Secure and Energy Aware Cluster based Routing using Trust Centric – Multiobjective Black Widow Optimization for large scale WSN

Original Scientific Paper

Sampath Reddy Chada
Sree Chaitanya Institute of Technological Sciences,
Department of Computer Science and Engineering,
Karimnagar, Telangana, India
Sampath553@gmail.com

Narsimha Gugulothu
JNTUH College of Engineering,
Department of Computer Science and Engineering, Sultanpur, Telangana, India
Narsimha06@jntuh.ac.in

Abstract *– Wireless Sensor Network (WSN) is a promising approach that is developed for a wide range of applications due to its low installation cost. However, the nodes in the WSN are susceptible to different security threats, because these nodes are located in hostile or harsh environments. Moreover, an inappropriate selection of routing path affects the data delivery of the WSN. The important goal of this paper is to obtain secure data transmission while minimizing energy consumption. In this paper, Trust Centric - Multiobjective Black Widow Optimization (TC-MBWO) is proposed for selection of Secure Cluster Head (SCH) from the large-scale WSN. Moreover, the secure routing path is generated by using the TC-MBWO, in which the factors considered for the cost function are: residual energy, distance, trust and node degree. Therefore, the secured clustering and routing achieved by using TC-MBWO, provides the resistance against malicious nodes and simultaneously the energy consumption is also minimized by identifying the shortest path. The proposed TC-MBWO method is analyzed in terms of alive nodes, dead nodes, energy consumption, throughput, and network lifetime. Here, the TC-MBWO method is compared with different existing methods such as Low Energy Adaptive Clustering Hierarchy (LEACH), Particle Swarm Optimization - Grey Wolf Optimizer (PSO-GWO), Particle-Water Wave Optimization (P-WWO) and Particle-based Spider Monkey Optimization (P-SMO). The alive nodes of the TC-MBWO are 70 for 2800 rounds which are higher in number when compared to the PSO-GWO, P-WWO and P-SMO.*

Keywords*: Cluster head, Energy Consumption, Secure Clustering and Routing process, Trust Centric- Multiobjective Black Widow Optimization, Wireless Sensor Networks.*

1. INTRODUCTION

WSN contains a huge amount of sensors for observing environmental situations such as sound, humidity, temperature, etc. [1]. WSNs are used in various applications comprising security systems, disaster management, agricultural areas, medical domains, weather forecasting and military applications wherein, the WSN gathers data to perform an appropriate analysis [2] [3]. The sensors in the network have a power supply, communication unit, and microcontroller. The sensor unit analyzes the environment, gathers the data, processes it and then transfers the processed information to other sensors over the communication medium. But, the sensor faces certain issues related to memory, computation and energy [4]. Security is considered as an important issue when broadcasting sensitive information in WSN. Broadcasting the information through the multi-hop route with a higher distance, leads to intrusion of different malicious attacks [5] [6] [7]. Moreover, energy preservation is also a main issue in the WSN. The major prevalent approach i.e., clustering of sensor nodes is accomplished for solving the issue of energy consumption [8] [9] [10].

The clustered routing protocol efficiently deals with the requirements of large-scale applications for hierarchical WSN. But the selection of SCH and secure routing is difficult during the clustering and routing phase respectively [11] [12]. Clustering is generally an energy efficient approach wherein the sensors are divided into numerous clusters. Accordingly, the Cluster Members

(CM) observe the surroundings and broadcast the information to the Cluster Head (CH). Next, the CH eliminates the unwanted data from the aggregated data. Since, the CH is closer to the BS, it rapidly exhausts its energy over the network [13]. An optimal path is identified by the routing algorithm and is used to broadcast the observed data over the discovered path which helps to increase lifetime and minimize energy consumption [14]. Moreover, the issue of energy consumption also persists when the sensors are involved in malicious behaviors. Hence, the node's energy is preserved by avoiding the malicious nodes [15]. Therefore the main issues of WSN are energy efficiency and security. Because, the existence of malicious nodes in the network causes packet drop and unwanted energy consumption. These issues of WSN are the main motivations of this research, therefore the TC-MBWO based secure clustering and routing are developed to ensure the reliable communication.

The major contributions of the research paper are given below:

- An SCH and routing path selection is achieved by using the TC-MBWO with distinct cost parameters. Here, the MBWO is taken for selecting the SCH and routes, due to its efficient global search process.
- Therefore, a secure and energy aware routing is developed for achieving reliable communication. This kind of communication minimizes energy consumption while improving the throughput.

