Received: August 12, 2021. Revised: September 15, 2021.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Hybrid Optimization Algorithm and Shamir Secret Sharing Based Secure Data Transmission for IoT based WSN

Shilpa VenkataRao[1]* **Vidya Ananth[1]**

[1]*Department of Computer Science and Engineering, Vivekananda Institute of Technology, Bangalore, India*
* Corresponding author's Email: shilpavraghuram@gmail.com

Abstract: Nowadays, Wireless Sensor Networks (WSNs) are extensively utilized as the communication system in the Internet of Things (IoT). Security of the sensor nodes is considered as one of the important aspects of the IoT-based WSN because the nodes in the network are susceptible to malicious attackers. The main objective of this investigation is to generate secure routing and mutual authentication over the IoT-based WSN. In this paper, the Hybrid Optimization Algorithm (HOA) based secure Cluster Head (CH) selection and routing path generation is obtained for secure data transmission. The HOA is the combination of the Grey wolf optimization (GWO) and Moth Flame Optimization (MFO) whereas the fitness functions are trusted value, residual energy, distance and node degree. Additionally, the Shamir Secret Sharing (SSS) method is used for providing mutual authentication between the nodes. The performance of the HOA-IoT-WSN is analyzed in terms of Packet Delivery Ratio (PDR). Packet Loss Ratio (PLR), Average End-to-End Delay (AEED) and network overhead. An existing method such as Energy-efficient and Secure Routing (ESR) protocol, Hybrid Harris Hawk and Salp Swarm (HHH-SS), and Light Weight Trust Sensing (LWTS) methods are used to evaluate the proposed HOA-IoT-WSN method. The PDR of the HOA-IoT-WSN method is 99.848% for 100 nodes, it is high when compared to the ESR, HHH-SS and LWTS.

Keywords: Hybrid optimization algorithm, Internet of things, Packet delivery ratio, Shamir secret sharing method, Wireless sensor networks.

1. Introduction

Sensor networks that use both wireless and wired technology have attracted a lot of academic attention during the last few decades. The internet of things (IoT) is enormously developed for a diverse variety of sensor network applications which includes military, smart sensing, pollution sensing, undersea sensing, industrial and farming applications. Specifically, the applications of leakage detection, target tracking, intrusion detection, and fall detection are performed using the IoT [1-3]. A huge amount of nodes are installed in the IoT paradigm where each node performs monitoring, sensing, and processing operation based on connection and coverage [4]. IoT-enabled devices, such as computers, tablets, and smartphones, can access data about the environment and other things without the need for human participation [5-7]. While the internet of things' mission is to combine all types of sensing, communication, information management, and networking so that anybody may use any item or system. Sensors installed in a home, for example, may keep a person updated about any medical or security risks via mobile phone.

The wireless sensor network (WSN) is a critical component of IoT-enabled smart city applications. A WSN is a collection of wireless networks that are linked together to form a distributed network of autonomous devices [8, 9]. Sensors in WSN are movable, which means the sensor nodes can join or leave the network at any time. Because of the mobility nature of the sensor, security concerns related to malicious node intrusions are increased in the network [10]. There have been a number of technical problems with the WSN implementation for creating IoT applications, including battery life, transmission range, and processing capacity [11, 12].

Along with these restrictions, one of the most significant difficulties for WSN is to accomplish dependability while maintaining data security in a susceptible environment against hostile nodes [13] [14]. As a result, an efficient security method for identifying and mitigating rogue nodes from IoT-based WSNs that are utilized to decrease packet loss must be created. On the other hand, has created an optimization-based clustering and routing system to reduce sensor node energy usage [15]. The major contributions of this research paper are given as follows:

- Initially, the k-means clustering algorithm is used to divide the network into clusters. Next, the hybrid GWO-MFO (i.e., HOA) is used to select an appropriate CHs and to detect an appropriate routing path by using the four different fitness values such as trust value, residual energy, distance and node degree.
- The selection of CH and routing path avoids the malicious nodes which lead to minimizing the packet loss over the network.
- Additionally, the SSS method is used to provide mutual authentication for the nodes in the IoT-WSN.

