Received: October 26, 2022. Revised: January 13, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Secure Cluster based Routing Using Multiobjective Trust Centric Reptile Search Algorithm for WSN

Seresane Venkata Krishna Reddy[1]* **Jayanthi Keshava Murthy[1]**

[1]*Department of Electronics and Communication Engineering, B.M.S College of Engineering, Bengaluru, India*
* Corresponding author's Email: Krishnareddy.dbit@gmail.com

Abstract: Wireless sensor networks (WSN) is self-organizing network that has numerous tiny sensor nodes used to track and monitor applications in an extensive range. However, security and energy consumption are considered two important issues, because of the open medium and restricted energy resources. In this paper, the multiobjective-trust centric reptile search algorithm (M-TCRSA) is proposed to perform the secure cluster based routing for WSN. The M-TCRSA is used to ensure the secure cluster head (SCH) and secure route discovery to achieve reliable communication over the WSN. Hence, the developed M-TCRSA method provides improved security against malicious attacks while enhancing energy efficiency. The main objective of the M-TCRSA is to achieve secure data transmission while increasing the life expectancy of the WSN. The performance of M-TCRSA is analyzed by means of packet delivery ratio (PDR), throughput, end to end delay (EED), jitter and life expectancy. The existing research such as trust-based routing using adaptive genetic algorithm (TAGA), trusted cluster based energy and lifetime aware routing (TCELR), secure clustering and routing using IMFO (SCRIMFO) and cost centric cuckoo search algorithm (CCCSA) are compared with the M-TCRSA. The PDR of the M-TCRSA is 99.27% for 400 nodes which is high when compared to the TAGA, TCELR, SCRIMFO and CCCSA.

Keywords: Cluster based routing, Energy consumption, Multiobjective-trust centric reptile search algorithm, Packet delivery ratio, Security, Wireless sensor network.

1. Introduction

Wireless sensor networks (WSN) have huge amounts of small autonomous devices dispersed through an area of interest where the collected data is broadcasted using wireless links [1, 2]. Generally, the sensors of the WSN have some key abilities such as sensing, computing, mobilizing, and data transmission [3]. Generally, the sensors are organized in a network formation that is mostly utilized for monitoring purposes. The sensors are utilized for observing the events and observed data is transmitted to the sink node and utilized for making decisions [4, 5]. WSNs are positioned in various application fields because of their less cost and ease of deployment features. The WSN applications are familiar in areas such as health care, smart buildings, railway monitoring, home security, military supervision, remote monitoring, and the agricultural field [6]. Sensors in the WSN depend on its onboard, restricted, irreplaceable and non-rechargeable batteries. Moreover, the sensors are restricted in memory, storage and CPU processing abilities [7, 8]. If the sensor's battery power is drained, the ongoing data broadcasting path is disturbed as well as path breaks and data losses are occurring in the network [9].

The important issue of the WSN is the limited energy of the sensors. The sensor receives the energy from the attached battery which is irreplaceable. The life expectancy of the sensor is denoted by the battery power; therefore, energy is required to be effectively utilized throughout the network [10]. An energy efficient approach namely clustering-based approach is used to solve the issue related to the battery lifetime [11]. The clustering of the sensors, cluster head (CH) selection and routing are used to minimize the amount of participating sensors in the route which helps to minimize energy consumption [12]. However, apart from maximizing life expectancy, numerous real-time and mission-critical application needs the guarantee of a quality of service (QoS). Similarly, security is also a serious problem in WSN, because the unreliable channels and unattended operation exposes the sensors vulnerable to malicious attacks [13]. To confirm the WSN's security, the trust based approaches have been confirmed to be highly robustness against malicious attacks [14, 15].

The contributions of this paper are as follows:

- The conventional reptile search algorithm (RSA) is modified into M-TCRSA to ensure secure communication in WSN. Here, the RSA is selected due to its effective equilibrium among exploitation and exploration processes.
- The trust-based approach M-TCRSA is used to perform the SCH selection which leads to improved security against malicious attacks and energy efficiency. Further, the secure route via the SCHs is discovered using the same M-TCRSA. Therefore, the M-TCRSA is used to minimize packet loss and unwanted energy consumption caused by malicious attacks.

The remaining paper is organized as follows: The related works about secure communication in WSN are provided in section 2. Section 3 delivers a detailed explanation of the M-TCRSA. The outcomes of the M-TCRSA method are provided in section 4 whereas the conclusion is presented in section 5.

2. Related work

Sajan [16] developed the three-level weighted trust evaluation-based grey wolf optimization (GWO) for effectively detecting the secure route over the trusted nodes. The clustering over the network was performed using the trust score and the CHs were chosen based on the weight computed using node distance, trust and energy. Next, the GWO was used to identify the optimal secure route that was used to broadcast the data from the source to the destination. The developed GWO-based routing was used to minimize the packet loss, however, the selection of CH mainly depends on the node distance, trust and energy.