This research paper is arranged as follows: Section 2 provides the related work about the secure data transmission performed in the WSN. A detailed explanation of the TC-MBWO is given in Section 3. Section 4 delivers the outcomes of the TC-MBWO method. The conclusion is made in Section 5.

2. RELATED WORK

Hu et al. [16] provided security against the attacks by developing a Trust-aware Secure Routing Protocol (TSRP). Here, the node's trust value was calculated using the residual energy, volatilization factor, direct trust value and indirect trust value. Next, the hop count and link quality were used to identify the optimal path. However, the developed TSRP failed to perform analysis in large scale WSNs.

Shi et al. [17] implemented the information-aware secure routing for a network wherein cost functions such as trust metric and each node's status, were considered during the secure route identification. The distance and residual energy were included in the node's status. The node's energy consumption was minimized by detecting the path with a lesser distance. Sometimes, the packet loss was huge because of the energy exhaustion in the sensor.

Sefati et al. [18] presented the optimized black hole algorithm to detect appropriate CHs and Ant Colony Optimization (ACO) for route detection. The parameters used to optimize the selection of CH were distance, node's free buffer and residual energy. This work considered both the single and multi-hop data transmission to transmit the data, but it had not considered the trust values to improve the security.

Prithi and Sumathi, [19] developed a hybrid PSO-GWO for effective usage of energy and secure broadcast of data. The environment's dynamic role was learned by developing the Learning Dynamic Deterministic Finite Automata (LD2FA) which was used for providing the learned data to PSO-GWO. This work failed to properly utilize the advantages of the fitness function used in PSO-GWO, which is an important requirement alongside optimization, in an effective research.

Kumar and Vimala [20] developed energy and trust based routing by using Exponentially-Ant Lion Whale Optimization (E-ALWO). This E-ALWO was the combination of the exponentially weighted moving average with ant lion and whale optimizations. The designed E-ALWO provided less delay while transmitting the data packets. The E-ALWO selected the CH only based on the energy and delay.

Khot and Naik, [21] presented the P-WWO for routing the data in the optimal secure path. The P-WWO was the integration of Particle Swam Optimization (PSO) and water wave optimization. Here, the PSO selected the CHs according to their fitness which included maintainability factor, consistency factor, trust, energy and delay. Moreover, the routing path with less delay and distance was chosen as an optimal path. However, the distance measure was not considered in the selection of CH which caused higher energy consumption.

Khot and Naik [22] developed the P-SMO which is the combination of PSO and spider monkey optimization. The developed P-SMO was used to perform the secure data transmission through the CH whereas the secure routing was accomplished by considering trust, consistency factor, energy and delay. However, the packets received by the BS were not analyzed in this P-SMO.

The drawbacks found from the related works are mentioned as follows: high amount of packet loss due to node failure, higher energy consumption and inappropriate cost function selection. To overcome the aforementioned issues, the secure and energy aware routing is developed by using the TC-MBWO. In this TC-MBWO, the malicious nodes are avoided while broadcasting the data packets, which results in lesser energy consumption and reduced packet drop.

3. TC-MBWO METHOD

In this TC-MBWO, a secure and energy aware cluster based routing is developed to improve the network lifetime and packet delivery. The important processes ac-

complished in the TC-MBWO are sensor deployment, SCH selection, clustering and routing path generation. Here, the malicious nodes that exist in the network are avoided during SCH selection and routing, by considering the trust value of the nodes. Accordingly, the energy consumption of the nodes are minimized in the network. The block diagram for the TC-MBWO is shown in Figure 1.

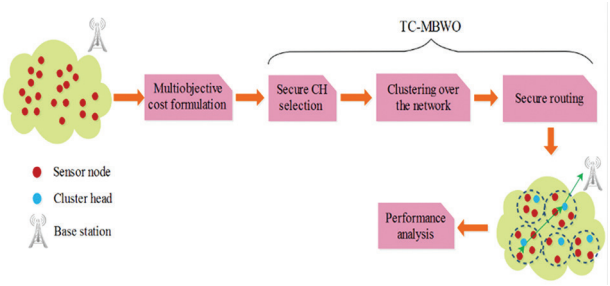

Fig. 1. Block diagram of the TC-MBWO method

3.1 INITIALIZATION OF SENSORS

At first, the sensor nodes are randomly deployed in the large-scale network area. Here, two sinks are considered to create the multi sink large scale WSN environment. The SCH and route generation using TC-MBWO are explained in the following section.