The overall organization of the paper is given as follows: section 2 provides the related works according to the secure data transmission in the IoT-WSN. A detailed explanation about the proposed HOA-IoT-WSN is provided in section 3. Section 4 provides the results and discussion of the HOA-IoT-WSN method. The conclusion of this research paper is made in section 5.

2. Related work

Haseeb [16] developed an ESR protocol for IoT intrusion protection based on WSN. ESR improved the cluster head selection process and employed a dispersed strategy to produce clusters with uniform energy consumption distribution. Furthermore, the ESR protocol was utilized in conjunction with a lightweight secret sharing mechanism to enable safe network-wide data routing in the face of hostile nodes. The ESR was computationally secure, extendable in terms of network field expansion, and dynamic in terms of key changes. However, this ESR protocol did not take into account multi-hop network communication or mobility requirements.

Sheron [17] presented a decentralized scalable security architecture to improve the security of WSN-IoT communications. The tree-based hash is used for request authentication, and the framework's central authority–based security feature ensures device-level security, guaranteeing improved privacy and integrity in communications. The scalability characteristics were utilized to cut down on latency, calculation time, transaction costs, and energy consumption. The integrity of the forwarded messages was verified to keep the nodes from being overloaded. The complexity of request handling was enhanced by the sending of communication (control) bits.

Ghani [18] developed an improved symmetric key-based authentication mechanism for IoT-based WSN. The gateway node was used to execute the encryption and decryption. To assess the proposed protocol's security and performance, it was formally validated using ProVerif and BAN logic to ensure its correctness and key freshness. The user traceability, stolen verifier, and DoS threats were all defeated using this authentication mechanism. However, the developed symmetric key-based authentication mechanism was failed to analyze the QoS parameters.

Haseeb [19] introduced an energy-aware and secure multi-hop routing (ESMR) protocol for IoT-WSN using an XOR-based secret sharing method. The security between the clusters was achieved using this ESMR, which was produced using the k-nearest neighbors (k-NN) method. The ESMR was utilized to ensure energy efficiency and reliable transmission of data threats via secure intermediary nodes. However, the developed ESMR was not analyzed with mobile sensors.

Haseeb [20] developed interference prevention architecture to obtain safe routing in mobile IoT-WSNs. The mobile CHs with the least fluctuations in momentum were chosen by using the uncertainty principle. Furthermore, safe and reliable data routing was achieved using blockchain technology and a lightweight XOR hash function. The clustering over the network was utilized to reduce communication cost and routing overhead under high network size. However, the cluster head provided the high priority only to the residual energy.

Srinivas, M. and Amgoth, T [21] presented the HHH-SS algorithm for selecting the CH whereas the clustering over the network was performed by using the k-medoid clustering method. Next, an adaptive ant colony optimization was developed to discover the routing path from the source to the destination. Here, the delay between the nodes was calculated using internet protocol network. The developed HHH-SS was minimized the interference created by long distance communication and it supported secure data delivery by using single mobile sink. However, the data packets transmitted over the network was

susceptible to the malicious nodes, because the HHH-SS was failed to consider the node's trust value.

Prasad, M & Reddy, D [22] developed the light weight trust sensing (LWTS) method for routing over the IoT. In this LWTS, the node's trust was calculated by using different factors such as packet repetition factor, packet forwarding factor and packet consistency factor. Additionally, the trust calculation of LWTS was also included the indirect trust, therefore the calculated trust value was used to categorize an each neighbor node while generating the routing path. But, the developed LWTS was mainly concentrated only on node's rust value. For an effective route generation, the routing protocol also required to be considered some appropriate parameters such as hop count, distance and residual energy of the node.

3. HOA-IoT-WSN method

In this HOA-IoT-WSN method, a hybrid GWO and MFO method is used to select a secure CH and routing path for achieving reliable communication in the IoT-based WSN. The secure data transmission over the network is obtained by considering the trust value which helps to eliminate the black hole attack. Additionally, the residual energy, distance and node degree are considered in the hybrid GWO-MFO algorithm to minimize the packet loss while reducing the energy utilization of the nodes. Further, the mutual authentication between the nodes are obtained by generating the key from the SSS method. The mitigation of black hole attacks and mutual authentication using the SSS method helps to improve the data delivery over the IoT-based WSN. The flowchart for the HOA-IoT-WSN method is shown in Fig. 1.

