Received: August 24, 2021. Revised: October 26, 2021. 214

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

# Secured Data Transmission Using Multi-Objective Trust Based Bat Optimization Algorithm and Enhanced Homomorphic Cryptosystem for WSN

**Gouramma Halidoddi[1]*** **Rubini Pandu[2]**

[1]*Department of Computer Science and Engineering, Guru Nanak Dev Engineering College, Bidar, India*
[2]*School of Engineering and Technology, CMR University, Bengaluru, India*
* Corresponding author's Email: gouramma.16phd@cmr.edu.in

**Abstract:** Wireless Sensor Networks (WSNs) have gained huge attention in different areas due to their self-configurability, easy maintenance and scalability features. WSN is configured with more nodes to transfer the data inside the network. The sensor networks are usually classified by low bandwidth, limited energy, limited power supplies and small size memory which leads to a very demanding environment to provide security. In recent years, accomplishing the network security objective with low energy utilization is a major issue in WSN. In this paper, two-level security is proposed to secure data transmission over the WSN. First, the secure clustering and routing operation are performed by using the Multi-Objective Trust-based Bat Optimization Algorithm (MOTBOA). Second, the data security of the network is improved by the Enhanced Homomorphic Cryptosystem (EHC). This paper aims to offer secure communication in WSN. It is achieved by using the EHC method for the operation of encryption and decryption over the data during communication among the nodes. The performance of the proposed MOTBOA-EHC method is evaluated in terms of detection rate, delay, throughput, routing load and Packet Delivery Ratio (PDR). The existing methods namely Trust based Dynamic Source Routing (TDSR), Monarch-Cat Swarm Optimization-based routing protocol and Secured Quality of Service aware Energy Efficient Routing (SQEER) are used to evaluate the performances of the MOTBOA-EHC method. The PDR of the MOTBOA-EHC method is 92% at 100 rounds that are high when compared to the TDSR, MCSO and SQEER.

**Keywords:** Detection rate, Enhanced homomorphic cryptosystem, Network security, Packet delivery ratio, Trust-based bat optimization algorithm, Wireless sensor networks.

## 1. Introduction

WSNs is a promising technology used globally in different real time applications such as healthcare monitoring, battlefield monitoring, emergency response and environmental monitoring [1-3]. In WSN, the sensor nodes are unsystematically organized in the search areas to gather data in a periodic or event-driven form. Here, the wireless broadband channels are utilized by the end-users to access the required sensor data from base station (BS) over the internet [4, 5]. Besides, all the data collection and data transmission in WSN is performed through the sensor nodes deployed in the network area. The energy required in the sensor nodes for data transmission and collection is provided by the battery [6]. Hence, the lifespan of the network is mainly dependent on the sensor nodes. The nodes are only able to participate in data transmission until they run out of power. The replacement or charging of the failed sensor nodes in the network is expensive and complicated [7, 8].

Security is one of the essential requirements in WSN [9]. The security of WSN includes four major factors such as confidentiality, integrity, authentication and availability of data. In the WSN network, the confidentiality and authentication of data in every node is essential to secure the data transmission over the network [10, 11]. Generally, WSN is vulnerable to various threats [12, 13]. Hence, the sensor nodes are easily affected by the enemies and act as malignant nodes. The malignant nodes in the network cause insecurity to the entire network during data transmission. The occurrence of unauthenticated data access is possible that results in

loss of essential information stored in the nodes [14-16]. As a result of this, a secured and energy-efficient routing protocol is an extreme concern in extending the lifespan and providing security to the network. While designing a protocol to obtain a secured communication over WSN, the following factors have to be taken into consideration: integrity, forward secrecy, backward secrecy, freshness, non-repudiation and availability [17]. Hence, this paper proposed a secured clustering and routing with encrypted data transmission by using the MOTBOA-EHC method. Furthermore, the main contribution of this research work by using MOTBOA-EHC method are given as follows.

- The MOTBOA is mainly utilized for an effective CH selection between the nodes present in the network. Since, the bat optimization has the capacity of automatic zooming into the search space where the promising solution is found by the bat during the searching process.
- The clustering and routing are performed based on the multi objective fitness functions such as trust value, residual energy, communication cost, and node degree. The secured cluster head (CH) selection is performed by eliminating the malicious nodes in the cluster according to the trust value calculation.
- The EHC method is introduced in this paper for the encryption and decryption of the transmitted data to ensure its the security.

The overall structure of this research paper is organized as follows. The outline of the related work is represented in the 2nd section. The proposed approach of the MOTBOA-EHC method is represented in the 3rd section. The experimental simulation and results are provided in the 4th section. At long last, the paper is finished up in section 5.

## 2. Related works

The related works about the recent techniques implemented for secure and energy-efficient routing in WSN are reviewed in this section.

Salari-moghaddam, taheri and karimi [18] utilized the trust based routing algorithm to improve the quality of services in dynamic source routing (DSR) protocol. The developed method was prevented the untrusted nodes in routing path by using the trust based DSR (TDSR). Next, the developed method was introduced enhanced DSR (EDSR) which was used to improve the quality of services. Therefore, the DSR method was achieved better performance in PDR and reduced the energy consumption in the network. However, the DSR and TDSR protocols provided low performance in discovering the shortest path and sometimes it selected the longer path which caused the higher delay in WSN.