Han [17] implemented the TAGA for creating robustness against attacks used to choose secure and energy-aware routes. The developed TAGA mainly uses trust value and energy to ensure the SCH selection and secure path discovery. Therefore, the TAGA selected the path with small energy and high security. However, this TAGA doesn't consider the distance while broadcasting the data.

Khot and Naik [18] presented the particle-based spider monkey optimization (P-SMO) to ensure secure communication through WSN. The P-SMO was the combination of particle swarm optimization (PSO) and spider monkey optimization. The learning automata-based cell clustering was used to select the CH followed by the P-SMO was used to discover the secure route. The developed P-SMO based secure routing was used to obtain better energy balancing in WSN, though this P-SMO was analyzed with only less number of nodes.

Thahniyath and Jayaprasad [19] developed secure and load balanced routing (SLBR) for cluster based WSN. The low latency energy efficient clustered based multipath (LLEECMP) routing was used by SLBR for choosing the CHs. The developed LLEECMP has broadcasted the data packets over the shortest path that is used to minimize the latency. This LLEECMP mainly depends on the trust values while selecting the CH and route.

Vasanthi and Prabakaran [20] implemented the hybrid swarm swarm-differential search to develop the trusted cluster based energy and lifetime aware routing (TCELR) for WSN. The enhanced leader PSO used in TCELR to cluster the nodes followed by flower pollination is used for measuring the trust values. The node with a higher trust degree was considered CH. Next, the inter-cluster routing was ensured using the group search optimizer with multiple producers. This TCELR doesn't consider some other important fitness metrics such as energy and distance while selecting CHs.

Ramachandra and Surekha [21] presented the secure clustering and routing using IMFO (SCRIMFO) for WSN. Shivakumaraswamy and Mala [22] developed cost centric cuckoo search algorithm (CCCSA) for the WSN. The fitness parameters of trust, distance, node degree and residual energy considered for both the SCRIMFO and CCCSA. These approaches were used to mitigate the malicious nodes for enhancing the data delivery. However, the balancing among the clusters of the network was not considered in SCRIMFO and CCCSA.

Sunitha [23] presented the clustering and routing using congestion centric multi-objective reptile search algorithm (CC-MORSA) for cognitive radio sensor networks (CRSNs). The developed CC-MORSA was mainly considered lifetime improvisation as primary objective by minimizing the transmission distance. However, the developed CC-MORSA was failed to consider the security issues in the network. Since, the CRSNs were

Received: October 26, 2022. Revised: January 13, 2023.

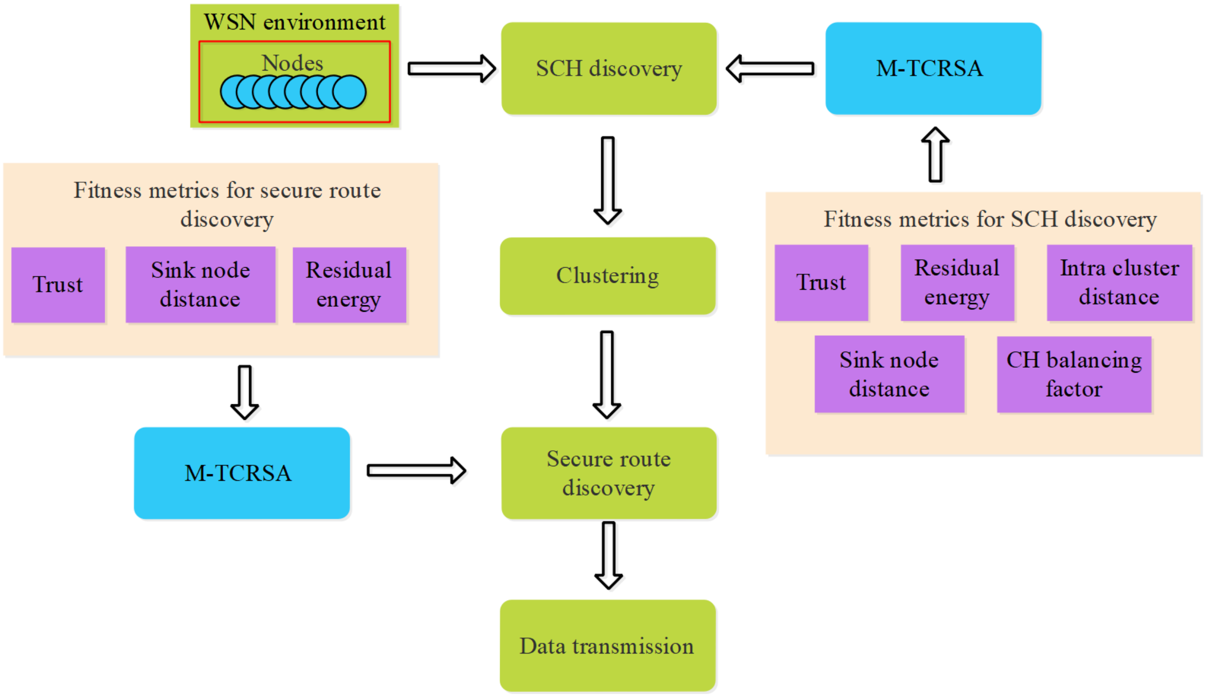

Figure. 1 Block diagram of the M-TCRSA method

operated in open wireless medium, the devices of CRSNs were vulnerable to the malicious attacks.