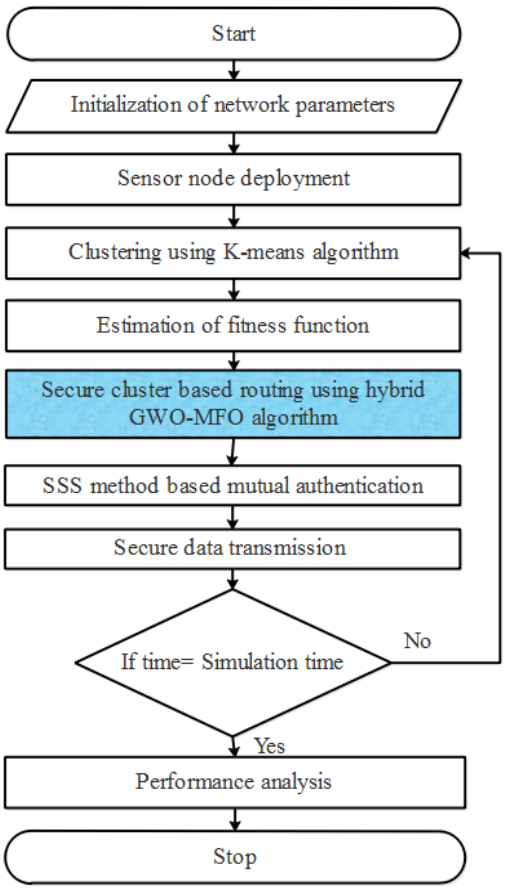

Figure. 1 Flowchart for the HOA-IoT-WSN method

3.1 K-means algorithm for the clustering process

The partition-based k-mean algorithm is a classification technique. The n number of samples are split into k number of subgroups in the k-mean technique. These clustering subgroups result in a high level of similarity inside the cluster. The k samples are randomly chosen from the data sets at first. The Euclidean distance between K centers and each sample is computed. The mean of the subgroups is then computed, resulting in a new clustering center. The new cluster center is generated using the k-means clustering method, which is dependent on the previous phases.

3.2 Overview of hybrid GWO and MFO

GWO is a novel metaheuristic method based on population. Grey wolves' hunting behavior and social order are modeled in this technique. The GWO algorithm's leadership hierarchy is characterized as alpha, beta, delta, and omega. GWO depends on the grey wolf behavior, in which a number of grey wolves in a pack travel across a multi-dimensional search space in pursuit of prey. Each individual's mobility is controlled by four processes such as exploration, encircling prey, hunting and exploitation.

3.2.1. Exploration

To look for a victim, the grey wolves separate from one another. To persuade the search agent to deviate from the victim, utilize $\vec{AM}$ with random values. Random weights are provided by the $\vec{CM}$ component when looking for prey in the search space. As a result of $\vec{AM}$ and $\vec{CM}$ the investigation, this algorithm can search the entire area. The $\vec{CM}$ vector also depicts the influence of incoming prey barriers. $\vec{AM}$ and $\vec{CM}$ are expressed as Eq. (1) and (2),

$$\vec{AM} = 2 \times \vec{a} \times \vec{r1} - \vec{a} \quad (1)$$

$$\vec{CM} = 2 \times \vec{r2} \quad (2)$$

where, $A\vec{M}$ and $C\vec{M}$ are coefficient vectors, the $r\vec{1}$ and $r\vec{2}$ are the generated random vectors between 0 and 1. $\vec{a}$ is reduced from 2 to 0 linearly.

3.2.2. Encircling prey

The locations of the three optimal wolves are used to update the location of the other wolves. The alpha, beta, and delta are used to evaluate the locations. $D\vec{M}$ is used to illustrate the encircling behavior. The following Eq. (3) express the anticipated border mathematically,

$$D\vec{M} = \left|C\vec{M}.X\vec{P}(t) - \vec{X}(t)\right| \tag{3}$$

where t represents the current iteration, prey's location vector is represented as $X\vec{P}(t)$ and grey wolf's location vector is represented as $\vec{X}(t)$.