Rathee [19] developed an ant colony optimization (ACO) based quality of service (QoS) aware balancing secure routing algorithm for WSN. The developed method was considering two algorithms such as energy efficient routing with node compromised resistance (EENC) and distributed energy balancing routing (DEBR) algorithm which was used to improve the network lifetime, minimized the delay and sending data through the trusted nodes. Moreover, the delay of the DEBR is low when compared with the EENC algorithm. Due to the EENC considered only the distance between communication nodes, the delay is low.

Patil, deshpande, and mane [20] integrated monarch butterfly optimization algorithm with cat swarm optimization algorithm i.e., monarch-cat swarm optimization (MCSO) for opportunistic routing in WSN. The optimal route for data transmission was obtained through performing two major steps such as secure node selection and opportunistic routing. The optimal path to the destination was provided by selecting the nodes among the secure nodes. The presented hybrid algorithm achieved high throughput, high detection rate and less delay when compared with the other existing algorithms. The computational overhead of the developed hybrid algorithm was unable to minimize.

Alghamdi [21] was presented dij-huff (DH) method for selecting the secure and energy efficient path optimization techniques in WSN. The developed method was used to discover the optimum distance path and nodes with maximum energy. Furthermore, the DH method was utilized the huffman coding and binary hop count which was used to obtain end-to-end security code. The advantage of the developed method was capable of transfer the information to the node with higher energies and provided secure communication. However, the cluster head was overloaded as it has to carry out all the activities in the network system.

Sun [22] implemented the secure routing protocol based on multi-objective (SRPMA) ant-colony-algorithm for WSN. The developed method was mainly considering two objective functions. The first objective function was considering the typical residual energy of routing path which is decreased the energy utilization and assures the energy utilization

being usual. The second objective function was considering the typical trust value of the routing path which ensures the route nodes are being trusted. However, the SRPMA method was consuming more time to predict the energy utilization level in the network.

Kalidoss [23] presented the secured QoS aware energy efficient routing (SQEER) to improve the WSN's security by using the energy and trust model. Here, the trust scores were delivered by using the authentication method with a key-based security technique in the trust model. Moreover, QoS metrics such as PDR, delay and error rate were used to select the CH whereas the energy, hop-count and path-trust were used to generate the final path. However, this SQEER was failed to consider the distance while generating the routing path. Therefore, the energy consumption of the SQEER was high, when the distance of data transmission path is high in the network.

The limitations found from the existing researches are high transmission distance, high routing load/ overhead and high energy consumption. To overcome the aforementioned drawbacks, two level security is developed for improving the performances of WSN. To achieve less energy consumption, the MOTBOA generates the transmission path with less distance whereas the routing load is reduced by minimizing the broadcasted control packets during route discovery. Moreover, data security of the WSN is improved by using the trust value in the MOTBOA and EHC method.

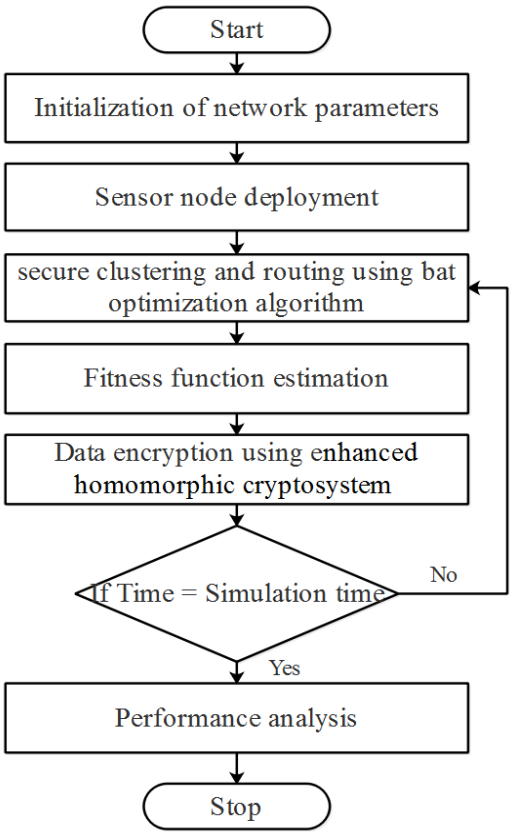


Figure. 1 Flowchart of the proposed MOTBOA-EHC method

## 3. Proposed method

The proposed MOTBOA-EHC method has three different phases such as clustering, routing and encryption & decryption. The clustering and routing process are performed by using MOTBOA and the encryption and decryption are performed by using enhanced homomorphic cryptosystem (EHC). The CH selection is performed based on the fitness functions considered in the proposed method. The considered fitness functions are trust value, residual energy, communication cost, and node degree. The trust value of the nodes is computed to prevent the network from denial-of-service (DoS) and blackhole attacks. Therefore, the developed two level security is used to improve the packet delivery of the MOTBOA-EHC method. The flowchart of the proposed MOTBOA-EHC method is shown in Fig. 1.

