Secure cluster-based routing using multi objective-trust centric artificial algae algorithm for wireless sensor network

Divyashree Habbanakuppe Balachandra[1], Puttamadappa Chaluve Gowda[1], Nandini Prasad Kanakapura Shivaprasad[2]
[1]Department of Electronics and Communication Engineering, Dayananda Sagar University, Bengaluru, India
[2]Department of Information Science and Engineering, Dr. Ambedkar Institute of Technology, Bengaluru, India

Article Info

Article history:

Received Jun 8, 2022
Revised Sep 25, 2022
Accepted Oct 21, 2022

Keywords:

Energy consumption
Multi objective-trust centric artificial algae algorithm
Packet delivery ratio
Wireless sensor network

ABSTRACT

Nowadays, wireless sensor network (WSN) is developed as a key technology to observe and track applications over a wide range. However, energy consumption and security are considered as important issues in the WSN. In this paper, the multi objective-trust centric artificial algae algorithm (M-TCAAA) is proposed to accomplish a secure broadcasting over the WSN. The proposed M-TCAAA is used to choose the secure cluster head (SCH) as well as routing path, based on the distinct fitness measures such as trust, communication cost, residual energy, and node degree. Hence, the M-TCAAA is used to ensure a secure data transmission while decreasing the energy consumed by the nodes. The performance of the M-TCAAA is analyzed by means of energy consumption, packet delivery ratio (PDR), throughput, end to end delay (EED), normalized routing load (NRL), and network lifetime. The existing researches namely energy aware trust and opportunity-based routing with mobile nodes (ETOR-MN), grey wolf updated whale optimization (GUWO), secure cluster-based routing protocol (SCBRP), secure routing protocol based on multi-objective ant-colony-optimization (SRPMA) and multi objective trust aware hybrid optimization (MOTAHO) are considered for evaluating the M-TCAAA. The PDR of the M-TCAAA for 100 nodes is 99.87%, which is larger than the ETOR-MN, GUWO, SRPMA and MOTAHO.

Corresponding Author:

Divyashree Habbanakuppe Balachandra
Department of Electronics and Communication Engineering, Dayananda Sagar University
Bengaluru, India
Email: divyabalachandra94@gmail.com

1. INTRODUCTION

Wireless sensor networks (WSNs) are a generation of networks that usually have a huge amount of inexpensive sensors connected through wireless signals. The objective is to collect data from the environment using nearby network sensors followed by broadcasting the collected data to the base station (BS) [1], [2]. In general, the sensors have some important abilities such as mobilizing, sensing, computing, and data transmission [3]. The advantages of the WSN are less installation cost, easy deployment, self-configuration capacity and it has the probability of distribution through a huge area [4]. WSN is employed in many fields such as intelligent agriculture, environment monitoring, industrial safety, smart home, medicine, education, military and so on [5]–[8]. The sensors of the WSN have inadequate memory for data storage, less computing capability, and less battery power [9]. The energy consumption is considered a primary issue because the battery of the sensor is not rechargeable and replaceable. Therefore, a cluster based routing is developed to minimize the energy consumption [10]–[12].

The sensor nodes are grouped into many clusters from their transmission range. One leader node namely cluster head (CH) is chosen to handle the clusters and the sensor nodes (i.e., cluster members (CMs)) gather the data from the environment and broadcast it to the CH. Cluster communication is generally categorized into two types known as intra-cluster and inter-cluster communication. The single-hop broadcasting takes place in intra-cluster data transmission and the respective CMs directly send the data to the CH [13]. Subsequently, the CH broadcasts the gathered information to BS using either a single-hop or multi-hop routing approach [14]. Security is considered a most important issue because the WSN is open and it is not completely protected from adversaries. This is generally associated with the sensor's working conditions and the environment of WSN applications. Since the sensors are installed without any security, it is susceptible to malicious attacks [15]. It is difficult to increase the sensors' energy, due to naturally unsuitable conditions of the environment, hence it is required to develop a secure and energy aware routing for the network [16], [17].

Pavani and Rao [13] presented secure cluster-based routing protocol (SCBRP) to develop a secure clustering and routing in WSN. The SCBRP was used the adaptive particle swarm optimization (PSO) for clustering and optimized firefly algorithms for identifying the shortest path. The advanced encryption standard and RC6 are used to encrypt the input data before broadcasting over the network. The path developed using firefly algorithms does not considered the trust value of the node. Khot and Naik [18] developed a secure routing using the particle-water wave optimization (P-WWO). The P-WWO was the integration of and PSO and water wave optimization. At first, the PSO based cellular automata were employed to select the CH which was utilized in the secure route for transmitting the data. Hence, the transmission path with less delay and distance was selected using the P-WWO. For an effective analysis, the analysis of data delivery was important, but this P-WWO failed to analyze the data delivery. Hajiee *et al.* [19] presented the existing researches namely energy aware trust and opportunity based routing with mobile nodes (ETOR-MN) to select the best route over the network. This energy-aware trust and opportunity-based routing (ETOR) comprised of two main steps: first, choosing a secure sensor and second, choosing opportunistic sensors from secure sensors, to accomplish the routing in WSN. The routing overhead of the ETOR-MN was high due to the high amount of control packers used during the route identification.