3.2 SCH SELECTION USING TC-MBWO

In this phase, secure cluster heads are selected to enhance the security and to lessen the energy consumption of the network. This SCH selection is used to avoid the malicious nodes during the communication. In general, the Black Widow Optimization (BWO) is operated on the idea of reproduction style and cannibalism of black widows [21].

3.2.1. Representation and Initialization

The potential solution of TC-MBWO is denoted as spider population, in which it specifies the candidate sensors that can be selected as SCHs. In this phase, the candidate solutions are referred to as spiders that specify the nodes which can be chosen as SCHs. The widow's dimension is equal to the amount of SCHs. Here, a random node ID from 1 to N is used to initialize the position of each widow, wherein the total nodes in the WSN is represented as N. The i^{th} widow initialized in the TC-MBWO is expressed in Equation (1).

$$x_i = (x_{i,1}, x_{i,2}, .., x_{i,NCH}) \quad (1)$$

Wherein, the $x_{i,d}$ defines the widow's position and the candidate nodes between the total nodes is represented as $1 \le d \le NCH$.

3.2.2. Iterative process of SCH selection using TC-MBWO

The iterative process of the TC-MBWO involves the movement and pheromone update that are detailed as follows:

3.2.2.1. Movement

Equation (2) shows the spider's motion which is exhibited in liner and spiral manner.

$$\vec{x}_i(t+1) = \begin{cases} \vec{x}_*(t) - m\vec{x}_{r1}(t) & if\ rand() \le 0.3, \\ \vec{x}_*(t) - \cos(2\pi\beta)\,\vec{x}_i(t) & in\ other\ case \end{cases} \quad (2)$$

Wherein, the $\vec{x}_i(t+1)$ defines the spider's new position which denotes the motion of the spider; $\vec{x}_*(t)$ specifies the best spider identified from the whole population; m is the floating value created between [0.4,0.9]; $r1$ defines the random number generated between 1 and the total search agent size; $\vec{x}_{r1}$ is the chosen $r1$ search agent where $i \neq r1$; β denotes the random float number created between [- 1.0,1.0] and $\vec{x}_i(t)$ denotes the current search agent.

3.2.2.2. Pheromone update

In this searching process, the emitted pheromones from the spider are important for the courtship-mating process. Here, the male spider provides a high response to the sex pheromones received from the healthy females which have a high fertile possibility. Moreover, this kind of activity is utilized to avoid the dangerous mating attempt with hungry cannibal females. In this TC-MBWO, the male black widow chooses the high fertile females rather than the female spider with cannibalism. Therefore, a male black widow chooses only the female spider with high pheromone. Equation (3) shows the computation of spider's pheromone rate.

$$Pheromone = \frac{Cost_{max} - Cost\ (i)}{Cost_{max} - Cost_{min}} \quad (3)$$

Where, the finest and worst costs in the recent population are denoted as $Cost_{max}$ and Cos_{tmin} respectively; the i^{th} spider's current cost is specified as $Cost\ (i)$. The female black widow is specified as cannibal when it has less pheromone and the corresponding female is interchanged with another spider as shown in the equation (4).

$$\vec{x}_i(t) = \vec{x}_*(t) + \frac{1}{2}[\vec{x}_{r1}(t) - (-1)^{\sigma} \times \vec{x}_{r2}(t)] \quad (4)$$

Wherein, $\vec{x}_i(t)$ refers to females with less pheromone; $r1$ and $r2$ are the random values generated from 1 and the total black widow population ($r1 \neq r2$) and σ is the random binary number. The cost function that is used to measure the pheromone rate is formulated in the following section.

3.3 MULTIOBJECTIVE COST FORMULATION FOR SCH SELECTION

The cost functions considered in the TC-MBWO for selecting optimal SCHs are trust (f_1), residual energy (f_2), intracluster distance (f_3), distance from the SCH to BS (f_4) and node degree (f_5). These cost functions are converted into a single objective as shown in equation (5).

$$Cost = \gamma_1 \times f_1 + \gamma_2 \times f_2 + \gamma_3 \times f_3 + \gamma_4 \times f_4 + \gamma_5 \times f_5 \quad (5)$$

Where, γ_1, γ_2, γ_3, γ_4 and γ_5 denotes the weighted parameters allocated to each cost parameter.