### 3.1 Overview of bat optimization algorithm

Bat optimization algorithm (BOA), a new population-based algorithm, was inspired by the echolocation of the bat species known as microbats for looking through target. The refreshed arrangements of BOA are built dependent on triple essential factors like 1.echolocation, 2.frequency and 3.commotion. Bats are used the echolocation for finding their target, foundation frequency for convey the variable frequency, and commotion for search the target. Solutions for the BOA are made by changing the boundaries like frequencies, pulse emission rates, and commotion of the bats, as indicated by the estimation of the objective function. Equations for upgrading the locations and speeds of BOA in d-dimensional inquiry space are as per the following:

$$f_i = f_{min} + (f_{max} - f_{min}) \times \beta \quad (1)$$

where, the frequency for changing velocity is referred as $f_i$, the maximum and minimum frequency of the bats emanating the pulse is referred as $f_{max}$ and $f_{min}$ respectively and the randomly generated vector is represented as $\beta$. At initially, a frequency in a consistent range $\in [f_{min}, f_{max}]$ is assigned to each bat. BA improves the bat areas' vectors and velocity $v$, and $x$ in search space of d-dimensional.

$$v_i^t = v_i^{t-1} + (x_i^{t-1} - x_{best}) \times f_i \quad (2)$$

$$x_i^t = x_i^{t-1} + v_i^t \quad (3)$$

where, the current iteration is the superscript of t, and the global best solution is represented as $x_{best}$. Using the phase technique, creating a new site for the bats is written as:

$$x_i = x_i + \varepsilon \times A^t \quad (4)$$

where, $\varepsilon$ is a random variable in the range $\in [-1, 1]$, and denotes the weight for the commotion of the bats at the present generation. The commotion of bats $A$ is expressed as:

$$A_i^{t+1} = \alpha \times A_i^t \quad (5)$$

where, variable constant is α. The symbol denotes the rate of the pulse emission $r$ and $\in [0, 1]$. The pulse emission rate is formulated as:

$$r_i^{t+1} = r_i \times [1 - e^{-\gamma \times t}] \quad (6)$$

where, γ is the constant variable. In the process, this rate $r$ is taken as the control to switch between the global and local search. A local search with a random walk is activated if a random number is greater than $r$.

## 3.2 MOTBOA based clustering algorithm

The fitness functions considered for the MOTBOA based CH selection are trust value, residual energy, communication cost, and node degree. The CH selection is performed by eliminating the malignant node in the cluster based on the trust value calculation. Hence, the DoS and black hole attacks are avoided in the network.

### 3.2.1. Bat representation

A bat is referenced to as a viable solution in BOA. A bat indicates a group of sensor nodes to be chosen as CHs in the CH selection process. Each bat has a dimension equal to the number of CHs in the network.

### 3.2.2. Bat initialization

A random node_id between 1 and $n$ is assigned to each bat location. Let $B_i = (B_{i,1}(t), B_{i,2}(t), \ldots\ldots\ldots\ldots, B_{i,m}(t))$ be the $i^{th}$ bat. where, each bat position $B_{i,d}, 1 \leq d \leq m$ represents node_id between 1 to $n$ in the network.

### 3.2.3. Fitness function derivation

The fitness functions for the MOTBOA based clustering algorithm is derived using the following parameters:

**a. Trust value**

In the proposed method, the trust value of the individual node is calculated and an optimal path for secure communication is selected by using bat optimization algorithm. The trust model of the node is computed as follows:

$$F_1 = TR_{i,j}^{direct} + TR_{i,j}^{indirect} + TR_{i,j}^{recent} + TR_{i,j}^{bytes} \quad (7)$$

The trust model computation is given in Eq. (7). The trust utilized for the calculation of the individual node are direct trust $TR_{i,j}^{direct}$, indirect trust $TR_{i,j}^{indirect}$, recent trust $TR_{i,j}^{recent}$ and trust based on data bytes $TR_{i,j}^{bytes}$. The direct trust value depends on the estimated time of the nodes. The calculation of the indirect trust is performed with the recommendation received from the adjacent nodes. The direct trust and the indirect trust are combined together to get the recent trust. The trust factor based on data bytes calculated by using the total numbers of bytes send from the sensor node and aggregate sum of data bytes received via destination node. The equation for the direct trust (8), indirect trust (9), recent trust (10) and trust based on data bytes (11) are given below.

$$TR_{i,j}^{direct}(t) = \frac{a}{a+b} \quad (8)$$

where, $t$ represents the time; $i$ & $j$ represents the node in the network; amount of successful and unsuccessful interactive behaviors is represented as $a$ and $b$ respectively.

$$TR_{i,j}^{indirect}(t) = \sum_{k=1}^{q} s_k R_{i,j}^k \quad (9)$$

where, the amount of received recommendations are denoted as $q$; the $j^{th}$ node reputation saved by the $i^{th}$ node is $R_{i,j}$, the recommendation provided by the adjacent node $k$ is $R_{i,j}^k$ and the weight of $R_{i,j}^k$ is $s_k$.

$$TR_{i,j}^{recent}(t) = \alpha \times T_{i,j}^{direct}(t) + (1 - \alpha) \times T_{i,j}^{indirect}(t) \quad (10)$$

$$TR_{i,j}^{bytes}(t) = \frac{\partial_{i,j}^{i}}{d} + \frac{\partial_{i,j}^{j}}{d} \quad (11)$$

where, α=0.3; the data bytes forwarded by the source node is represented as $\partial_{i,j}^{i}$; the data bytes received by the destination is $\partial_{i,j}^{j}$ and limit of packet transmission is represented as $d$.

**b. Residual energy**

The residual energy of the nodes in the network is one of the important factors during the selection of the CH. Since, the CH consumes huge amount of energy for data collection, processing and data transmission and path selection. The equation to calculate the residual energy is given below.

$$F_2 = E_0 - E_c \tag{12}$$

Where, the initial energy is represented as $E_0$ and the energy employed by the node is represented as $E_c$.