Reddy *et al.* [20] implemented the grey wolf updated whale optimization (GUWO) to select a CH from the network [17]. The fitness functions considered in the GUWO were distance, energy, delay and security. However, this work considered the basic routing as low energy adaptive clustering hierarchy (LEACH). But the LEACH directly transmitted the data to BS which affected the network performance. Kumar and Vimala [21] developed an exponentially-ant lion whale optimization (E-ALWO) to broadcast the data over the WSN. The developed E-ALWO was the combination of an exponentially weighted moving average approach with ant lion and whale optimizations. The E-ALWO selected the CH only based on the delay and energy whereas the route was generated based on the energy and trust update. Prithi and Sumathi [22] presented a secure data transmission using the deterministic finite automata and PSO in WSN. The learning dynamic deterministic finite automata were established to examine the node as well as packet route, and it dynamically learned about the network. Further, the route was optimized by using the PSO which was used to obtain an energy efficient communication [23]. But this work created the clusters based only on the geographical information which caused higher energy consumption.

Sun *et al.* [24] implemented a secure routing protocol based on multi-objective ant-colony-optimization (SRPMA) for WSN where the routing was done based two different objectives such as energy and trust value of the node. Here, an improved D-S evidence theory was used to evaluate the trust value of the node. The developed SRPMA mainly considered only on secure routing among the network. Veerabadrappa and Lingareddy [25] developed the multi objective trust aware hybrid optimization (MOTAHO) for performing secure data broadcasting over the WSN. The MOTAHO was the combination of chicken swarm and moth flame optimization where it was optimized by using number of hops, distance, energy and trust. However, the distribution radius of nodes are required to be considered for achieving better energy efficiency.

An energy efficient routing is considered as a significant task for transmitting the information among the sensors and BS. Further, the routing and trust evaluation is considered as a key issue in the WSN. Other essential issues of the WSN also include energy consumption, security, higher routing overhead, single hop data transmission and inappropriate fitness function computation. More specifically, the malicious nodes misroute or drop the information during the communication. These issues in the existing routing approaches are considered as motivations behind this research, therefore, secure cluster-based routing using multi objective-trust centric artificial algae algorithm (M-TCAAA) is proposed to achieve a reliable communication over the network.

The research contributions are concisely stated as follows: i) the M-TCAAA with a distinct fitness function is proposed to select the optimal secure cluster head (SCH) and the secure route from the network. The artificial algae algorithm (AAA) is considered in this research because of its effective balance among the exploration and exploitation phases; ii) the K-means clustering approach is used along with the M-TCAAA-based SCH selection for lessening the energy consumption of the WSN. The malicious nodes that exist in the network are avoided during SCH and route selection which are used to obtain reliable communication over the network; and iii) the M-TCAAA based secure multi hop routing is used to increase the number of packets received by the destination. Further, the optimal shortest path selection is used to minimize the energy consumption.

This research paper is organized as follows: A detailed description of the M-TCAAA based CH selection and route discovery are given in section 2. Section 3 delivers the outcome of the M-TCAAA along with its comparative analysis. Finally, section 4 presents the conclusion.

2. M-TCAAA METHOD

In this research, the SCH from the clusters and secure routes over the network are discovered using the M-TCAAA. Since, the malicious attack causes the packet drop [26] and unwanted energy consumption, the proposed M-TCAAA avoids the malicious attacks while broadcasting the data over the WSN. Moreover, energy consumption of the sensors is also minimized by using the M-TCAAA which improves the lifetime of the WSN [27]. The architecture of the M-TCAAA is shown in Figure 1.

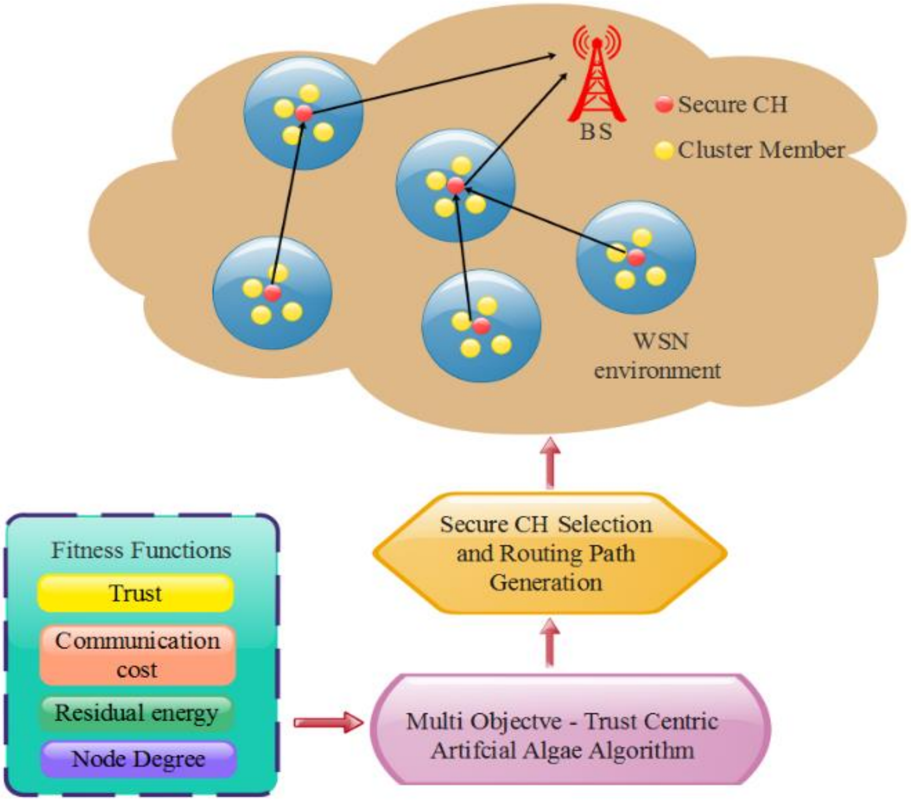

Figure 1. Architecture of the M-TCAAA

2.1. Clustering process

Initially, the sensors are randomly deployed followed by the K-means approach which is used to cluster the sensors of the WSN. The K-means mainly depends on the calculation of Euclidian distance between the sensors. After clustering the network, an SCH and a secure route are identified using the M-TCAAA method.