- The primary cost value considered in this TC-MBWO is the trust value of each node, in which two distinct trust values are considered, named as direct and indirect trust values. The direct trust (*DT*) value is the ratio between the received packets and broadcasted packets from the source node which is expressed in equation (6). On the other hand, indirect trust (*IDT*) is calculated according to the direct trust measured from the target node which is expressed in equation (7). Accordingly, the calculation of final trust value is shown in equation (8).

$$DT = \frac{R_{a,b}(t)}{S_{a,b}(t)} \tag{6}$$

$$IDT = \frac{1}{NN}\sum_{u=1}^{U} DT_{u,s} \tag{7}$$

$$f_1 = \sum_{i=1}^{P} (DT + IDT)/i \tag{8}$$

Wherein the received and sent packets between the nodes a and b at time t are represented as $R_{a,b}(t)$ and $S_{a,b}(t)$; NN denotes the number of nodes adjacent to the node s and P specifies the total amount of participating nodes

- During the communication, the energy utilization of SCH becomes high as it performs various tasks such as packet receiving, aggregation and broadcasting over the network. Hence, the sensor with higher residual energy is preferred as SCH and the residual energy is expressed in equation (9).

$$f_2 = \sum_{i=1}^{NCH} \frac{1}{E_{CH_i}} \tag{9}$$

Wherein, the E_{CH_i} is the residual energy of the i^{th} SCH.

- Two different distances known as; i) intracluster distance and ii) distance from the SCH to BS, are considered in the cost, because the energy consumption of the node mainly depends on the transmission distance over the network. Hence, the node with less transmission distance is preferred to minimize the energy consumption. Equation (10) and (11) expresses the intra-cluster distance and distance from the SCH to BS.

$$f_3 = \sum_{j=1}^{M} \left(\sum_{i=1}^{I_j} dis(N_i, CH_j)/I_j \right) \tag{10}$$

$$f_4 = \sum_{i=1}^{M} dis(CH_i, BS) \tag{11}$$

Where, distance from i^{th} node to j^{th} SCH and distance from i^{th} SCH to BS are represented as $dis(N_i, CH_j)$ and $dis(CH_i, BS)$ respectively; The amount of normal sensors in the cluster *j* is specified as I_j.

- The amount of normal nodes belonging to the next hop node is node degree which is expressed in equation (12). The node consumes less energy, when it has less node degree in the network.

$$f_5 = \sum_{i=1}^{M} I_j \tag{12}$$

The selection of optimal SCH is done by using the derived cost function. The malicious nodes are avoided using trust value while choosing the SCHs, because the malicious nodes cause packet losses and unwanted energy consumption. The energy used in the cost is used to avoid the node failure which results in high packet delivery, as well as minimal distance, which is used to minimize the energy consumption. Further, the node degree is used to minimize the energy distribution. Therefore, the proposed TC-MBWO selects the optimal SCH to achieve reliable transmission.

3.4 CLUSTER FORMATION

In this phase, the CMs are assigned to chosen SCHs, in which the clusters are created based on the distance and residual energy. The potential function to form the clusters in the network is expressed in equation (13).

$$Potential\ of\ sensor\ (N_i) = \frac{E_{CH}}{dis(N_i, CH)} \tag{13}$$

The derived function is used to allocate the CM to the SCH with less distance and high residual energy.

3.5. ROUTING PATH GENERATION USING TC-MBWO

The TC-MBWO method was also used to discover the secure routing path. In this multi-sink scenario, the sink which is near the source node is taken as the final destination. The steps processed in this routing stage are mentioned as follows:

1. The possible routes between the source SCH and BS are initialized in the spiders whereas the dimension of each spider is equal to the amount of relay nodes.
2. Subsequently, location and pheromone updates are accomplished based on the cost computed for the route.
3. The cost usage while generating the transmission path, involves considering residual energy, the distance from SCH to BS and node degree. Equation (14) shows the cost used in the TC-MBWO based route generation.

$$Cost = \varphi_1 \times \sum_{i=1}^{P} \frac{(DT+IDT)}{i} + \varphi_2 \times \sum_{i=1}^{NCH} \frac{1}{E_{CH_i}} + \varphi_3 \times \sum_{i=1}^{M} dis(CH_i, BS) + \varphi_4 \times \sum_{i=1}^{M} I_j \tag{14}$$

Where, φ_1, φ_2, φ_3 and φ_4 are weighted parameters assigned to each objective of route generation.

The overall flowchart of the TC-MBWO method is shown in the Figure 2. As illustrated in the Figure 2, initially the nodes are deployed randomly in the network area. Subsequently, the cost formulation of TC-MBWO for CH selection takes place as shown in the section 3.3. The formulated cost value is used to choose an appropriate SCH, followed by the clusters, formed as shown in section 3.4. Fi-

nally, the secure path over the network is identified using the TC-MBWO. For a better analysis of the TC-MBWO, the simulation is executed until the dead nodes of the WSN is equal to the total number of initialized nodes. Therefore, the proposed TC-MBWO helps to identify the secure path with higher residual energy, lesser transmission distance and lesser node degree. Hence, the energy consumption of the nodes are minimized by using the TC-MBWO-based routing which helps to improve the network lifetime.