**c. Communication cost**

The energy consumed by the transmitting data is directly proportional to the square of the distance between the candidate nodes as well as the source node. The equation for the computation of communication cost is given in Eq. (13).

$$F_3 = \frac{d_{avg}^2}{d_0^2} \tag{13}$$

where, the average distance between the nodes and the adjacent nodes is represented by $d_{avg}$ and the transmitting radius of the nodes is represented by $d_0$.

**d. Node degree**

The node degree is the significant factor in next-hop selection. If the next- hop is chosen as a low node degree, after that the performance of the node is lasted for a long duration and received low data from its member. Thus, the next-hop mostly preferred low node degree. The node degree in the fitness function is conveyed in Eq. (14).

$$F_4 = \frac{1}{\sum_{i=1}^{m} I_i} \tag{14}$$

Further, all the above-mentioned multiple objective functions are changed into a single objective function by utilizing the weighted-sum approach in Eq. (15). Here, the weights combined with each objective function is denoted as $\beta_1$, $\beta_2$, $\beta_3$and $\beta_4$.

$$Fitness\ Function = \beta_1(F_1) + \beta_2(F_2) + \beta_3(F_3) + \beta_4(F_4) \tag{15}$$

where, $\sum_{i=1}^{3} \beta_i = 1$ , $\beta_i \in (0,1)$ .

### 3.3 MOTBOA based routing algorithm

The fitness functions considered for the route selection process are trust value, residual energy, communication cost, and node degree. The route selection process is performed based on the aforementioned fitness functions.

#### 3.3.1. Bat representation

A bat is referenced to as a viable solution in BOA. A bat indicates a group of sensor nodes to be chosen as CHs in the CH selection process. Each bat has a dimension equal to the number of CHs in the network.

#### 3.3.2. Bat initialization

A random node_id between 1 and $n$ is assigned to each bat location. Let $B_i = (B_{i,1}(t), B_{i,2}(t), \dots\dots\dots, B_{i,m}(t))$ be the $i^{th}$ bat. Where each bat position $B_{i,d}, 1 \leq d \leq m$ represent node_id between 1 to n in the network.

### 3.4 Enhanced homomorphic cryptosystem

WSN are defenseless against the hackers exploring the wireless communication framework and its transmission nature. The energy and asset imperatives are likewise extra shortcomings on the sensor side. Generally, the sensor gadgets are arbitrarily arranged in an uncontrolled environment. Subsequently, they are effortlessly presented to actual assaults. The significant security prerequisites in WSN are availability, integrity, confidentiality, authentication and non-reputation. For that, an enhanced homomorphic cryptosystem (EHC) is proposed in this research for data encryption and decryption operation. By encrypting the data in the network during data transmission, the information in the nodes are prevented from the DoS attack and blackhole attack.

Homomorphic encryption (HE) is the combination of addition, multiplication, or mixed multiplication homomorphism. HE is an operation performed over the scrambled data and it provides similar results after the computation as the working straightly on the clear data. Here, the decryption performing over the sum of the two ciphertexts is the same as the addition operation performing over the two plain text represented as $E(a+b) = E(a) + E(b)$. The decryption performing over the product of two ciphertexts is the same as multiplication of two plain texts represented as $E(a \times b) = E(a) \times E(b)$.

The proposed EHC is utilized as additive

homomorphic encryption-based cryptographic algorithms. This cryptographic algorithm uses large number $m$, where $m = p \times q$. Here $p$ and $q$ are enormous indivisible numbers, which are kept private. $q$ is a sharing private key. That number m is additionally a private key to scramble the information.

Tracking down an arbitrary number $r$ is a very troublesome issue, so which is kept private. The EHC algorithm incorporates three principle cycles such as private key generation (K), the encryption algorithm (E) and the decryption algorithm (D).

#### 3.4.1. Key generation (K)

i. $p, q \in P$, where $P$ is prime, and $m = p \times q$.
ii. Random number $r$ is generated.
iii. The set of original plaintext messages $P = Z_p = \{x: x <= p\}, Z_m = \{x: x < m\}$ has the set of ciphertext messages.
iv. Private values $r, m$ and $q$.
v. Shared key $K = p$.

#### 3.4.2. Encryption algorithm (E)

i. $x \in Zp$
ii. The ciphertext $C$ is calculated as $y = E_p(x) = (x + r \times pq)(mod\ m)$.

#### 3.4.3. Decryption algorithm (D)

i. The plaintext $x$ is recovered as $x = D_p(y) = y\ mod\ p$.

In this MOTBOA-EHC method, two levels of security are provided for improving the data delivery of the WSN. In the first level, secure clustering and routing is accomplished by using the MOTBOA, where trust value is considered as an important parameter for mitigating malicious attackers. Next, the residual energy considered in the MOTBOA is used to avoid node failure. The communication cost and node degree used in the MOTBOA is used to identify the shortest path with less number of hops that helps to minimize the delay. In the second level of security, the EHC based data encryption/ decryption is used to provide the data security that helps to secure the data from the unauthorized users. Therefore, the data security over the network is obtained while minimizing the delay and routing load.

## 4. Discussion of the experimental results

In this section, the NS2 platform is utilized for simulation result and 100 nodes are randomly arranged in the area of 1200 m × 1200 m to simulate the proposed MOTBOA-EHC method. The MOTBOA-EHC method is applicable for both DoS attacks as well as black hole attacks. In this research, the simulation results for DoS attack is analyzed. To simulate DoS attack, various quantity of nodes presented as malignant node. The sink node's energy is limitless and the starter energy of every sensor node is steady. Table.1 gives the details of the parameter settings of the nodes.