2.2. SCH selection using M-TCAAA

From the clusters, an optimal SCH is selected using the M-TCAAA which is used to avoid malicious attacks. Therefore, the packet drops and unwanted energy consumption caused by the malicious attacks are avoided while accomplishing the data delivery. Generally, the conventional AAA [28] imitates the living activities of algae. The SCH selection process is detailed as follows:

2.2.1. Initialization for SCH selection

The initialization of M-TCAAA's algal colony contains the group of candidate sensors that is required to be chosen as secure cluster head (SCH). Each algal colony is set with the random sensor ID from 1 to M, where M denotes the total sensors in the WSN. Let's consider the M-TCAAA's i^{th} algal colony is $x_i = (x_{i,1}, x_{i,2}, \dots, x_{i,D})$, where the algal colony's dimension (i.e., number of SCHs) is represented as D. The location of the algal colony is $x_{i,rc}, 1 \leq rc \leq D$ which determines the random sensor from the total sensors of the WSN.

2.2.2. Iterative process of M-TCAAA

The iterative process of algae includes three different phases that are: evolutionary process, adaption, and helical movement phase. The algae location where it gets adequate amount of light is defined as the global optimal point. The alga replicates into two new algae cells during the evolutionary process which is related to the original mitotic division. This reproduction delivers sufficient nutrients and the colony obtains sufficient light, otherwise, the algal colony expires after some time. As shown in (1) shows the Monod model used to calculate the kinetics of the Algal colony.

$$\mu = \frac{\mu_{max} S}{K_S + S} \tag{1}$$

where, the growth rate and maximum specific growth are represented as μ and μ_{max} respectively; the nutrient amount/fitness value is denoted as S and the constant denoting the substrate half-saturation of the colony is represented as K_S. As shown in (2) is algae's colony size in a certain time $t + 1$.

$$G_i^{t+1} = \mu_i^t G_i^{t+1} \tag{2}$$

where the size of the algal colony i in time t is represented as G_i^t and i ranges from 1 to N; N defines the total number of populations.

The smallest and biggest algal colony are chosen for reproduction purposes according to the nutrient content whereas (3) and (4) show the selection of the smallest and biggest algal colony.

$$biggest^t = \max(G_i^t) \tag{3}$$

$$smallest^t = \min(G_i^t) \tag{4}$$

From the smallest set, an algal cell m is randomly chosen and (5) shows the accomplished reproduction by duplicating the huge algal cell.

$$smallest_m^t = biggest_m^t \quad m = \{1,2, \dots, D\} \tag{5}$$

In the adaptation, the algal colony that has not grown adequately, attempts to bear the similarity of the colony that has huge algae. Initially, the artificial alga is fixed with 0 starvation value. If the algal cell does not receive enough light, then the starvation value is increased according to the time t. The artificial alga has a high starvation value as shown in (6) and it is adapted as shown in (7).

$$starving^t = \max(A_i^t) \tag{6}$$

$$starving^{t+1} = starving^t(biggest^t - starving^t) \times rand(0,1) \tag{7}$$

where, the i^{th} algal colony's starvation value is denoted as A_i^t; the colony with a higher starvation level is denoted as $starving^t$. Here, the process of adaption is determined by constant value ranges between $[0, 1]$.

Further, the new solution is generated using the helical movement as shown in the (8) to (10).

$$x_{im}^{t+1} = x_{im}^t + (x_{jm}^t - x_{im}^t)(\Delta - \tau^t(x_i))p \tag{8}$$

$$x_{ik}^{t+1} = x_{ik}^t + \left(x_{jk}^t - x_{ik}^t\right)\left(\Delta - \tau^t(x_i)\right) \cos \alpha \tag{9}$$

$$x_{il}^{t+1} = x_{il}^t + \left(x_{jl}^t - x_{il}^t\right)\left(\Delta - \tau^t(x_i)\right) \sin \beta \tag{10}$$

where, the randomly chosen current solutions are denoted as x_{im}^t, x_{ik}^t and x_{il}^t; the neighbor algal colony detected using tournament selection is denoted as x_j^t; α and β are in the range of $[0, 2\pi]$; p is in the range of $[-1,1]$; shear force is denoted as Δ and the i^{th} algal cell's friction surface area is denoted as $\tau^t(x_i)$. Therefore, this iterative process returns optimal set of SCHs from the clusters according to the derived fitness functions. The fitness function derivation of M-TCAAA is explained in the following section.

2.2.3. Derivation of fitness function

The M-TCAAA considers multiple fitness functions while selecting the SCHs from the clusters. There are four fitness measures namely trust (fm_1), communication cost (fm_2), residual energy (fm_3), and node degree (fm_4) that are considered in M-TCAAA. The fitness function mentioned in (1) is expressed in (11).

$$S = \delta_1 \times fm_1 + \delta_2 \times fm_2 + \delta_3 \times fm_3 + \delta_4 \times fm_4 \tag{11}$$

where, $\delta_1 - \delta_4$ are the weight parameters allocated to each fitness measure. Trust expressed in (12) is considered as the primary objective for this SCH selection. The nodes in the WSN exchanges the information based on the mutual trust relationship for avoiding the malicious attacks during data delivery. Here, the trust is computed based on the communication carried out by the nodes. Therefore, the trust is the ratio of packets received by the node and packets sent by the source node. The required communication cost for interacting with the adjacent node is shown in (13). The sensors are supposed to perform data collection and transmission over the network. Therefore, the node with high residual energy is preferred for data delivery. As shown in (14) shows the expression for residual energy. Further, the node degree defines the number of hops connected to the CH. A lesser node degree is used to achieve a lesser energy consumption.