3. M-TCRSA method

In this research, secure and reliable communication is ensured by using the M-TCRSA method. The M-TCRSA method mainly comprises four phases such as sensor deployment, SCH discovery, cluster formation and route discovery. The SCH and secure route discovery are used to avoid malicious attacks while broadcasting the data packets. Therefore, the unwanted packet drop and energy consumption are minimized by using the M-TCRSA method. The block diagram of the M-TCRSA method is shown in Fig. 1.

3.1 Sensor deployment

Initially, the nodes are randomly positioned in the WSN followed by an optimal SCH and secure paths are discovered by using M-TCRSA that helps to achieve secure reliable data broadcasting in the network.

3.2 SCH discovery using M-TCRSA

The optimal SCHs from the normal nodes are identified using the M-TCRSA with distinct fitness metrics. The conventional RSA is one of the meta-heuristic methods which replicates the crocodile's encircling and hunting activities. RSA is understood by its exploration and exploitation principles that are same as the remaining meta-heuristic method. The M-TCRSA based SCH discovery is explained in the following section,

3.2.1. Representation and initialization

The group of nodes is considered candidate SCHs at the time of solution initialization where the dimension of each solution is equal to the number of SCHs. In this phase, each solution is set with the random sensor ID between 1 and N, where the total sensors initialized in the WSN are denoted as N. Let, the ith solution of the M-TCRSA is denoted as $y_i = (y_{i,1}, y_{i,2}, \dots, y_{i,D})$, where the dimension of the solution is denoted as D. The location of the solution is $y_{i,rs}, 1 \le rs \le D$ which represents the random sensor among the total sensors.

3.2.2. Iterative process of M-TCRSA

The principles of exploration and exploitation are accomplished by crocodile motion during the encircling of the target prey. There are two motions such as high walking and belly walking are done according to the encircling behavior at the exploration phase (i.e., encircling). The location update of M-TCRSA is shown in Eq. (1). The high walking is initialized, when the current iteration (t) is lesser than the $T/4$, where the maximum iteration count is denoted as T; Else, the belly walking is initialized as shown in Eq. (1).

$$y_{(i,j)}(t+1) = \begin{cases} B_j\ (t) \times -\rho_{(i,j)}(t) \times \mu - RF_{(i,j)}(t) \times r, & t \le \frac{T}{4} \\ B_j\ (t) \times y_{(r_1,j)} \times ES(t) \times r & t \le 2\frac{T}{4}\ and\ \ t > \frac{T}{4} \end{cases} \tag{1}$$

Where, the jth position of ith solution is denoted as $y_{(i,j)}$; t defines the current iteration; $B_j\ (t)$ denotes best solution obtained from entire population; r is the random value generated in the range of $[0,1]$; $\rho_{(i,j)}(t)$ defines the hunting parameter which is shown in Eq. (2); the value of μ is fixed as 0.1; the reduce function shown in Eq. (3) defines the $RF_{(i,j)}$; the random numbers are $r_1 - r_4$ and random location is $y_{(r_1,j)}$. Eq. (4) defines the Evolutionary Sense $(ES(t))$.

$$\rho_{(i,j)} = B_j\ (t) \times P_{(i,j)} \tag{2}$$

$$RF_{(i,j)} = \frac{B_j\ (t) - y_{(r_2,j)}}{B_j\ (t) + \epsilon} \tag{3}$$

$$ES(t) = 2 \times r_3 \times \left(1 - \frac{1}{T}\right) \tag{4}$$

Where, the ϵ is a small value and the difference value $P_{(i,j)}$ is shown in Eq. (5).

$$P_{(i,j)} = \alpha + \frac{y_{(i,j)} - M(y_i)}{B_j(t) + (UB_j - LB_j) + \epsilon\prime} \tag{5}$$

Where, the $M(y_i)$ represents the average positions that are shown in Eq. (6). LB_j and UB_j denotes the lower and upper limits of the M-TCRSA and the α is fixed as 0.1.

$$M(y_i) = \frac{1}{D}\sum_{j=1}^{D} y_{(i,j)} \tag{6}$$

Additionally, the exploitation (i.e., hunting) is performed where it employs two methods such as hunting coordination and hunting collaboration. If the condition of $t \le 3\frac{T}{4}$ and $t > 2\frac{T}{4}$ are satisfied, the M-TCRSA is processed with hunting coordination; Else, the hunting cooperation is performed as shown in Eq. (7).

$$y_{(i,j)}(t+1) = \begin{cases} B_j\ (t) \times P_{(i,j)}(t) \times r, & t \le 3\frac{T}{4}\ and\ t > 2\frac{T}{4} \\ B_j\ (t) - \rho_{(i,j)}(t) \times \epsilon - RF_{(i,j)}(t) \times r, & t \le T\ and\ \ t > 3\frac{T}{4} \end{cases} \tag{7}$$

The fitness metrics are employed to discover the SCHs from the network which is derived in the subsequent section.