Table 1. Specification parameters

| Parameters | Values |
|---|---|
| Network interface type | Wireless phy |
| Communication radius | 250mm |
| Number of connections | 20 |
| Number malignant nodes | 10 |
| Mac protocol | Mac/802.11 |
| Antenna pattern | Omni antenna |
| Wireless propagation protocol | Two ray ground |
| Initial energy | 50J |
| Queue type | Pri Queue |
| Speed of the data flow | 448kbits/s |
| Size of packets | 210Byte |
| Simulation time | 100s |

### 4.1 Performance evaluation

The performance of the MOTBOA-EHC method is analyzed in terms of detection rate, delay, throughput, routing load and PDR. Here, three different existing methods namely TDSR [18], MCSO [20] and SQEER [23] are used to evaluate the MOTBOA-EHC. This TDSR [18], MCSO [20] and SQEER [23] are designed and simulated by using the same specifications mentioned in Table 1. The performance evaluation is explained as follows:

#### 4.1.1. Detection rate

Detection rate ($T_{det}$) provides the accurate value of the correctly identified attacks in the network. The detection rate of the system is calculated by using the Eq. (16)

$$T_{det} = \frac{\sum D_i}{|X|} \forall_i \in X, where\ D_i = \begin{cases} 1, if\ d_i = c_i, \\ 0, if\ d_i \neq c_i. \end{cases} \quad (16)$$

where, $X$ represents the aggregate sum of the identified attackers by the system. $d$ represents the detection value is performed. $c$ represents the node behavior. Fig. 2 illustrates the comparison between the TDSR [18], MCSO [20], SQEER [23] and the MOTBOA-EHC method in term of detection rate. Here, the detection rate of the MOTBOA-EHC method is high when compared to the existing TDSR [18], MCSO [20] and SQEER [23]. The trust value calculation is performed in the proposed method.

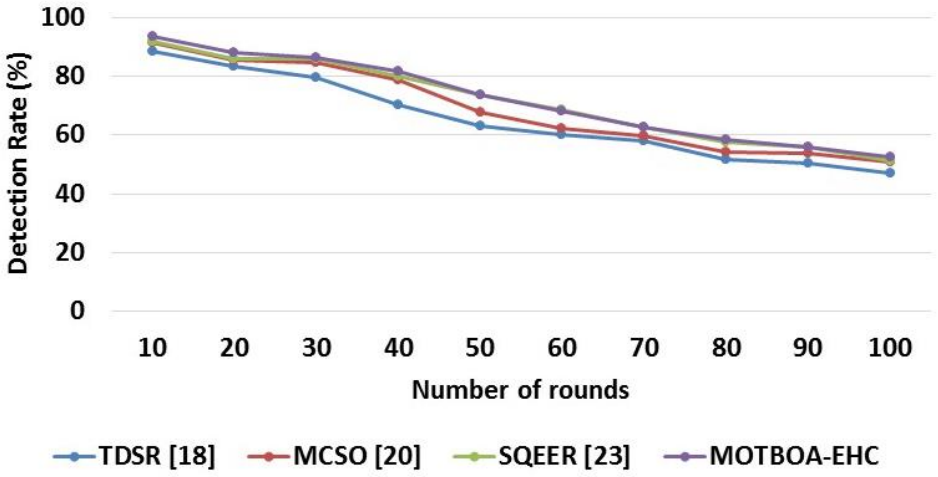


Figure. 2 Detection rate

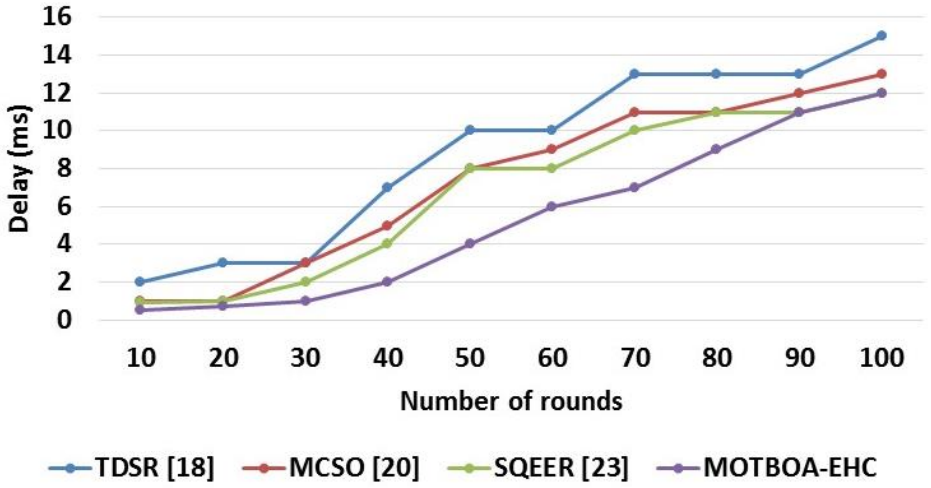


Figure. 3 Delay

Hence, the malignant node detection increased in the network that improves the security of the WSN network.

#### 4.1.2. Delay

The calculation of delay depends upon the quantity of the nodes. When the quantity of nodes rises, then the delay is increased. To obtain effective routing, the delay of the network should be low. The delay is calculated from the time consumption of the nodes to respond.