$$fm_1 = \frac{Packets\ received_{a,b}}{Packets\ sent_{a,b}} \tag{12}$$

$$fm_2 = \frac{d_{avg}^2}{d_0^2} \tag{13}$$

$$fm_3 = \sum_{i=1}^{D} E_{SCH_i} \tag{14}$$

$$fm_4 = \sum_{i=1}^{D} CM_i \tag{13}$$

where, a and b are the example nodes; the average distance between the sensor and neighbour node is represented as d_{avg}^2; the sensor's distribution radius is denoted as d_0^2; the residual energy of i^{th} SCH is denoted as E_{SCH_i} and the number of CMs connected to the i^{th} CH is denoted as CM_i. Therefore, an appropriate SCH is selected using the aforementioned fitness function. The trust used in the fitness measures helps to avoid the malicious nodes, because these malicious nodes cause packet drop over the network. Next, the communication cost is used to identify the path with small distance that results in lesser energy consumption. The residual energy is used to identify whether the node has enough energy to broadcast the data or not. Based on this, the packet delivery to the BS is improved over the network. Further, the node degree is also considered for minimization of energy consumption of the nodes.

2.3. Routing using M-TCAAA

After selecting the SCH from the clusters, the route discovery is made using the M-TCAAA. The developed M-TCAAA is used to discover the secure route based on the fitness function derived in sub sub section 2.2.3. The flowchart of the overall M-TCAAA method is shown in the Figure 2.

At first, the route request message is transmitted by the source CH to all the nearby existing CHs in the network. Next, the optimal relay node identified from the M-TCAAA sends the route reply residential real estate project (RREP) message back to the source CH. The same procedure is continued until it reaches the destination node i.e., BS. When the source CH receives the RREP message, the secure route is established in the WSN.

The proposed M-TCAAA based secure CH selection and routing is used to avoid the malicious nodes. By avoiding the malicious nodes, the packet drop and energy consumption are minimized in the WSN. The reduction in the node's energy consumption is used to enhance the network lifetime that results in higher amount of data delivery. Therefore, the M-TCAAA is used to achieve the secure reliable communication over the network. The Pseudo code of the M-TCAAA based SCH selection is given in algorithm 1. In M-TCAAA based route discovery, the possible paths are given as input instead of candidate CH position.

Algorithm 1: Initialize algal colonies as candidate SCH node location and their ID.

```
Compute fitness ($S$) of initialized solution based on (11).
for time=simulation time do
        for i=1 to total populations do
                Randomly choose three algae cells of colony.
                Create the new solutions based on (8)to(10).
                Copy a randomly chosen single cell of huge colony to small colony.
                Discover most starveling colony by applying (7) with huge colony, when
        adaptation rate control is met.
                Compute fitness of updated solution based on (11).
                Find the optimal SCH using fitness value ($S$).
                if $S_i < S_{best}$
                        $S_{best} = S_i$.
                        Returns updated solution as optimal solution.
                end if
        end for
end for
```

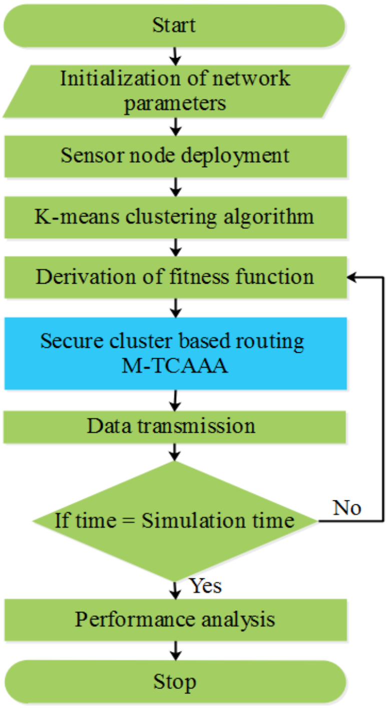
Start
Initialization of network parameters
Sensor node deployment
K-means clustering algorithm
Derivation of fitness function
Secure cluster based routing M-TCAAA
Data transmission
If time = Simulation time
No
Yes
Performance analysis
Stop

Figure 2. Flowchart of the overall M-TCAAA method

3. RESULTS AND DISCUSSION

The implementation and simulation of the M-TCAAA is done in the network simulator (NS) -2.34 in a system featured with 6 GB RAM and i5 processor. The sample deployment of WSN for 20 nodes is displayed using network animator in Figure 3. The simulation parameters that are used to design the M-TCAAA is shown in the Table 1. The performance of the M-TCAAA is analyzed by means of energy consumption, packet delivery ratio (PDR), throughput, end to end delay (EED), normalized routing load (NRL) and network lifetime. Here, the electronic test orders and results (ETOR) with mobile node (ETOR-MN) [19] is considered to analyze the efficiency of the M-TCAAA.

3.1. Energy consumption

Energy consumption is defined as the amount of energy consumed while receiving and broadcasting the data packets over the network. The energy consumption comparison for ETOR-MN [19] with the M-TCAAA is shown in Figure 4. From Figure 4, it can be concluded that the M-TCAAA achieves reduced energy consumption than the ETOR-MN [19]. For instance, the energy consumption of the M-TCAAA for 100 nodes is 0.41 J whereas the energy consumption of ETOR-MN [19] is 1.94 J. The SCH and secure route selected using the M-TCAAA minimizes the unwanted energy consumption of the nodes. Whereas, the mobile nodes cause higher energy consumption in ETOR-MN [19].