3.2.3. Hunting

The grey wolf's recovery might be aided by the preservation of regional habitat connectivity. Here, the alpha wolves are used to accomplish the hunting process. Next, the beta and delta wolves are joined with the alpha wolves. It's difficult to forecast where the best prey is found. The gamma (i.e., candidate solution), beta and alpha wolf position is used to define grey wolf's hunting process which is represented in the Eq. (4), (5), (6).

$$\overrightarrow{DM_\alpha} = \left|C\overrightarrow{M_\alpha}.X\overrightarrow{P_\alpha}(t) - \vec{X}\right| \tag{4}$$

$$\overrightarrow{DM_\beta} = \left|C\overrightarrow{M_\beta}.X\overrightarrow{P_\beta}(t) - \vec{X}\right| \tag{5}$$

$$\overrightarrow{DM_\partial} = \left|C\overrightarrow{M_\partial}.X\overrightarrow{P_\partial}(t) - \vec{X}\right| \tag{6}$$

Further, the location of the different types of wolves are altered as shown in Eq. (7), (8), (9).

$$\overrightarrow{X_{\alpha 1}} = \overrightarrow{X_\alpha} - A\vec{M}1.\overrightarrow{DM_\alpha} \tag{7}$$

$$\overrightarrow{X_{\beta 1}} = \overrightarrow{X_\beta} - A\vec{M}2.\overrightarrow{DM_\beta} \tag{8}$$

$$\overrightarrow{X_{\partial 1}} = \overrightarrow{X_\partial} - A\vec{M}3.\overrightarrow{DM_\partial} \tag{9}$$

$$\overrightarrow{X(t+1)} = \frac{\overrightarrow{X_{\alpha 1}}+\overrightarrow{X_{\beta 1}}+\overrightarrow{X_{\partial 1}}}{3} \tag{10}$$

3.2.4. Exploitation

When the victim stops moving, the grey wolves attack it, putting an end to the hunt. The exploitation is determined by $\vec{a}$, where $A\vec{M}$ is a random number generated between the range of $[-2a, 2a]$. The position of alpha, beta, and delta wolves stated in the hunting stage and attack towards the prey is updated by search agents in GWO. The solution obtained from the GWO is further processed by using the moth flame optimization (MFO) algorithm.

The original MFO algorithm was inspired by the transverse orientation mechanism, which is a unique technique for moths to fly at night. It assists them in flying in a straight line by allowing them to maintain a constant angle with the distant moon. The flames reflect the moths' superior options and their associated positions. The moths are represented by matrix M as Eq. (11),

$$M = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1d} \\ m_{21} & m_{22} & \cdots & m_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{nd} \end{bmatrix} \tag{11}$$

where, the number of moths is represented as n and the number of dimensions is represented as d. The flames are represented by matrix F as Eq. (12),

$$F = \begin{bmatrix} f_{11} & f_{12} & \cdots & f_{1d} \\ f_{21} & f_{22} & \cdots & f_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n1} & f_{n2} & \cdots & f_{nd} \end{bmatrix} \tag{12}$$

where, the number of flames is represented as n and the number of dimensions is represented as d. Both moths and flames are solutions, while they use distinct updating mechanisms in the evolutionary process. Each moth is allocated to a single flame, and its location is updated via a spiral around that flame, as given in Eq. (13),

$$M_i = S\left(M_i, F_j\right) \tag{13}$$

3.3 Secure CH selection using hybrid GWO-MFO algorithm

The optimal sensor node as CH for each cluster is chosen using a hybrid GWO-MFO algorithm in this study. The data delivery is improved by selecting a secure optimal CH. Because the CH's responsibilities have expanded to encompass data aggregation and cluster management, all cluster members must designate a qualified node. The fitness values such as distance, node degree, residual energy, and trust value are used to select the CH.

3.3.1. Representation and initialization

In hybrid GWO-MFO, the group of sensor nodes that is required to select as CH is represented as

population. The amount of CHs is equal to the dimension (dim) of each population. At first, the location of each population is generated with the random node ID between 1 to N, where N is the number of sensor nodes deployed in the network. Consider, the i^{th} population is $X_i = (X_{i,1}(t), X_{i,2}(t), \dots, X_{i,dim}(t))$, where a location and each population $X_{i,z}(t), 1 \le z \le dim$ defines the node ID among the nodes in the network.