Fig. 3 illustrates the comparison between the TDSR [18], MCSO [20], SQEER [23] and the MOTBOA-EHC method in term of delay. Here, the delay of the MOTBOA-EHC method is low when compared to the existing TDSR [18], MCSO [20] and SQEER [23]. By considering communication cost and trust value in the fitness function, the link failure during data transmission is avoided. Hence, there is minimum delay only occur during data transmission.

#### 4.1.3. Throughput

The throughput is derived as the number of packets attained in a particular time and then the packet delivery is recognized. The throughput calculation is performed by using Eq. (17).

$$Throughput = \frac{N_r}{T} \times 100\% \quad (17)$$

where, $N_r$ represents the aggregate sum of the nodes and $T$ represents the simulation time.

Fig. 4 illustrates the comparison between the TDSR [18], MCSO [20], SQEER [23] and the MOTBOA-EHC method in term of throughput. Here, the throughput of the MOTBOA-EHC method is high when compared to the existing TDSR [18], MCSO [20] and SQEER [23]. The fitness functions considered in the proposed MOTBOA-EHC method improve the overall throughput of the system.

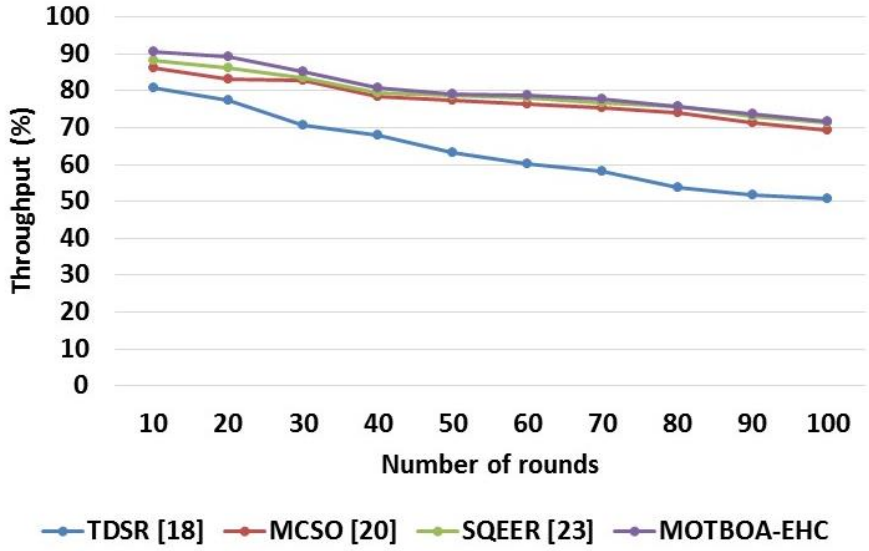


Figure. 4 Throughput

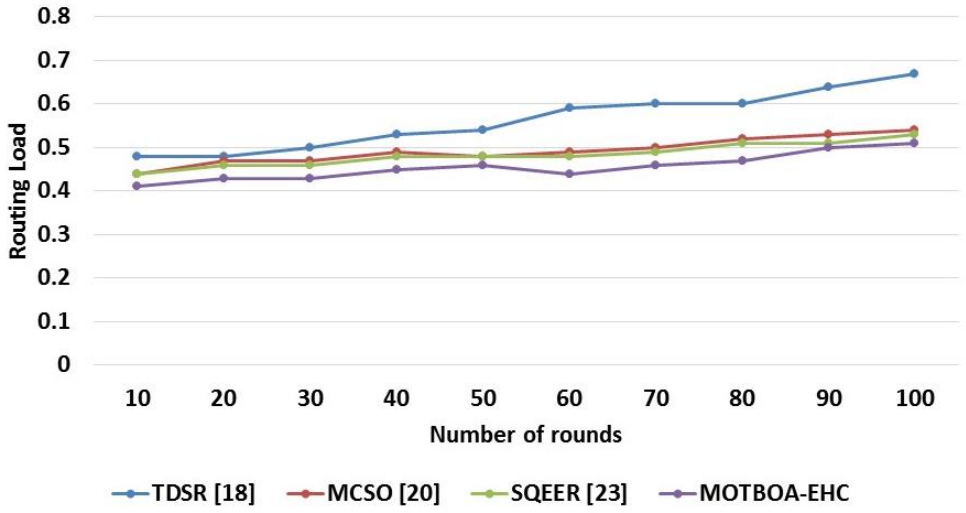


Figure. 5 Routing load

#### 4.1.4. Routing load

Routing load is explained as the ratio of the amount of routing messages created by the node to the number of data packets delivered successfully to all destination nodes is mentioned in Eq. (18).

$$Routing\ load = \frac{Y}{X} \tag{18}$$

Fig. 5 illustrates the comparative analysis of the TDSR [18], MCSO [20], SQEER [23] and MOTBOA-EHC method in term of routing load. Here, the routing load of the MOTBOA-EHC method is smaller when compared to the existing TDSR [18], MCSO [20] and SQEER [23]. Since the number of packets obtained in the destination node is increased, the routing load is minimized.

#### 4.1.5. Packet delivery ratio

PDR is characterized as the aggregate sum of packets received at the destination partitioned by the aggregate sum of packets send by the source node is mentioned in Eq. (19)

$$PDR = \frac{\sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} Y_i} \times 100\% \tag{19}$$

where, $X$ is denoted as number of packets received, $Y$ is denoted as number of packets send, $i$ is denoted as number of destination node and $n$ is denoted as amount of source nodes.