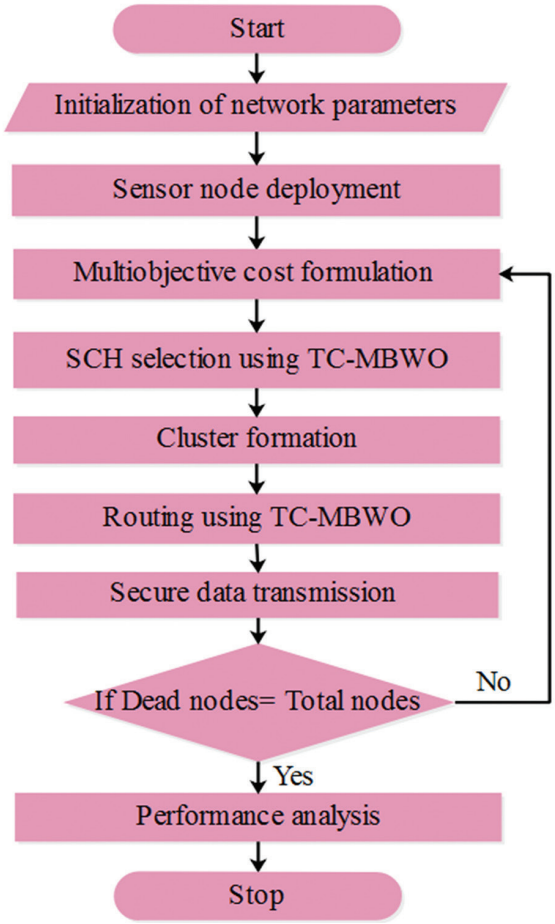

Fig. 2. Flowchart of the TC-MBWO method

4. RESULTS AND DISCUSSION

The design and implementation of reliable transmission using TC-MBWO are done using MATLAB R2018a. The system used in the analysis is operated with i5 processor having 6GB of RAM. The main objective of the TC-MBWO method is to achieve an improved security and energy efficiency for large scale WSN. The simulation parameters of the TC-MBWO are mentioned in Table 1.

Table 1. Simulation parameters

Parameters	Value
Area	500m×500m
Nodes	100
Location of sink	(500, 500) & (250, 250)
Packet size	4000 bits
Initial energy	0.5 J

4.1 PERFORMANCE ANALYSIS

The performance of the TC-MBWO is analyzed by means of alive nodes, dead nodes, energy consumption, throughput, and network lifetime. Here, the TC-MBWO's performances are evaluated with one classical approach i.e., LEACH in which the implementation is done with the same specifications as in Table 1.

4.1.1. Alive nodes and dead nodes

Alive nodes are defined as the nodes with enough residual energy to transmit the data packets to the sink. On the contrary, the dead nodes are inversely proportional to the alive nodes of the network. Specifically, the node is declared as dead when it exhausts its energy while transmitting the packets. Figures 3 and 4 respectively show the alive node and dead node comparison, for the TC-MBWO and LEACH. From the analysis, it is concluded that the TC-MBWO achieves higher alive nodes and lesser dead nodes than the LEACH. In general, the malicious nodes that exist in the network cause higher energy consumption. But, the TC-MBWO avoids the malicious nodes during the SCH selection and routing, therefore the energy consumption of the nodes is minimized. This helps in increasing the alive nodes of the TC-MBWO.