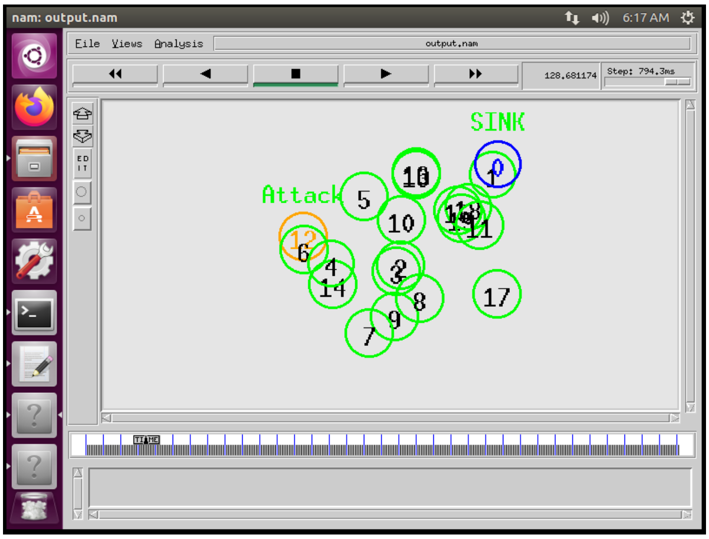

Figure 3. Simulated network for 20 nodes

Table 1. Simulation parameters

Parameter	Value
Number of nodes	20, 40, 60, 80 and 100
Area	200 × 200 m
Initial energy	5J
Network interface type	Wireless PHY
Mac	IEEE 802.11 DCP
Traffic source	CBR
Propagation model	Two-ray ground reflection
Antenna pattern	Omni antenna

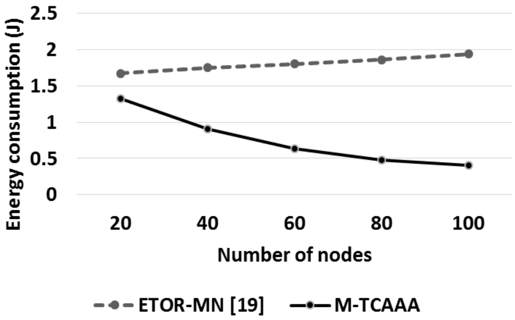

Figure 4. Analysis of energy consumption

3.2. Packet delivery ratio

PDR is defined as the proportion between amount of packets received by the BS and amount of packets created by the BS. The analysis of PDR for ETOR-MN [19] with the M-TCAAA is shown in the Figure 5. This PDR analysis shows that the M-TCAAA has higher PDR than the ETOR-MN [19]. For example, the PDR of the M-TCAAA for 100 nodes is 99.87 % whereas the PDR of the ETOR-MN [19] is 66 %. The proposed M-TCAAA method achieves higher PDR by avoiding the malicious attacks based on the node’s trustworthiness. Whereas, the link failure that occurs in ETOR-MN [19] results in lesser PDR.

3.3. Throughput

Throughput is defined as the amount of packets successfully received at the BS at a time T. The throughput comparison for ETOR-MN [19] with the M-TCAAA is shown in Figure 6. From Figure 6, it becomes clear that the M-TCAAA achieves higher throughput than the ETOR-MN [19]. For example, the throughput of the M-TCAAA for 100 nodes is 1089.54 Kbps whereas the throughput of ETOR-MN [19] is

324.5 Kbps. The malicious nodes avoided by the M-TCAAA improves the amount of packets successfully received by the BS. Accordingly, the throughput of the M-TCAAA is increased while transmitting the data packets.

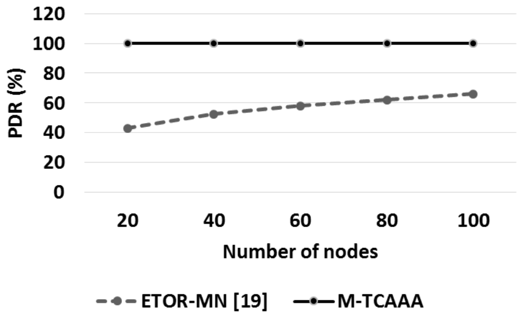

Figure 5. Analysis of PDR

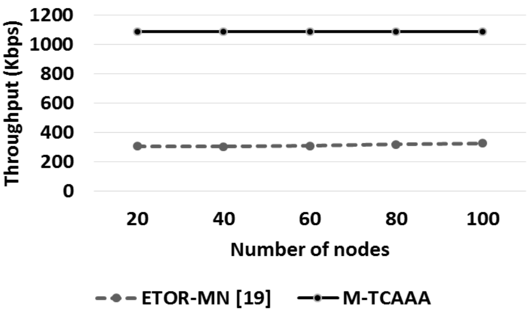

Figure 6. Analysis of throughput

3.4. End to end delay

EED defines the amount of time taken by the node to transmit the data to the BS over the network. Figure 7 shows the comparison of EED for ETOR-MN [19] and M-TCAAA. This EED analysis shows that the M-TCAAA achieved less EED than the ETOR-MN [19]. For example, the EED of the M-TCAAA for 100 nodes is 0.028 ms whereas the EED of the ETOR-MN [19] is 10.5 ms. The M-TCAAA achieves lesser EED because of its lesser amount of control packet utilization and lesser transmission distance. On the other hand, the link failure caused in the ETOR-MN [19] increases the delay while delivering the data.

3.5. Normalized routing load

NRL is the proportion between the number of routing packet transmission and number of data packet transmission. The NRL comparison for ETOR-MN [19] with the M-TCAAA is shown in the Figure 8. From the Figure 8, it is can be concluded that the M-TCAAA achieves lesser NRL than the ETOR-MN [19]. For example, the NRL of the M-TCAAA for 100 nodes is 0.184 whereas the NRL of ETOR-MN [19] is 13. The M-TCAAA uses lesser amount of control packets due to its distinct fitness measures that results in lesser NRL.