Fig. 6 illustrates the comparison between the TDSR [18], MCSO [20], SQEER [23] and MOTBOA-EHC method in term of PDR. Here, the proposed MOTBOA-EHC method provide better performance with the comparison of the existing

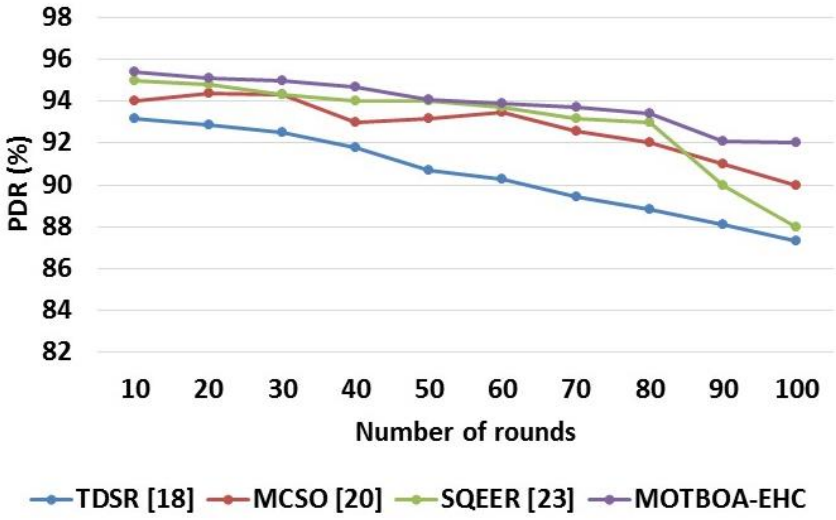


Figure. 6 Packet delivery ratio

Table 2. Comparative analysis of detection rate, delay & throughput for MOTBOA-EHC

| Number of rounds | Detection Rate (%) | | | | Delay (ms) | | | | Throughput (%) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | TDSR [18] | MCSO [20] | SQEER [23] | MOTBOA-EHC | TDSR [18] | MCSO [20] | SQEER [23] | MOTBOA-EHC | TDSR [18] | MCSO [20] | SQEER [23] | MOTBOA-EHC |
| 10 | 88.4 | 91.5 | 92.0 | 93.7 | 2 | 1 | 0.9 | 0.5 | 80.9 | 86.1 | 88.3 | 90.5 |
| 20 | 83.5 | 85.7 | 85.9 | 88.2 | 3 | 1 | 1 | 0.75 | 77.4 | 83.1 | 86.1 | 89.4 |
| 30 | 79.7 | 84.8 | 86.0 | 86.4 | 3 | 3 | 2 | 1 | 70.8 | 82.7 | 83.4 | 85.3 |
| 40 | 70.3 | 78.7 | 80.2 | 81.6 | 7 | 5 | 4 | 2 | 68.1 | 78.6 | 79.5 | 80.9 |
| 50 | 63.2 | 67.9 | 73.5 | 73.7 | 10 | 8 | 8 | 4 | 63.4 | 77.5 | 78.8 | 79.1 |
| 60 | 60.2 | 62.2 | 68.8 | 68.3 | 10 | 9 | 8 | 6 | 60.1 | 76.5 | 78.2 | 78.8 |
| 70 | 58.1 | 59.8 | 62.5 | 62.9 | 13 | 11 | 10 | 7 | 58.3 | 75.3 | 76.7 | 77.9 |
| 80 | 51.8 | 54.1 | 57.8 | 58.4 | 13 | 11 | 11 | 9 | 53.7 | 74.2 | 75.9 | 75.6 |
| 90 | 50.4 | 53.9 | 55.7 | 55.7 | 13 | 12 | 11 | 11 | 51.8 | 71.5 | 73.2 | 73.7 |
| 100 | 47.1 | 50.7 | 51.1 | 52.4 | 15 | 13 | 12 | 12 | 50.6 | 69.2 | 71.5 | 71.8 |

Table 3. Comparative analysis of routing load and PDR for MOTBOA-EHC

| Number of rounds | Routing Load | | | | PDR (%) | | | |
|---|---|---|---|---|---|---|---|---|
| | TDSR [18] | MCSO [20] | SQEER [23] | MOTBOA-EHC | TDSR [18] | MCSO [20] | SQEER [23] | MOTBOA-EHC |
| 10 | 0.48 | 0.44 | 0.44 | 0.41 | 93.2 | 94 | 95 | 95.4 |
| 20 | 0.48 | 0.47 | 0.46 | 0.43 | 92.9 | 94.4 | 94.8 | 95.1 |
| 30 | 0.50 | 0.47 | 0.46 | 0.43 | 92.5 | 94.3 | 94.3 | 95 |
| 40 | 0.53 | 0.49 | 0.48 | 0.45 | 91.8 | 93 | 94 | 94.7 |
| 50 | 0.54 | 0.48 | 0.48 | 0.46 | 90.7 | 93.2 | 94 | 94.1 |
| 60 | 0.59 | 0.49 | 0.48 | 0.44 | 90.3 | 93.5 | 93.7 | 93.9 |
| 70 | 0.60 | 0.5 | 0.49 | 0.46 | 89.4 | 92.6 | 93.2 | 93.7 |
| 80 | 0.60 | 0.52 | 0.51 | 0.47 | 88.8 | 92 | 93 | 93.4 |
| 90 | 0.64 | 0.53 | 0.51 | 0.5 | 88.1 | 91 | 90 | 92.1 |
| 100 | 0.67 | 0.54 | 0.53 | 0.51 | 87.3 | 90 | 88 | 92 |

TDSR [18], MCSO [20] and SQEER [23]. The PDR of the proposed method is improved by calculating the trust value of the nodes and communication cast through fitness function calculation.