3.2.3. Derivation of fitness metrics for SCH discovery

The fitness metrics used to discover the SCH using M-TCRSA are trust (fm_1), residual energy (fm_2), intra-cluster distance (fm_3), sink node distance (fm_4) and CH balancing factor (fm_5). Eq. (8) shows the fitness metrics which are converted into a single objective value (Fit).

$$Fit = \delta_1 \times fm_1 + \delta_2 \times fm_2 + \delta_3 \times fm_3 + \delta_4 \times fm_4 + \delta_5 \times fm_5 \tag{8}$$

Where, the Fit denotes the overall fitness metric; $\delta_1 - \delta_5$ denotes the weight metric assigned to each fitness metrics. The definition of fitness metrics used in this M-TCRSA are given as follows:

- The key fitness metric used in this M-TCRSA is the node's trust value which includes two different trust values such as direct and indirect trust. The direct trust value (DTV) is the proportion between the collected packets and transmitted packets by the source node that is shown in Eq. (9). On the contrary, the indirect trust value (ITV) is computed based on the DTV evaluated from the target node that is shown in Eq. (10). Therefore, the computation of the final trust of each node is expressed in Eq. (9).

$$DTV = \frac{Col_{a,b}(t)}{Sen_{a,b}(t)} \tag{6}$$

$$IDT = \frac{1}{AN}\sum_{u=1}^{AN} DT_{u,b} \tag{7}$$

$$fm_1 = \sum_{i=1}^{PN} (DT + IDT)/PN \tag{8}$$

Where the number of sent and collected packets among sensor a and b at time t is denoted as $Sen_{a,b}(t)$ and $Col_{a,b}(t)$; the number of adjacent nodes is denoted as AN and total amount of participated nodes are defined as PN.

- The SCH is required to receive, aggregate and broadcast the data to the BS. Consequently, the sensor with higher energy is preferred as the next hop SCH and this energy computation is expressed in the following Eq. (9).

$$fm_2 = \sum_{i=1}^{D} \frac{1}{E_{SCH_i}} \tag{9}$$

Received: October 26, 2022. Revised: January 13, 2023.

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

- The M-TCRSA considered two distance functions such as intra cluster distance and sink node distance which are expressed in Eqs. (10) and (11) respectively. The sensors in the WSN consume energy while broadcasting the data from transmitter SCH and BS. The energy consumption of sensor is directly proportional to the transmission distance. Therefore, it is required to the relay SCH which has a lesser distance from the CMs and BS.

$$fm_3 = \sum_{j=1}^{D} \left(\sum_{i=1}^{I_j} dis(N_i, SCH_j) / I_j \right) \qquad (10)$$

$$fm_4 = \sum_{i=1}^{D} dis(SCH_i, BS) \qquad (11)$$

Where, the distance between the jth SCH and ith node is denoted as $dis(N_i, SCH_j)$ and distance between i th SCH and BS is denoted as $dis(SCH_i, BS)$. The amount of cluster members belonging to the jth cluster is denoted as I_j.

- In WSN, there is a possibility that some huge clusters are formed with a few small clusters. Consequently, the CH balancing factor shown in Eq. (12) is taken for balancing the cluster used to obtain the energy balancing in WSN.

$$fm_5 = \sum_{i=1}^{D} \frac{A}{D} - I_j \qquad (12)$$

Where, the total number of alive nodes is denoted as A.

The trust measure considered in the SCH discovery avoids the attacker nodes which helps to minimize the packet drop and unwanted energy consumption. The failure of a node is avoided by using the residual energy whereas the transmission distance is minimized by using intra-cluster and sink node distances. Further, the balancing among the clusters is also used to improve energy efficiency while enhancing network security against malicious attackers.

3.3 Generation of clusters

In cluster generation process, the normal sensors are allocated to the SCHs. The distance and residual energy considered in the potential function are shown in Eq. (13) which is used to assign the normal sensors to desired SCHs.

$$Potential\ function\ (N_i) = \frac{E_{SCH}}{dis(N_i, SCH)} \qquad (13)$$

3.4 Route discovery using M-TCRSA

The M-TCRSA method was also used to perform the route discovery. The steps processed in the route discovery are given as follows:

1. The possible paths from the transmitter SCH to BS are considered as initial solutions for route discovery. The dimension of each solution is equal to the amount of relay SCHs exist in the route.
2. Additionally, the fitness metric computed using trust, energy and distance shows in Eq. (14) which is used to update the location of the solution. The location update of route discovery is done based on the iterative process of M-TCRSA.

$$Routing\ fitness = \tau_1 \times \sum_{i=1}^{PN} \frac{(DT+IDT)}{PN} + \tau_2 \times \sum_{i=1}^{n} dis(CH_i, BS) + \tau_3 \times \sum_{i=1}^{n} \frac{1}{E_{CH_i}} \qquad (14)$$

Where, τ_1, τ_2 and τ_3 are the weight parameters assigned to the fitness metrics of the routing process. Hence, the optimal secure route is selected for improving the security of the WSN while improving the data delivery.