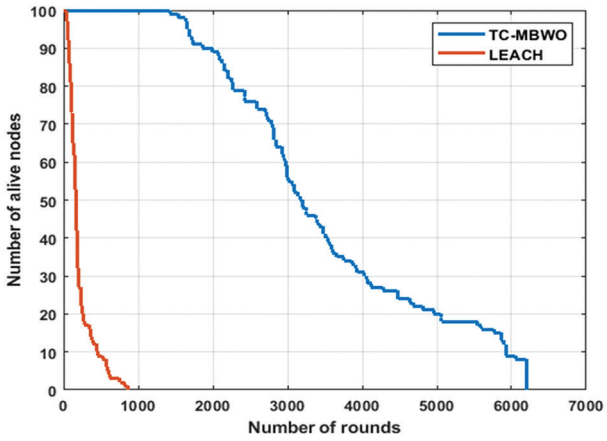

Fig. 3. Alive nodes Vs. rounds

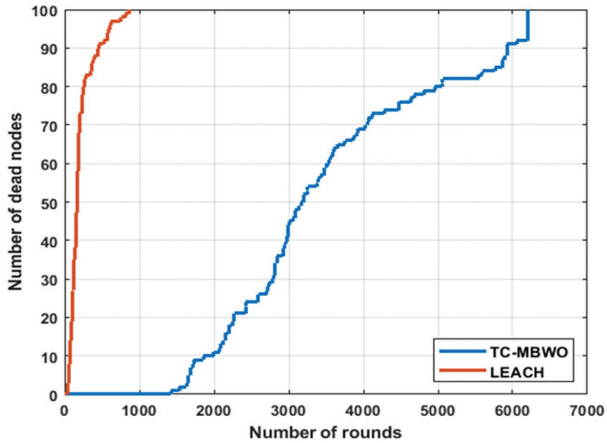

Fig. 4. Dead nodes Vs. rounds

4.1.2 Energy consumption

Energy consumption of the network is defined as the amount of energy consumed while receiving and broadcasting the data packets. The energy consumption comparison for the TC-MBWO and LEACH is shown in Figure 5. From Figure 5, it is concluded that the energy consumption of the TC-MBWO is lesser when compared to LEACH, which achieves higher energy consumption because it fails to mitigate the malicious nodes and also performs single hop transmission. Moreover, TC-MBWO achieves higher energy efficiency because of the mitigation of malicious nodes using trust and the generation of the shortest route.

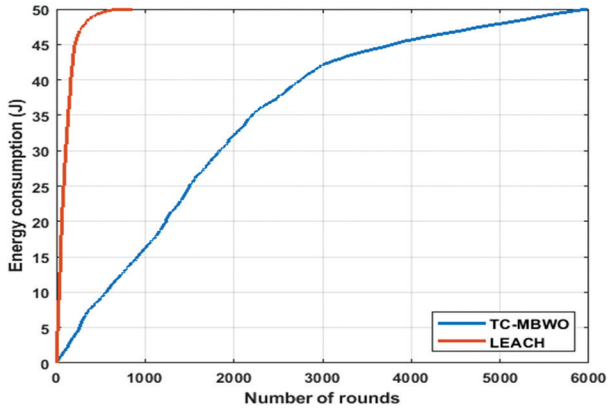

Fig. 5. Energy consumption Vs. rounds

4.1.3. Throughput

Throughput is defined as the amount of packets successfully received at the sink, and is analyzed in bits per second. Figure 6 shows the throughput comparison for the TC-MBWO and LEACH. The throughput of TC-MBWO is greatly increased than the LEACH, because of the secure data transmission. Specifically, the data delivery of the TC-MBWO is improved by avoiding node/link failure and malicious nodes while broadcasting the data packets.

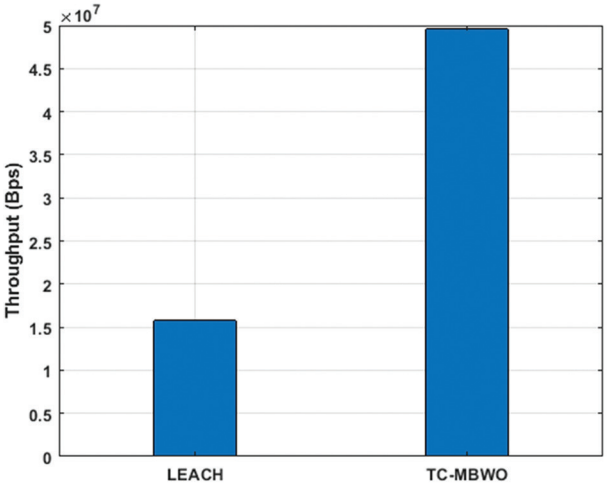

Fig. 6. Throughput Vs. rounds

4.1.3. Network lifetime

Network lifetime is defined as the round where all the nodes exhaust their energy over the large-scale WSN. Here, the lifetime is analyzed by using three metrics: First Node Die (FND), Half Node Die (HND) and Last Node Die (LND). The lifetime comparison for the TC-MBWO and LEACH is shown in Figure 7. From Figure 7, it is inferred that the lifetime of the TC-MBWO is high when compared to the LEACH. For example, the LND of the TC-MBWO is 6204 whereas the LND of the LEACH is 864. The LEACH results in lesser lifetime due to the presence of malicious attacks and single hop transmission. But, the proposed TC-MBWO achieves a higher lifetime due to its appropriate cost function.

