
F_i	Objective function for coati i
X_i^{P1}	New location computed for coati i
$x_{i,j}^{P1}$	New coati in dimension j
I	Integer value that is either 0 or 2
Iguana	Location of prey
Iguana_j	Location of prey in dimension j
Iguana^G	Prey's location in ground
Iguana_j^G	Prey's location in ground at dimension j
F_{Iguana}	Fitness value of Iguana^G
$\lfloor . \rfloor$	Floor function
ub_j and lb_j	Upper and lower values of the j th decision variable
r	Random variable among [0,1]
F_i^{P1}.	Fitness of the new location
$P2$	Location and fitness of coati in the 2nd phase
ub_j^{local} and lb_j^{local}	Local upper and lower bounds of jth decision variable
f_1	Trust
DT	Direct trust
IDT	Indirect trust
a & b	Nodes
t	Time
NN	Amount of neighboring nodes
τ	Constant
f_2	Residual energy
E_{SCH_i}	Remaining energy of ith SCH
f_3	Interspace between sensors & SCH
f_4	Interspace between SCH & BS
CM_j	Cluster members of the jth cluster
$dis(S_i, SCH_j)$	Distance among sensor i and SCH j
$dis(SCH_i, BS)$	Distance among ith SCH and BS
f_5	Node degree
μ_i	Weighted coefficient
SCH_{weight}	Weight coefficient for clustering
RF	Routing objective
δ_i	Routing weighted coefficient

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The supervision and project administration, have been done by 2nd author.

References

[1] M.K. Roberts, and P. Ramasamy, "An improved high performance clustering based routing protocol for wireless sensor networks in IoT", *Telecommunication Systems*, Vol. 82, No. 1, pp. 45-59, 2023.

[2] P.P.I. Vazhuthi, A. Prasanth, S.P. Manikandan, and K.K.D. Sowndarya, "A hybrid ANFIS reptile optimization algorithm for energy-efficient inter-cluster routing in internet of things-enabled wireless sensor networks", *Peer-to-Peer Networking and Applications*, Vol. 16, No. 2, pp. 1049-1068, 2023.

[3] P. Velmurugadass, S. Dhanasekaran, S.S. Anand, and V. Vasudevan, "Quality of Service aware secure data transmission model for Internet of Things assisted wireless sensor networks", *Transactions on Emerging Telecommunications Technologies*, Vol. 34, No. 1, p. e4664, 2023.

[4] I. Kala, S. Karthik, and K. Srihari, "Advanced hybrid secure multipath optimized routing in Internet of Things (IoT)-based WSN", *International Journal of Communication Systems*, Vol. 34, No. 8, p. e4782, 2021.

[5] Y. Zhang, Q. Ren, K. Song, Y. Liu, T. Zhang, and Y. Qian, "An Energy-Efficient Multilevel Secure Routing Protocol in IoT Networks", *IEEE Internet of Things Journal*, Vol. 9, No. 13, pp. 10539-10553, 2022.

[6] A. Srivastava, and R. Paulus, "ELR-C: A Multi-objective Optimization for Joint Energy and Lifetime Aware Cluster Based Routing for WSN Assisted IoT", *Wireless Personal Communications*, Vol. 132, No. 2, pp. 979-1006, 2023.

[7] I.G. Loretta, and V. Kavitha, "Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment", *Peer-to-Peer*

Networking and Applications, Vol. 14, No. 2, pp. 821-836, 2021.

[8] G. Thahniyath, and M. Jayaprasad, "Secure and load balanced routing model for wireless sensor networks", *Journal of King Saud University-Computer and Information Sciences*, Vol. 34, No. 7, pp. 4209-4218, 2022.

[9] U. Panahi, and C. Bayılmış, "Enabling secure data transmission for wireless sensor networks based IoT applications", *Ain Shams Engineering Journal*, Vol. 14, No. 2, p. 101866, 2023.

[10] N.P.R. Kumar, and G.J. Bala, "A cognitive knowledged energy-efficient path selection using centroid and ant-colony optimized hybrid protocol for WSN-assisted IoT", *Wireless Personal Communications*, Vol. 124, No. 3, pp. 1993-2028, 2022.

[11] G.A. Senthil, A. Raaza, and N. Kumar, "Internet of things energy efficient cluster-based routing using hybrid particle swarm optimization for wireless sensor network", *Wireless Personal Communications*, Vol. 122, No. 3, pp. 2603-2619, 2022.

[12] N. Subramani, S.K. Perumal, J.S. Kallimani, S. Ulaganathan, S. Bhargava, and S. Meckanizi, "Controlling energy aware clustering and multihop routing protocol for IoT assisted wireless sensor networks", *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 21, p. e7106, 2022.

[13] M. Alotaibi, "Improved Blowfish Algorithm-Based Secure Routing Technique in IoT-Based WSN", *IEEE Access*, Vol. 9, pp. 159187-159197, 2021.

[14] A.W. Mudasser, and S.A.A.A. Gafoor, "Secure Internet of Things based hybrid optimization techniques for optimal centroid routing protocol in wireless sensor network", *Concurrency and Computation: Practice and Experience*, Vol. 35, No. 6, p. 1, 2023.

[15] A.S. Reegan, and V. Kabila, "Highly secured cluster based WSN using novel FCM and enhanced ECC-ElGamal encryption in IoT", *Wireless Personal Communications*, Vol. 118, No. 2, pp. 1313-1329, 2021.

[16] P.S. Prakash, D. Kavitha, and P.C. Reddy, "Safe and secured routing using multi-objective fractional artificial lion algorithm in WSN", *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 21, p. e7098, 2022.

[17] S. Gali, and V. Nidumolu, "An intelligent trust sensing scheme with metaheuristic based secure routing protocol for Internet of Things", *Cluster Computing*, Vol. 25, No. 3, pp. 1779-1789, 2022.

[18] A. Vinitha, M.S.S. Rukmini, and Dhirajsunehra, "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*, Vol. 34, No. 5, pp. 1857-1868, 2022.

[19] S.S. Kalburgi, and M. Manimozhi, "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*, Vol. 81, No. 11, pp. 15815-15839, 2022.

[20] L. Kumar, and P. Kumar, "BITA-Based Secure and Energy-Efficient Multi-Hop Routing in IoT-WSN", *Cybernetics and Systems*, Vol. 54, No. 6, pp. 809-835, 2023.

[21] P.D. Kusuma, and A. Dinimaharawati, "Extended stochastic coati optimizer", *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 3, pp. 482-494, 2023.

[22] P.D. Kusuma, and F.C. Hasibuan, "Attack-Leave Optimizer: A New Metaheuristic that Focuses on The Guided Search and Performs Random Search as Alternative", *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 3, pp. 244-257, 2023, doi: 10.22266/ijies2023.0630.19.

[23] P.D. Kusuma, and A.L. Prasasti, "Walk-Spread Algorithm: A Fast and Superior Stochastic Optimization", *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 5, pp. 275-288, 2023, doi: 10.22266/ijies2023.1031.24.