4. Results and discussion

This section carried out the performance evaluation of the implemented M-TCRSA method. The MATLAB R2018a is used to implement and simulate the M-TCRSA based secure clustering and routing for WSN. Here, the system is operated with 6GB of RAM and an i5 processor. The evaluation of the M-TCRSA method is done by varying the number of nodes in the testing scenarios. Here, the SCH and secure route discovery are done using M-TCRSA to achieve secure communication. The simulation parameters of the M-TCRSA method are given in Table 1.

The performance of the M-TCRSA method is analyzed using packet delivery ratio (PDR), throughput, end to end delay (EED), jitter and life

Table 1. Simulation parameters

Parameters	Values
Cluster based routing method	M-TCRSA
Area	$1000m \times 1000m$
Number of nodes	400, 600, 800, 1000 and 2000
Packet size	512 bytes

Received: October 26, 2022. Revised: January 13, 2023.

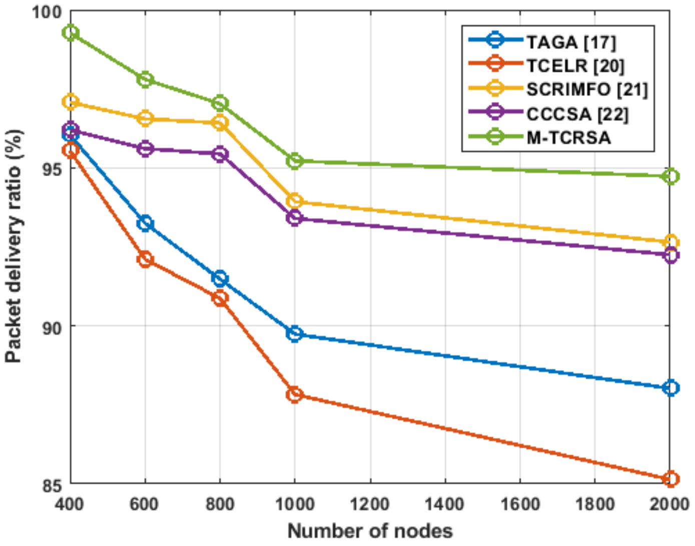

Figure. 2 PDR Vs. nodes

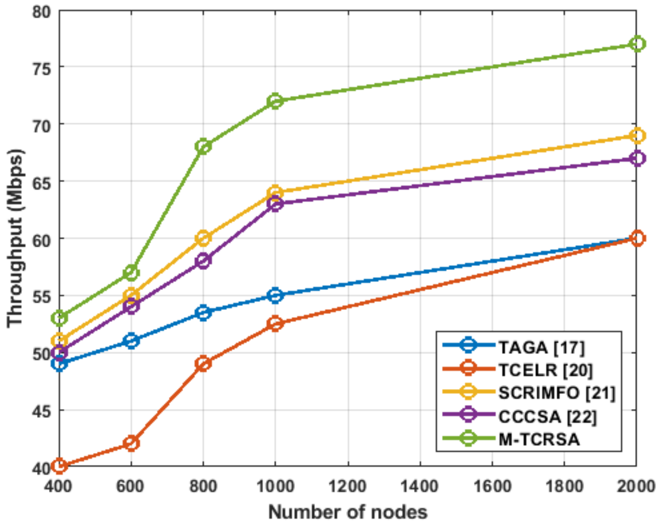

Figure. 3 Throughput Vs. nodes

expectancy. The existing methods such as TAGA [17], TCELR [20], SCRIMFO [21] and CCCSA [22] are used to evaluate the performance of M-TCRSA method where these existing methods are developed for the same specifications mentioned in Table 1.

4.1 Packet delivery ratio

PDR is defined as the ratio between the amount of packets received by BS and amount of packets broadcasted by the transmitter node. Fig. 2 shows the PDR comparison of M-TCRSA with TAGA [17], TCELR [20], SCRIMFO [21] and CCCSA [22]. This PDR analysis shows that the M-TCRSA achieves higher PDR than the TAGA [17], TCELR [20], SCRIMFO [21] and CCCSA [22]. For example, the existing TAGA [17] and TCELR [20] methods mainly considered trust as the primary fitness metric, but it failed to concentrate on the energy and distance which leads to packet drop over the network. However, the M-TCRSA method considered the residual energy which helps to mitigate the node failure, as well as the unwanted packet drop, is minimized by avoiding the malicious attacks. Therefore, the data delivery of the M-TCRSA is increased in the WSN.

4.2 Throughput

Throughput is defined as the number of data packets successfully received at the destination (BS), since the throughput is analyzed as bits per second. The comparison of throughput for TAGA [17], TCELR [20], SCRIMFO [21] CCCSA [22] and M-TCRSA is shown in Fig. 3. From Fig. 3, it is concluded that the M-TCRSA achieves higher

Received: October 26, 2022. Revised: January 13, 2023.