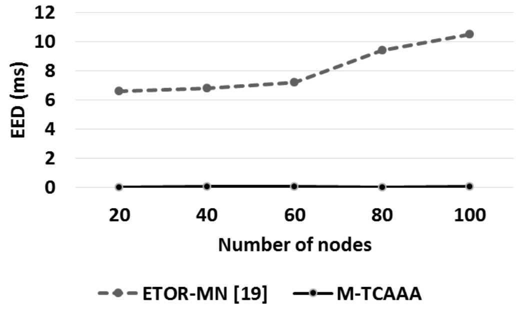

Figure 7. Analysis of EED

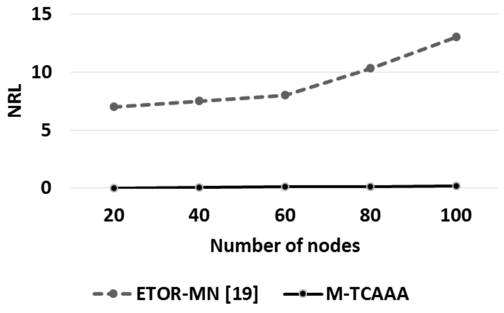

Figure 8. Analysis of NRL

3.6. Network lifetime

Network lifetime is the time measure in which the sensor in the WSN exhausts its complete energy during the communication. Figure 9 shows the comparison of network lifetime for ETOR-MN [19] and M-TCAAA. This network lifetime analysis shows that the M-TCAAA achieved higher network lifetime than the ETOR-MN [19]. For example, the network lifetime of the M-TCAAA for 100 nodes is 781.58 s whereas the network lifetime of the ETOR-MN [19] is 265 s. An unwanted energy consumption caused by the area of the malicious node is avoided by using the M-TCAAA, Moreover, the route with a lesser transmission distance identified from the M-TCAAA also minimizes the energy consumption. Therefore, the nodes with lesser energy consumption tend to have a higher network lifetime.

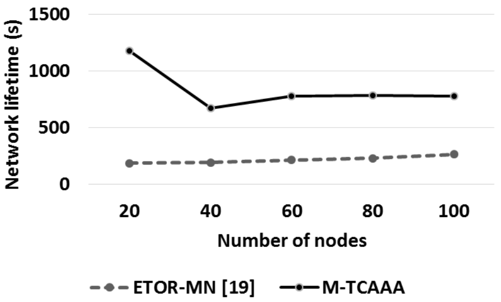

Figure 9. Analysis of network lifetime

Table 2 provides the comparative analysis of the M-TCAAA with SCBRP [13], ETOR-MN [19], GUWO [20], SRPMA [24] and MOTAHO [25], where NA defines the values which are not available in those existing researches. Here, the comparison is done by varying the nodes. This comparison shows that the M-TCAAA performs well than the SCBRP [13], ETOR-MN [19], GUWO [20], SRPMA [24] and MOTAHO [25]. For example, the PDR of the M-TCAAA for 100 nodes is 99.87% which is much higher than the ETOR-MN [19], GUWO [20], SRPMA [24] and MOTAHO [25]. The high amount of control packets used during the route discovery increases the routing overhead of the ETOR-MN [19]. Moreover, the direct data transmission of LEACH used in the GUWO [20] increases the packet drop over the network. The distinct fitness metrics used in the route discovery of M-TCAAA helps to minimize the control packets that leads to achieve less NRL. Additionally, the multi hop routing accomplished by the M-TCAAA is used to improve the data delivery of the WSN. The malicious nodes that exist in WSN are avoided based on the trust value considered in the M-TCAAA. Therefore, the proposed M-TCAAA is used to minimize energy consumption and improve the PDR of the WSN.

Table 2. Comparative analysis of M-TCAAA

Performances	Methods	Number of nodes				
		20	40	60	80	100
Energy consumption (J)	SCBRP [13]	NA	NA	NA	NA	42.85
	ETOR-MN [19]	1.67	1.75	1.8	1.86	1.94
	SRPMA [24]	NA	NA	NA	NA	37
	MOTAHO [25]	NA	NA	NA	NA	0.87
	M-TCAAA	1.32	0.91	0.64	0.48	0.41
PDR (%)	ETOR-MN [19]	43	52.5	58	62	66
	GUWO [20]	NA	NA	NA	NA	96.12
	SRPMA [24]	NA	NA	NA	NA	93
	MOTAHO [25]	NA	NA	NA	NA	97.44
	M-TCAAA	99.94	99.85	99.87	99.96	99.87
Throughput (Kbps)	ETOR-MN [19]	305	302	308	317.5	324.5
	GUWO [20]	NA	NA	NA	NA	242
	M-TCAAA	1089.75	1089.54	1089.54	1090.52	1089.54
EED (ms)	ETOR-MN [19]	6.6	6.8	7.2	9.4	10.5
	M-TCAAA	0.014	0.029	0.028	0.022	0.028
NRL	ETOR-MN [19]	7	7.5	8	10.3	13
	SRPMA [24]	NA	NA	NA	NA	0.5
	MOTAHO [25]	NA	NA	NA	NA	0.0685
	M-TCAAA	0.017	0.058	0.112	0.124	0.184
Network lifetime (s)	ETOR-MN [19]	185	193	212	230	265
	M-TCAAA	1177.56	671.56	781.58	782.58	781.58

4. CONCLUSION

The nodes of the WSN have limited battery power, therefore the problem of higher energy consumption caused by the malicious attacks should be addressed well for improving the network performances. Therefore, a secure cluster-based routing is developed for improving the network lifetime and data delivery under malicious attacks. In this research, the K-means clustering and M-TCAAA based SCH selection are done to minimize the energy consumption and to improve the security against malicious attacks. Subsequently, the secure route is selected via CHs for transmitting the data over the network. The M-TCAAA is optimized with distinct fitness measures such as trust, communication cost, residual energy, and node degree. Hence, the proposed M-TCAAA achieves a higher network lifetime and greater PDR after efficiently avoiding malicious nodes. The M-TCAAA outperforms than the SCBRP, ETOR-MN, GUWO, SRPMA and MOTAHO, which can be justified by these results: PDR of the M-TCAAA for 100 nodes is 99.87%, which is larger than the ETOR-MN, GUWO, SRPMA and MOTAHO. In the future, a novel optimization technique will be required to improve the performance of the WSN.