3.3.2. Fitness function calculation

The fitness function estimate is utilized to extend the network's lifespan by selecting the best CH from each cluster's nodes. The fitness functions utilized in CH selection include distance, node degree, residual energy, and trust value. The definition and derivation of fitness functions are given as follows:

a) Trust

The trust value of the nodes is considered as the main parameter in the fitness function of the hybrid GWO-MFO algorithm. Direct communication between the nodes is utilized for computing the trust value of the nodes. Specifically, the trust value is computed based on the forwarding ratio which is the ratio among the number of forwarded packets and the number of collected packets. Eq. (14) shows the expression for a trust value (FV_1) calculation.

$$FV_1 = \frac{T_{i,j}}{R_{i,j}} \tag{14}$$

where, $T_{i,j}$ and $R_{i,j}$ are the amount of forwarded and received packets between the node i and j.

b) Residual energy

One of the most essential variables to consider while choosing a CH is the residual energy of the nodes. Since the CH uses a lot of energy for data gathering, processing, transmission, and path selection, it consumes a lot of energy. The formula for calculating residual energy is shown in Eq. (15).

$$FV_2 = E_0 - E_c \tag{15}$$

The starting energy is denoted by E_0, while the energy used by the node is denoted by E_c.

c) Node degree

In next-hop selection, the node degree is a crucial element. If a low node degree is picked as the next hop, the node's performance is enduring for a long time and it gets little data from its members. As a result, the next–hop selected low node degree. Eq. (16) expresses the fitness function's node degree.

$$FV_3 = \frac{1}{\sum_{i=1}^{m} I_i} \tag{16}$$

where I_i is the amount of nodes in the i^{th} cluster.

d) Distance

It is the Euclidean distance (FV_4) between the nodes that exist in the IoT-based WSN. For effective data transmission, the distance should be considered during the communication. Because the energy utilization of the nodes is directly proportional to the distance. The energy consumption of the nodes is less when the transmission distance between the source and destination is less over the network.

The aforementioned fitness values aren't strongly conflicting with each other. Therefore, the multi-objectives are converted into a single objective by using the Eq. (17).

$$FV = \gamma_1 FV_1 + \gamma_2 FV_2 + \gamma_3 FV_3 + \gamma_4 FV_4 \tag{17}$$

where, $\gamma_1, \gamma_2, \gamma_3$ and γ_4 are the weighted values that is allocated for each fitness value. Therefore a secure optimal CH is selected from the clusters and CH has the responsibility to collect the information from the cluster members. The black hole attacker nodes are avoided during this CH selection based on the trust value. This leads to minimizing the packet loss during the data transmission. Additionally, the energy consumption is reduced by considering the node degree and distance values. The information about CH nodes is given as input for the routing process to generate the data transmission path.

3.4 Routing path generation using hybrid GWO-MFO algorithm

The generation of a near-optimal secure routing path is obtained by using a hybrid GWO-MFO algorithm. Similar to the CH selection, the routing process also considers the same fitness function. The process of routing using a hybrid GWO-MFO is explained in the following section.

3.4.1. Representation and initialization

In this phase, each population of the hybrid GWO-MFO denotes the possible transmission path between the source CH and the BS. Each population's dimension is equal to the number of CHs in the WSN. Consider, the i^{th} population is $X_i = (X_{i,1}(t), X_{i,2}(t), \dots, X_{i,dim}(t))$, where a location and

each population $X_{i,z}(t), 1 \leq z \leq dim$ defines the next hop CH of the data transmission path.

3.4.2. Route selection

The hybrid GWO-MFO utilizes the route request (RREQ), route reply (RREP), route error (RERR), and hello (HELLO) messages that are similar to the ad hoc on-demand distance vector routing protocol. The aforementioned control messages are used to generate the data transmission path. At first, the RREQ message is broadcasted by using the source CH at the route discovery process. Next, the CH which has a better fitness value sends the RREP message. Moreover, the key value is generated by using the SSS method and this key is included in the RREP message. The routing path is generated by transmitting the RREP message to the source CH over the reverse route. After accomplishing the mutual authentication between the nodes, the data is transmitted from the source CH to the BS. Furthermore, route maintenance is obtained by using the HELLO message.

3.5 Shamir's secret sharing method

The BS creates a secret key S that is separated across a collection of n CHs using (t, n) threshold based on the SSS method, where t subset of CHs is sufficient to recreate the secret key S. The following two requirements is should be required to satisfy the SSS method.