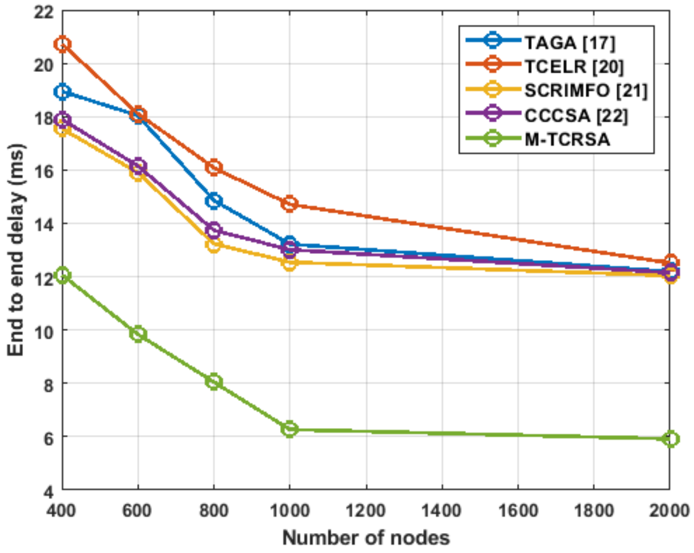

Figure. 4 EED Vs. nodes

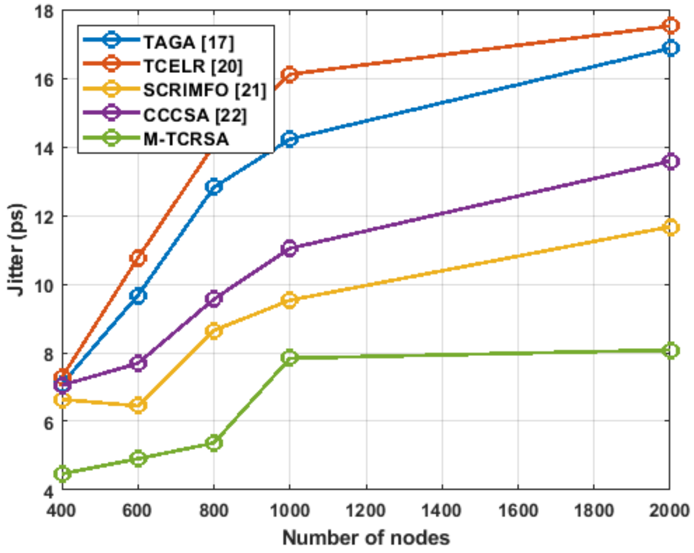

Figure. 5 Jitter Vs. nodes

throughput than the TAGA [17], TCELR [20], SCRIMFO [21] and CCCSA [22]. The higher throughput is achieved in M-TCRSA because of avoiding malicious attacks and node failure using trust and energy fitness metrics.

4.3 End to end delay and jitter

EED is defined as the amount of time taken to transmit the data packets from the source to the BS whereas jitter is the variance in packet delay. Figs. 4 and 5 show the EED and jitter comparison of M-TCRSA with TAGA [17], TCELR [20], SCRIMFO [21] and CCCSA [22]. From the figures, it is known that the M-TCRSA has lesser EED and jitter than the TAGA [17], TCELR [20], SCRIMFO [21] and CCCSA [22]. The M-TCRSA achieves lesser EED and jitter because of the shortest path generation and less control packet utilization during route discovery. But, some existing methods such as TAGA [17] and TCELR [20] use a high amount of control packets during route discovery that leads to an increase the EED and jitter.

4.4 Life expectancy

Life expectancy is defined as the period of time when the first sensor drains its whole energy during communication. The comparison of life expectancy for TAGA [17], TCELR [20], SCRIMFO [21], CCCSA [22] and M-TCRSA is shown in Fig. 6. From Fig. 6, it is concluded that the M-TCRSA achieves higher life expectancy than the TAGA [17], TCELR [20], SCRIMFO [21] and CCCSA [22]. The

Received: October 26, 2022. Revised: January 13, 2023.