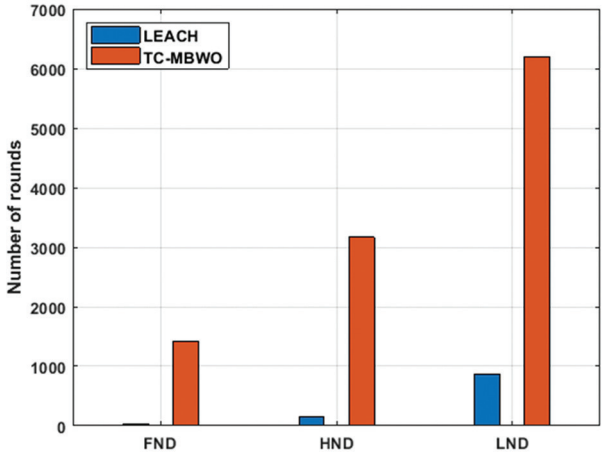

Fig. 7. Network lifetime Vs. rounds

4.2. COMPARATIVE ANALYSIS

The existing research PSO-GWO [19], P-WWO [21] and P-SMO [22] are used to evaluate the efficiency of the TC-MBWO. Table 2 provides the comparative analysis of the PSO-GWO [19], P-WWO [21], P-SMO [22] and TC-MBWO. Additionally, the graphical comparison of alive nodes is shown in Figure 8.

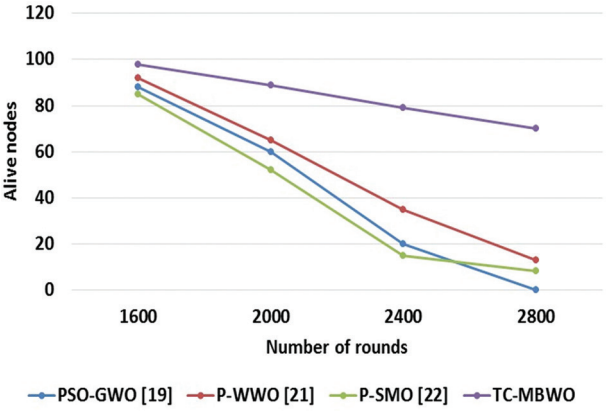

Fig. 8. Graphical comparison of alive nodes

From Table 2 and Figure 8, it is concluded that the TC-MBWO achieves better performance than the PSO-GWO [19], P-WWO [21], and P-SMO [22], because of its

optimal cost function selection. The derived multiobjective cost function is used to achieve a secure and energy-aware data transmission over the large scale WSN. The energy consumption of the nodes are minimized by avoiding malicious nodes and discovering shortest path using the TC-MBWO. The lesser energy consumption of the nodes increases the network lifetime, therefore the alive nodes of the TC-MBWO are higher in number in the WSN. Moreover, the throughput of the TC-MBWO is improved by avoiding the malicious nodes during the selection of SCH and route.

Table 2. Comparative analysis of TC-MBWO

Performance measures	Methods	Number of rounds			
		1600	2000	2400	2800
Alive nodes	PSO-GWO [19]	88	60	20	0
	P-WWO [21]	92	65	35	13
	P-SMO [22]	85	52	15	8
	TC-MBWO	98	89	79	70
Energy consumption	PSO-GWO [19]	920	1150	1400	1625
	TC-MBWO	26.5968	32.2538	36.7779	40.3968
Throughput	PSO-GWO [19]	15.8×104	16×104	16×104	16×104
	TC-MBWO	12.8×106	16×106	19.2×106	22.4×106

5. CONCLUSION

A secured clustering and a routing path are developed using the TC-MBWO algorithm to obtain secure data transmission between the nodes. The node's energy depletion is minimized by using the TC-MBWO-based optimal SCH selection. Next, the secure route between the desired nodes is generated by using the TC-MBWO. The SCH selection and secure routing path generation done by TC-MBWO are improved by using distinct cost parameters such as trust, residual energy, distance, and node degree. The trust considered in the TC-MBWO helps to mitigate malicious attacks during data transmission. From the obtained results, it is concluded that the TC-MBWO method outperforms the PSO-GWO, P-WWO and P-SMO in the comparative analysis. The number of alive nodes in TC-MBWO is 70 for 2800 rounds which is a much higher result, when compared to PSO-GWO, P-WWO and P-SMO. In the future, a novel optimization algorithm can be used for improving the performance of the WSN.