1. The secret key S can be reconstructed using any grouping of t or more subkeys $S_0,\ S_1, \dots,\ S_{t-1}$.
2. Reconstructing the secret key S with less than t or fewer subkeys is impossible.

A polynomial of $t-1$ degree is created in the SSS for the creation of t subkeys. $t-1$ random values $(b_1,\ b_2, \dots,\ b_{t-1})$ higher than zero are chosen to create a (t, n) threshold scheme. If $b_0 = S$, the coefficients of the polynomial are $(b_1,\ b_2, \dots,\ b_{t-1})$, as shown in Eq. (18)

$$f(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \cdots + b_t x^{t-1} \quad (18)$$

The lagrange basis polynomial must be computed to rebuild the secret keys S as given in Eq. (19).

$$l_j(x) = \prod_{\substack{0 \leq m \leq t \\ m \neq j}} \frac{x - x_m}{x_j - x_m} \quad (19)$$

Once the $t-1$ lagrange values is computed, Eq. (20) is used to compute the secret key S.

Table 1. Simulation parameters

Parameter	Value
Number of nodes	100, 200, 300 & 400
Area	100×100 m^2
Initial energy	5J
Packet size	512 Bytes
Antenna model	Omnidirectional
Network interface type	Phy/WirelessPhy
Propagation model	Two ray ground
Traffic type	CBR/ UDP
MAC protocol	IEEE 802.11
Routing protocol	Hybrid GWO-MFO
Simulation time	2000 s

$$f(x) = \sum_{j=0}^{t-1} y_i l_j(x) \quad (20)$$

Each cluster head receives a portion of the key S_i, which is then flooded to a single node in the cluster.

4. Results and discussion

The NS2 simulation tool is used for analyzing the performance of the HOA-IoT-WSN method. The HOA-IoT-WSN method is used to allow data transmission only among the authenticated nodes. Here, the simulation is carried out by varying the sensor nodes from 100 to 400. The nodes of the network are randomly located in the area of $100m \times 100m$, where the nodes used the hybrid GWO-MFO based routing protocol. The simulation parameters considered for this HOA-IoT-WSN method are provided in Table 1.

4.1 Performance analysis

The performance of the HOA-IoT-WSN method is evaluated using the four different metrics such as PDR, PLR and AEED and network overhead. Here, the proposed HOA-IoT-WSN method is compared with the ESR [16], HHH-SS [21] and LWTS [22] to shows its efficiency. In that, the existing methods such as ESR [16], HHH-SS [21] and LWTS [22] are compared based on the parameters available in its own analysis.

4.1.1. Packet delivery ratio

PDR is defined as the ratio between the amount of received packets and the amount of generated packets at the source. This PDR is expressed in the following Eq. (21).

$$PDR = \frac{Amount\ of\ received\ packets}{Amount\ of\ generated\ packets} \times 100 \quad (21)$$

The PDR comparison for the HOA-IoT-WSN method and ESR [16] is shown in Fig. 2. Additionally,

the Table 2 shows the comparison of PDR for the HOA-IoT-WSN method with ESR [16], HHH-SS [21] and LWTS [22], where the term NA indicates the parameters which are Not Available for the respective existing methods. From the analysis, it is concluded that the HOA-IoT-WSN method achieves high PDR compared to the ESR [16], HHH-SS [21] and LWTS [22]. However, the PDR of the HOA-IoT-WSN method is mainly improved by using the following two key strategies: 1) the black hole attacker node is avoided by considering the trust value in the clustering & routing phases, and 2) SSS method based mutual authentication between the nodes. Therefore the communication between the trusted nodes increases the PDR.