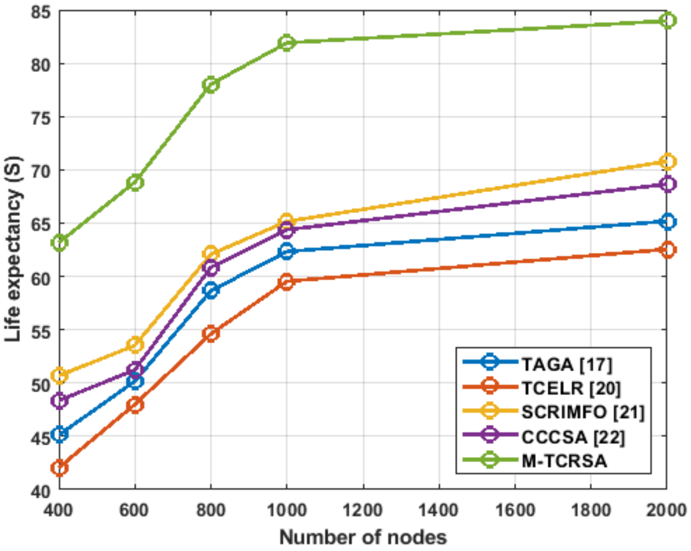

Figure. 6 Life expectancy Vs. nodes

Table 2. Comparative analysis of M-TCRSA method

Performances Metrics	Methods	Number of nodes				
		400	600	800	1000	2000
PDR (%)	TAGA [17]	96.04	93.25	91.48	89.74	88.02
	TCELR [20]	95.54	92.11	90.87	87.83	85.14
	SCRIMFO [21]	97.07	96.55	96.42	93.93	92.65
	CCCSA [22]	96.20	95.61	95.44	93.40	92.25
	M-TCRSA	99.27	97.80	97.03	95.22	94.73
Throughput (Mbps)	TAGA [17]	49	51	53.5	55	60
	TCELR [20]	40	42	49	52.5	60
	SCRIMFO [21]	51	55	60	64	69
	CCCSA [22]	50	54	58	63	67
	M-TCRSA	53	57	68	72	77
EED (ms)	TAGA [17]	18.95	18.04	14.86	13.22	12.19
	TCELR [20]	20.73	18.11	16.08	14.71	12.51
	SCRIMFO [21]	17.55	15.90	13.23	12.54	12.04
	CCCSA [22]	17.90	16.15	13.74	13.01	12.15
	M-TCRSA	12.07	9.84	8.05	6.27	5.92
Jitter (ps)	TAGA [17]	7.08	9.67	12.82	14.22	16.87
	TCELR [20]	7.28	10.76	14.05	16.11	17.52
	SCRIMFO [21]	6.64	6.45	8.65	9.53	11.67
	CCCSA [22]	7.05	7.69	9.56	11.04	13.58
	M-TCRSA	4.47	4.91	5.37	7.84	8.08
Life expectancy (S)	TAGA [17]	45.12	50.17	58.66	62.33	65.18
	TCELR [20]	42.07	48.00	54.61	59.54	62.55
	SCRIMFO [21]	50.69	53.53	62.08	65.16	70.79
	CCCSA [22]	48.35	51.24	60.86	64.38	68.66
	M-TCRSA	63.17	68.84	78.03	81.91	83.97

unwanted energy consumption caused by malicious attacks is avoided by M-TCRSA. Moreover, the energy efficiency of the M-TCRSA is enhanced by using the distance, CH balancing factor which helps to achieve the shortest path generation and effective load balancing through the network. Therefore, the M-TCRSA with lesser energy consumption of sensors helps to improve the life expectancy.

Table 2 shows the comparative analysis of the M-TCRSA with TAGA [17], TCELR [20], SCRIMFO [21] and CCCSA [22]. From this analysis, it is known that the M-TCRSA achieves better performance than the TAGA [17], TCELR [20], SCRIMFO [21] and CCCSA [22]. The proposed M-TCRSA is used to increase the robustness against the malicious attacks used to enhance the data delivery and life expectancy of WSN. Further, the balancing among the clusters developed in M-TCRSA is further used to enhance the energy efficiency of the network.

5. Conclusion

In this paper, the secure cluster based routing is developed using M-TCRSA for improving the security against malicious attacks. The SCH from the normal sensors and route via SCHs are selected using M-TCRSA which avoids malicious attacks during communication. Additionally, the clustering using M-TCRSA helps to improve the energy efficiency of the WSN. The developed trust based M-TCRSA is used to perform secure and reliable communication while improving the life expectancy of WSN. Moreover, the shortest path obtained from the M-TCRSA is used to minimize the delay over the network. Therefore, the data delivery of the M-TCRSA is improved in the WSN. From the results, it is known that the M-TCRSA outperforms well than the TAGA, TCELR, SCRIMFO and CCCSA. The PDR of the M-TCRSA is 99.27% for 400 nodes which is high when compared to the TAGA, TCELR, SCRIMFO and CCCSA. In the future, the novel optimization algorithm can be used for improving the WSN performances.