REFERENCES

[1] P. A. Patil, R. S. Deshpande, and P. B. Mane, "Trust and opportunity based routing framework in wireless sensor network using hybrid optimization algorithm," *Wireless Personal Communications*, vol. 115, no. 1, pp. 415–437, Nov. 2020, doi: 10.1007/s11277-020-07579-6.

[2] V. Gomathy, N. Padhy, D. Samanta, M. Sivaram, V. Jain, and I. S. Amiri, "Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 11, pp. 4995–5001, Nov. 2020, doi: 10.1007/s12652-020-01797-3.

[3] M. V. Babu, J. A. Alzubi, R. Sekaran, R. Patan, M. Ramachandran, and D. Gupta, "An improved IDAF-FIT clustering based ASLPP-RR routing with secure data aggregation in wireless sensor network," *Mobile Networks and Applications*, vol. 26, no. 3, pp. 1059–1067, Jun. 2021, doi: 10.1007/s11036-020-01664-7.

[4] N. Moussa and A. El Belrhiti El Alaoui, "An energy-efficient cluster-based routing protocol using unequal clustering and improved ACO techniques for WSNs," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1334–1347, May 2021, doi: 10.1007/s12083-020-01056-4.

[5] W. Fang, W. Zhang, W. Chen, J. Liu, Y. Ni, and Y. Yang, "MSCR: multidimensional secure clustered routing scheme in hierarchical wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, Dec. 2021, doi: 10.1186/s13638-020-01884-1.

[6] K. Selvakumar, L. Sairamesh, and A. Kannan, "An intelligent energy aware secured algorithm for routing in wireless sensor networks," *Wireless Personal Communications*, vol. 96, no. 3, pp. 4781–4798, Oct. 2017, doi: 10.1007/s11277-017-4417-7.

[7] V. Vijayalakshmi and A. Senthilkumar, "USCDRP: unequal secure cluster-based distributed routing protocol for wireless sensor networks," *The Journal of Supercomputing*, vol. 76, no. 2, pp. 989–1004, Feb. 2020, doi: 10.1007/s11227-019-03040-z.

[8] S. Prithi and S. Sumathi, "Automata based hybrid PSO–GWO algorithm for secured energy efficient optimal routing in wireless sensor network," *Wireless Personal Communications*, vol. 117, no. 2, pp. 545–559, Mar. 2021, doi: 10.1007/s11277-020-07882-2.

[9] K. Thangaramya, K. Kulothungan, S. I. Gandhi, M. Selvi, S. V. N. S. Kumar, and K. Arputharaj, "Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN," *Soft Computing*, vol. 24, no. 21, pp. 16483–16497, Nov. 2020, doi: 10.1007/s00500-020-04955-z.

[10] M. Revanesh, V. Sridhar, and J. M. Acken, "Secure coronas based zone clustering and routing model for distributed wireless sensor networks," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1829–1857, Jun. 2020, doi: 10.1007/s11277-020-07129-0.

[11] P. S. Khot and U. L. Naik, "Cellular automata-based optimised routing for secure data transmission in wireless sensor networks," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 34, no. 3, pp. 431–449, May 2022, doi: 10.1080/0952813X.2021.1882002.

[12] L. Tang, Z. Lu, and B. Fan, "Energy efficient and reliable routing algorithm for wireless sensors networks," *Applied Sciences*, vol. 10, no. 5, Mar. 2020, doi: 10.3390/app10051885.

[13] M. Pavani and P. T. Rao, "Adaptive PSO with optimised firefly algorithms for secure cluster-based routing in wireless sensor networks," *IET Wireless Sensor Systems*, vol. 9, no. 5, pp. 274–283, Oct. 2019, doi: 10.1049/iet-wss.2018.5227.

[14] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks," *Wireless Personal Communications*, vol. 110, no. 4, pp. 1637–1658, Feb. 2020, doi: 10.1007/s11277-019-06788-y.

[15] A. Saidi, K. Benahmed, and N. Seddiki, "Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks," *Ad Hoc Networks*, vol. 106, Sep. 2020, doi: 10.1016/j.adhoc.2020.102215.

[16] S. Gopinath, K. V. Kumar, P. Elayaraja, A. Parameswari, S. Balakrishnan, and M. Thiruppathi, "SCEER: Secure cluster based efficient energy routing scheme for wireless sensor networks," *Materials Today: Proceedings*, vol. 45, no. 2, pp. 3579–3584, 2021, doi: 10.1016/j.matpr.2020.12.1096.

[17] K. S. N. Prasad, G. R. Veerendra, and C. G. Puttamadappa, "Energy efficient data gathering scheme using cross layer cluster approach For wireless sensor networks," *International Journal on Computer Science and Engineering (IJCSE)*, vol. 3, no. 7, pp. 2661–2667, 2011.

[18] P. S. Khot and U. Naik, "Particle-water wave optimization for secure routing in wireless sensor network using cluster head selection," *Wireless Personal Communications*, vol. 119, no. 3, pp. 2405–2429, Aug. 2021, doi: 10.1007/s11277-021-08335-0.