6. REFERENCES:

[1] V. Kavidha, S. Ananthakumaran, "Novel energy-efficient secure routing protocol for wireless sensor networks with Mobile sink", Peer-to-Peer Networking and Applications, Vol. 12, No. 4, 2019, pp. 881-892.

[2] M. Selvi, S. V. N. Santhosh Kumar, S. Ganapathy, A. Ayyanar, H. Khanna Nehemiah, A. Kannan, "An energy efficient clustered gravitational and fuzzy based routing algorithm in WSNs", Wireless Personal Communications, Vol. 116, No. 1, 2021, pp. 61-90.

[3] C. Deepa, B. Latha, "HHSRP: a cluster based hybrid hierarchical secure routing protocol for wireless sensor networks", Cluster Computing, Vol. 22, No. 5, 2019, pp. 10449-10465.

[4] P. Rodrigues, J. John, "Joint trust: An approach for trust-aware routing in WSN", Wireless Networks, Vol. 26, No. 5, 2020, pp. 3553-3568.

[5] G. Dhand, S. S. Tyagi, "SMEER: secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks", Wireless Personal Communications, Vol. 105, No. 1, 2019, 17-35.

[6] M. Revanesh, V. Sridhar, J. M. Acken, "Secure coronas based zone clustering and routing model for distributed wireless sensor networks", Wireless Personal Communications, Vol. 112, No. 3, 2020, pp. 1829-1857.

[7] H. Zhou, Y. Wu, L. Feng, D. Liu, "A security mechanism for cluster-based WSN against selective forwarding", Sensors, Vol. 16, No. 9, 2016, p. 1537.

[8] W. Ke, O. Yangrui, J. Hong, Z. Heli, L. Xi, "Energy aware hierarchical cluster-based routing protocol for WSNs", The Journal of China Universities of Posts and Telecommunications, Vol. 23, No. 4, 2016, pp. 46-52.

[9] M. Pavani, 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, 2019, pp. 274-283.

[10] V. Vijayalakshmi, A. Senthilkumar, "USCDRP: unequal secure cluster-based distributed routing protocol for wireless sensor networks", The Journal of Supercomputing, Vol. 76, No. 2, 2020, pp. 989-1004.

[11] W. Fang, W. Zhang, W. Chen, J. Liu, Y. Ni, Y. Yang, "MSCR: multidimensional secure clustered routing scheme in hierarchical wireless sensor networks", EURASIP Journal on Wireless Communications and Networking, Vol. 2021, No. 1, 2021, pp. 1-20.

[12] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks", Wireless Personal Communications, Vol. 110, No. 4, 2020, pp. 1637-1658.

[13] M. Maheswari, R. A. Karthika, "A novel QoS based secure unequal clustering protocol with intrusion detection system in wireless sensor networks", Wireless Personal Communications, Vol. 118, No. 2, 2021, pp. 1535-1557.

[14] Y. U. Xiu-Wu, Y. U. Hao, L. Yong, X. Ren-rong, "A clustering routing algorithm based on wolf pack algorithm for heterogeneous wireless sensor networks", Computer Networks, Vol. 167, 2020, pp. 106994.

[15] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. Khannah Nehemiah, A. Kannan, "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks", Wireless Personal Communications, Vol. 105, No. 4, 2019, pp. 1475-1490.

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

[17] Q. Shi, L. Qin, Y. Ding, V. Xie, J. Zheng, L. Song, "Information-aware secure routing in wireless sensor networks", Sensors, Vol. 20, No. 1, 2020, p. 165.

[18] S. Sefati, M. Abdi, A. Ghaffari, "Cluster-based data transmission scheme in wireless sensor networks using black hole and ant colony algorithms", International Journal of Communication Systems, Vol. 34, No. 9, 2021, p. e4768.

[19] S. Prithi, 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, 2021, pp. 545-559.

[20] K. SureshKumar, P. Vimala, "Energy efficient routing protocol using exponentially-ant lion whale optimization algorithm in wireless sensor networks", Computer Networks, Vol. 197, 2021, p. 108250.

[21] P. S. Khot, U. Naik, "Particle-Water Wave Optimization for Secure Routing in Wireless Sensor Network Using Cluster Head Selection", Wireless Personal Communications, Vol. 119, No. 3, 2021, pp. 2405-2429.

[22] P. S. Khot, U. L. Naik, "Cellular automata-based optimised routing for secure data transmission in wireless sensor networks", Journal of Experimental & Theoretical Artificial Intelligence, 2021, pp. 1-19.