Nomenclature

Parameter	Description
N	Total sensors initialized in the WSN
y_i	ith solution of the M-TCRSA
D	Dimension of the solution
rs	Random sensor among the total sensors
T	Maximum iteration count
t	Current iteration
$y_{(i,j)}$	jth position of ith solution
$B_j\ (t)$	Best solution
r	Random value generated in the range of [0,1]
$\rho_{(i,j)}(t)$	Hunting parameter
$RF_{(i,j)}$	reduce function
$r_1 - r_4$	random numbers
$ES(t)$	Evolutionary Sense
$P_{(i,j)}$	Difference value
$M(y_i)$	Average positions
LB_j and UB_j	Lower and upper limits of the M-TCRSA
$\delta_1, \delta_2, \delta_3, \delta_4$ and δ_5	Weight values
fm_1	Trust
fm_2	Residual energy
fm_3	Intra-cluster distance
fm_4	Sink node distance
fm_5	CH balancing factor
Fit	Overall fitness metric
DTV	Direct trust value
ITV	Indirect trust value
$Col_{a,b}$	Number of sent packets among sensor a and b
$Sen_{a,b}$	Number of collected packets among sensor a and b
AN	Number of adjacent nodes
PN	Total amount of participated nodes
E_{SCH_i}	Remaining energy of the ith SCH
$dis(N_i, SCH_j)$	Distance between the jth SCH and ith node
$dis(SCH_i, BS)$	Distance between ith SCH and BS
I_j	Amount of cluster members belonging to the jth cluster
A	Total number of alive nodes
τ_1, τ_2 and τ_3	Weight parameters assigned to the fitness metrics of the routing process

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] L. Kanouni and F. Semchedine, “A new paradigm for multi-path routing protocol for data delivery in wireless sensor networks”, *International Journal of Computers and Applications*, Vol. 44, No. 10, pp. 939-952, 2021.

[2] 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, 2021.

[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, 2021.

[4] R. Kocherla, M. C. Sekhar, and R. Vatambeti,

"Enhancing the energy efficiency for prolonging the network life time in multi-conditional multi-sensor based wireless sensor network", *Journal of Control and Decision*, Vol. 31, pp. 1-10, 2022.

[5] H. Hu, Y. Han, M. Yao, and X. Song, "Trust based secure and energy efficient routing protocol for wireless sensor networks", *IEEE Access*, Vol. 10, pp. 10585-10596, 2021.

[6] S.R. Lahane and K. N. Jariwala, "Secured cross-layer cross-domain routing in dense wireless sensor network: A new hybrid based clustering approach", *International Journal of Intelligent Systems*, Vol. 36, No. 8, pp. 3789-3812, 2021.

[7] N. Mittal, S. Singh, U. Singh, and R. Salgotra, "Trust-aware energy-efficient stable clustering approach using fuzzy type-2 Cuckoo search optimization algorithm for wireless sensor networks", *Wireless Networks*, Vol. 27, No. 1, pp. 151-174, 2021.

[8] A. R. Basha, "Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network", *IET Wireless Sensor Systems*, Vol. 10, No. 4, pp. 166-174, 2020.

[9] R. Shukla, A. Kumar, and V. Niranjan, "An efficient elite group-based routing protocol for wireless sensor network", *International Journal of Electronics*, Vol. 107, No. 7, pp. 1031-1043, 2020.

[10] 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, 2021.

[11] M. A. Angel, and T. Jaya, "An Enhanced Emperor Penguin Optimization Algorithm for Secure Energy Efficient Load Balancing in Wireless Sensor Networks", *Wireless Personal Communications*, Vol. 125, pp. 2101-2127, 2022.

[12] M. Hajiee, M. Fartash, and N. Osati 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, 2021.

[13] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy, and R. Patan, "Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks", *IEEE Transactions on Engineering Management*, Vol. 68, No. 1, pp. 170-182, 2019.

[14] H. Hu, Y. Han, H. Wang, M. Yao, and C. Wang, "Trust-aware secure routing protocol for wireless sensor networks", *ETRI Journal*, Vol. 43, No. 4, pp. 674-683, 2021.

[15] 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, p. 108250, 2021.

[16] R. I. Sajan, V. B. Christopher, M. J. Kavitha, and T. S. Akhila, "An energy aware secure three-level weighted trust evaluation and grey wolf optimization based routing in wireless ad hoc sensor network", *Wireless Networks*, Vol. 28, No. 4, pp. 1439-1455, 2022.

[17] Y. Han, H. Hu, and Y. Guo, "Energy-Aware and Trust-Based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm", *IEEE Access*, Vol. 10, pp. 11538-11550, 2022.

[18] 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. 431-49, 2022.

[19] 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, 2020

[20] G. Vasanthi and N. Prabakaran, "Reliable network lifetime and energy-aware routing protocol for wireless sensor network using hybrid particle swarm-flower pollination search algorithm", *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-11, 2022.

[21] B. Ramachandra and T. P. Surekha, "Secure Cluster based Routing Using Improved Moth Flame Optimization for Wireless Sensor Networks", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 4, pp. 116-124, 2022, doi: 10.22266/ijies2022.0831.12.

[22] S. M. Shivakumaraswamy and C. S. Mala, "Security and Energy Aware Adaptive Routing using Cost Centric Cuckoo Search Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 14, No. 6, pp. 596-604, 2021, doi: 10.22266/ijies2021.1231.53.

[23] D. Sunitha, K. R. Balmuri, R. P. D. Prado, P. B. Divakarachari, R. Vijayarangan, and K. L. Hemalatha, "Congestion centric mult-objective reptile search algorithm-based clustering and routing in cognitive radio sensor network", *Transactions on Emerging Telecommunications Technologies*, p. e4629, 2022.