[19] M. Hajiee, M. Fartash, and N. O. Eraghi, "An energy-aware trust and opportunity based routing algorithm in wireless sensor networks using multipath routes technique," *Neural Processing Letters*, vol. 53, no. 4, pp. 2829–2852, Aug. 2021, doi: 10.1007/s11063-021-10525-7.

[20] D. L. Reddy, C. G. Puttamadappa, and H. N. G. Suresh, "Hybrid optimization algorithm for security aware cluster head selection process to aid hierarchical routing in wireless sensor network," *IET Communications*, vol. 15, no. 12, pp. 1561–1575, Jul. 2021, doi: 10.1049/cmu2.12169.

[21] K. S. Kumar and P. Vimala, "Energy efficient routing protocol using exponentially-ant lion whale optimization algorithm in wireless sensor networks," *Computer Networks*, vol. 197, Oct. 2021, doi: 10.1016/j.comnet.2021.108250.

[22] S. Prithi and S. Sumathi, "LD2FA-PSO: A novel learning dynamic deterministic finite automata with PSO algorithm for secured energy efficient routing in wireless sensor network," *Ad Hoc Networks*, vol. 97, Art. no. 102024, Feb. 2020, doi: 10.1016/j.adhoc.2019.102024.

[23] G. R. Veerendra, K. S. N. Prasad, N. V Babu, and C. G. Puttamadappa, "Topology based performance analysis of IEEE 802.15.4 for wireless sensor networks," *International Journal of Computer Science and Network Security*, vol. 10, no. 8, pp. 175–181, 2010.

[24] Z. Sun, M. Wei, Z. Zhang, and G. Qu, "Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks," *Applied Soft Computing*, vol. 77, pp. 366–375, Apr. 2019, doi: 10.1016/j.asoc.2019.01.034.

[25] K. Veerabadrappa and S. C. Lingareddy, “Secure routing using multi-objective trust aware hybrid optimization for wireless sensor networks,” *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 1, pp. 540–548, Feb. 2022, doi: 10.22266/ijies2022.0228.49.

[26] X. Wang, “Low-energy secure routing protocol for WSNs based on multiobjective ant colony optimization algorithm,” *Journal of Sensors*, vol. 2021, pp. 1–9, Oct. 2021, doi: 10.1155/2021/7633054.

[27] G. R. Veerendra, K. S. N. Prasad, N. V Babu, and C. G. Puttamadappa, “Performance analysis of low rate and low power IEEE 802.15.4 standard for personal wireless area networks,” *International Journal of Computer Science and Network Security*, vol. 10, no. 11, pp. 233–238, 2010.

[28] S. A. Uymaz, G. Tezel, and E. Yel, “Artificial algae algorithm (AAA) for nonlinear global optimization,” *Applied Soft Computing*, vol. 31, pp. 153–171, Jun. 2015, doi: 10.1016/j.asoc.2015.03.003.

BIOGRAPHIES OF AUTHORS

Divyashree Habbanakuppe Balachandra has completed her Master of Technology (M. Tech) with specialization in Industrial Automation & Robotics from National institute of engineering, An Autonomous institute affiliated to VTU and Bachelor of Engineering in Electronics and communication from VTU. She is pursuing her Ph.D. in Dayananda Sagar University, Bangalore, Karnataka. She has 4 years of teaching experience and has published 6 research papers in National and International Conferences. Her research interests include networking, automation and robotics. She has one year of industry experience as Project trainee in L&T. Currently, she is working as Assistant Professor in Department of Electronics and communication at Dayananda Sagar university, Bangalore, Karnataka. She can be contacted at email: divyabalachandra94@gmail.com.

Puttamadappa Chaluve Gowda obtained Doctorate degree from Jadavpur University in the area of Devices in 2004, M.E. degree in Power Electronics from Bangalore University in 1997 and B.E Degree in Electronics and Communication Engineering from Mysore University in 1992. He has 24 years of teaching and administrative experience in various capacities like HOD, Principal and Director in reputed Institutes and Universities. He has participated, presented papers and chaired sessions at various conferences in India and abroad. He has published papers in peer reviewed National and International Journals, reputed National and International Conferences and coauthored a book published by CRC Press. Under his guidance several research Scholars are awarded Ph.D degree. He is a member of several professional bodies like IEEE, Indian Society for Technical Education (ISTE) and System Society of India (SSI). He was also a member of BOS, BOE, and Academic Council of various universities and autonomous bodies. He can be contacted at: puttamadappa@gmail.com.

Nandini Prasad Kanakapura Shivaprasad is affiliated to the Department of ISE, Dr. AIT, Bengaluru, since September 2002. She is currently working as Professor at dept. of ISE. She is also serving as Dean (Foreign Affairs) at Dr. AIT. She has completed her B.E (CSE) from PESIT, Bangalore; M.Tech (CSE) from VTU and Ph.D (ECE) from Kuvempu University. She has 19 years of teaching experience and has published 3 books for Elsevier publication and 3 books for Cengage Learning publication. She has also published 21 research papers in International Journal and 24 papers in International Conferences, in India and abroad. She has won best paper awards at various conferences and also received “Bharat Jyothi Award” in 2012 at New Delhi. She has received appreciation certificates from NPTEL as one of the STAR PERFORMER. She has served as reviewer for various journals and conferences. She has obtained diverse fundings from AICTE, India. She has to her credit of serving as BoS member at IET, Ayodhya, Uttar Pradesh. Dr. Nandini is also serving as Nodal Officer (Academic), TEQIP-III at Dr. AIT. She has to her credit of having filed 4 patents. She is presently guiding research scholars under VTU. She can be contacted at email: nandini.is@drait.edu.in.