The comparative analysis of MOTBOA-EHC for 100 nodes with the existence of DoS attack in WSN is shown in Table 2 and Table 3. In that, Table 2 shows the comparison data of detection rate, delay & throughput, and Table 3 shows the comparison data of routing load and PDR. From the analysis, it is concluded that the MOTBOA-EHC method achieves better performance than the TDSR [18], MCSO [20] and SQEER [23]. Similarly, the MOTBOA-EHC method gives better performance for the network with black hole attacks. The delay of the TDSR [18] and SQEER [23] is high because it generates the

routing path with a higher transmission distance. Next, the overhead of the MCSO [20] is high, due to its high amount of control packets transmitted during the communication. However, the optimal fitness functions of MOTBOA-EHC such as trust value, residual energy, communication cost, and node degree are used to improve the performance of the WSN. The two level security i.e., secure clustering and routing using MOTBOA and data security using EHC improves the PDR of the MOTBOA-EHC method.

## 5. Conclusion

In MOTBOA-EHC, the two-level security is developed by designing the secure clustering and routing using MOTBOA, and data security using EHC is used to improve the PDR of the network. The CH selection is performed according to the four fitness functions considered in this paper. The fitness functions are trust value, residual energy, communication cost, and node degree. The CH selection is performed by eliminating the attacker node in the cluster according to the trust value calculation. Hence, the network nodes are prevented from the DoS attack and black hole attack. The secured data transmission is obtained by encrypting the data which is transmitted through the nodes. The EHC method is utilized for the successful encryption and decryption operation in this paper. Finally, the simulation results of the MOTBOA-EHC method is obtained by using the NS2 tool. The MOTBOA-EHC method achieves better performance than the TDSR, MCSO and SQEER. The PDR of the MOTBOA-EHC method is 92 % at 100 rounds, it is high when compared to the TDSR, MCSO and SQEER.

## 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] 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.

[2] P. S. Khot and U. Naik, "Particle-Water Wave Optimization for Secure Routing in Wireless Sensor Network Using Cluster Head Selection", *Wireless Personal Communications*, pp. 1-25, 2021.

[3] S. G. Qureshi and S. K. Shandilya, "Novel Fuzzy Based Crow Search Optimization Algorithm for Secure Node-to-Node Data Transmission in WSN", *Wireless Personal Communications*, pp. 1-21, 2021.

[4] K. Haseeb, K. M. Almustafa, Z. Jan, T. Saba, and U. Tariq, "Secure and energy-aware heuristic routing protocol for wireless sensor network", *IEEE Access*, Vol. 8, pp. 163962-163974.

[5] A. Vinitha and M. S. S. Rukmini, "Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm", *Journal of King Saud University-Computer and Information Sciences*, 2019.

[6] S. Gorgich and S. Tabatabaei, "Proposing an Energy-Aware Routing Protocol by Using Fish Swarm Optimization Algorithm in WSN (Wireless Sensor Networks)," *Wireless Personal Communications*, pp. 1-21, 2021.

[7] 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, 2021.

[8] X. Ren, J. Li, Y. Wu, Y. Chen, H. Sun, and Z. Shi, "An enhanced energy optimization routing protocol for WSNs", *Annals of Telecommunications*, pp. 1-12, 2021.

[9] A. Nayyar and R. Singh, "IEEMARP-a novel energy efficient multipath routing protocol based on ant Colony optimization (ACO) for dynamic sensor networks", *Multimedia Tools and Applications*, Vol. 79, No. 47-48, pp. 35221-35252, 2020.

[10] H. A. Babaeer and S. A. A. Ahmadi, "Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking", *IEEE Access*, Vol. 8, pp. 92098-92109, 2020.

[11] D. N. Biradar and T. S. Vishanath, "Secured Data Transmission and Malicious Node Detection in Wireless Sensor Network", *International Journal of Engineering and Advanced Technology*, Vol. 8, No. 6, pp. 1062-1069, 2019.

[12] D. N. Biradar and T. S. Vishanath, "Mitigation of Selective Forwarding attacks in Wireless Sensor Network", *International Journal of Engineering and Advanced Technology*, Vol. 8, No. 6, pp. 4354-4358, 2019.

[13] S. Karthick, "TDP: A novel secure and energy aware routing protocol for wireless sensor networks", *International Journal of Intelligent Engineering and Systems*, Vol. 11, No. 2, pp. 76-84, 2018.

[14] W. Fang, W. Zhang, W. Yang, Z. Li, W. Gao, and Y. Yang, "Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks", *Digital Communications and Networks*, 2021.

[15] 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, 2020.

[16] 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, 2019.

[17] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal, and A. Arshad, "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 21, pp. 547-566, 2021.

[18] S. S. Moghaddam, H. Taheri, and A. Karimi, "Trust based routing algorithm to improve quality of service in DSR protocol", *Wireless Personal Communications*, Vol. 109, No. 1, pp. 1-16, 2019.

[19] 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.

[20] 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, 2020.

[21] T. A. Alghamdi, "Secure and energy efficient path optimization technique in wireless sensor networks using DH method", *IEEE Access*, Vol. 6, pp. 53576-53582, 2018.

[22] 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, 2019.

[23] 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, 2020.