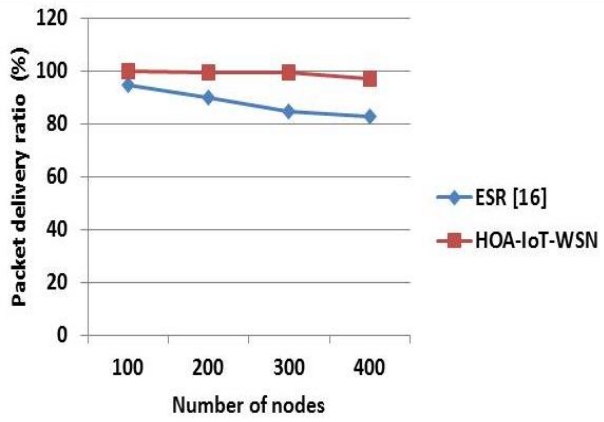

Figure. 2 Comparison of PDR

Table 2. Performance analysis of PDR

Number of nodes	ESR [16]	HHH-SS [21]	LWTS [22]	HOA-IoT-WSN
100	95%	81%	92%	99.848%
200	90%	78%	NA	99.6441%
300	85%	73%	NA	99.6193%
400	83%	69%	NA	97.3982%

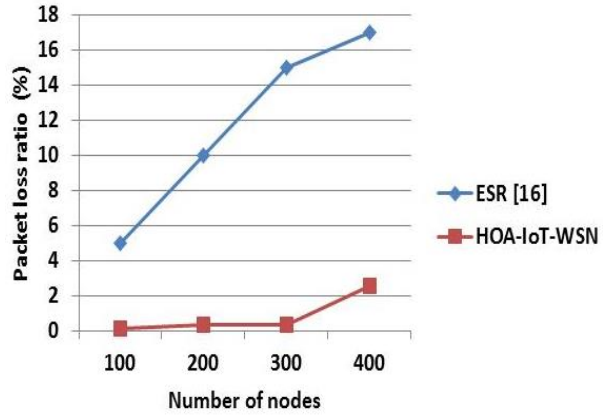

Figure. 3 Comparison of PLR

Table 3. Performance analysis of PLR

Number of nodes	ESR [16]	HHH-SS [21]	LWTS [22]	HOA-IoT-WSN
100	5%	7%	8%	0.151976%
200	10%	19%	NA	0.355872%
300	15%	27%	NA	0.380711%
400	17%	37%	NA	2.60181%

4.1.2. Packet loss ratio

PLR defines the amount of dropped packets in the communication phase. PLR is defined as the ratio among the amount of dropped packets by the amount of generated packets which is expressed in Eq. (22).

$$PLR = \frac{Amount\ of\ dropped\ packets}{Amount\ of\ generated\ packets} \times 100 \quad (22)$$

Fig. 3 show the comparison of PLR for ESR [16] and the HOA-IoT-WSN method. Similar to the PDR comparison, the Table 3 provides the PLR comparison of HOA-IoT-WSN method with ESR [16], HHH-SS [21] and LWTS [22]. The PLR of the HOA-IoT-WSN method is greatly minimized when compared to the ESR [16], HHH-SS [21] and LWTS [22]. For example, the PLR of the HOA-IoT-WSN is 0.38 % for 300 nodes which is less when compared to ESR [16], HHH-SS [21] and LWTS [22]. The PLR is minimized by avoiding the malicious nodes during the communication.

4.1.3. Average end to end delay

AEED is defined as an average time consumed by the packets forwarded from the source to the destination which is shown in Eq. (23). This AEED includes the processing time, queuing time, propagation delay, and transfer time.

$$AEED = \frac{Sum\ of\ all\ packets\ delay}{Total\ amount\ of\ received\ packets} \quad (23)$$

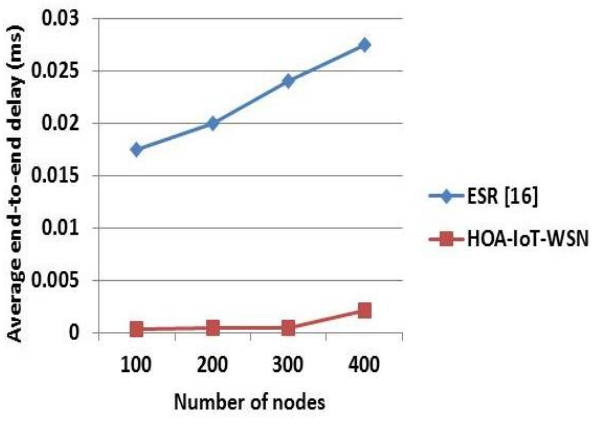

Figure. 4 Comparison of AEED

Table 4. Performance analysis of AEED

Number of nodes	ESR [16]	HOA-IoT-WSN
100	0.0175ms	0.000417088ms
200	0.02ms	0.000484898ms
300	0.024ms	0.000483543ms
400	0.0275ms	0.00217974ms

The AEED comparison for the HOA-IoT-WSN method and ESR [16] is shown in Fig. 4 and Table 4. From the analysis, it is concluded that the HOA-IoT-WSN method achieves less AEED compared to the ESR [16]. For example, the AEED for the HOA-IoT-WSN method with 300 nodes is 0.00048 ms, it is less when compared to the ESR [16]. The ESR [16] achieves higher AEED, because it failed to consider the multi-hop communication while transmitting the data packets. Meanwhile, the shortest path identification using HOA-IoT-WSN method helps to reduce the delay.

4.1.4. Network overhead

Network overhead is defined as an average amount of control packets created by each node during the communication.

Fig. 5 and Table 5 show the comparison of network overhead for ESR [16] and the HOA-IoT-WSN method. The network overhead of the HOA-IoT-WSN method is reduced when compared to the ESR [16]. For example, the network overhead of the HOA-IoT-WSN is 0.019 for 300 nodes, it is less when compared to ESR [16]. The network overhead of the HOA-IoT-WSN method is reduced by minimizing the control messages during the route discovery process.

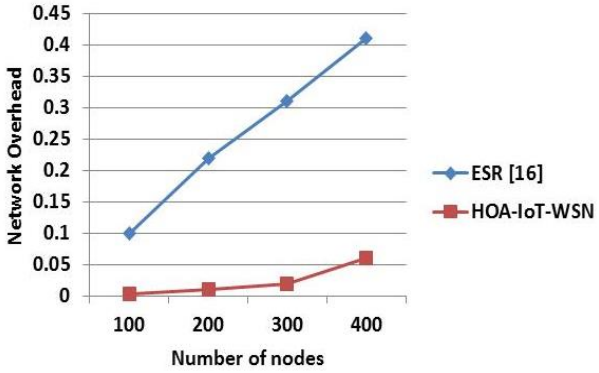

Figure. 5 Comparison of network overhead

Table 5. Performance analysis of network overhead

Number of nodes	ESR [16]	HOA-IoT-WSN
100	0.1	0.00465753
200	0.22	0.0108125
300	0.31	0.0192357
400	0.41	0.0605807

5. Conclusion

In this paper, the HOA-IoT-WSN method is used to select a near-optimal secure CH and secure data transmission path over the IoT-based WSN. The trust value considered in the hybrid GWO-MFO algorithm avoids the malicious nodes during the CH selection and routing path generation. The k-means-based clustering and hybrid GWO-MFO algorithm-based CH selection are used to improve the performances of the IoT-based WSN. Moreover, the hybrid GWO-MFO algorithm also identifies a secure transmission path to transmit the data packets from the source CH to the BS. The mutual authentication between the nodes in the IoT-based WSN is obtained by using the SSS method. Therefore, secure data transmission is obtained by using this HOA-IoT-WSN method. From the analysis, it is concluded that the HOA-IoT-WSN method provides better performance than the ESR, HHH-SS and LWTS. The PDR of the HOA-IoT-WSN method is 99.848 % for 100 nodes, which is high when compared to the ESR, HHH-SS and LWT. The performance of the IoT-WSN can be improved by using novel optimization algorithms.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The paper background work, conceptualization, methodology, dataset collection, implementation, result analysis and comparison, preparing and editing draft, visualization have been done by first author. The supervision, review of work and project administration, has been done by second author.

References

[1] A. Onasanya, S. Lakkis, and M. Elshakankiri, “Implementing IoT/WSN based smart Saskatchewan healthcare system”, *Wireless Networks*, Vol. 25. pp. 3999-4020, 2019.

[2] S. Sivakumar and P. Vivekanandan, “Efficient fault-tolerant routing in IoT wireless sensor networks based on path graph flow modeling with Marchenko–Pastur distribution (EFT-PMD)”, *Wireless networks*, Vol. 26, pp. 4543-4555, 2020.

[3] C. Iwendi, P. K. R. Maddikunta, T. R. Gadekallu, K. Lakshmanna, A. K. Bashir, and M. J. Piran, “A metaheuristic optimization approach for energy efficiency in the IoT networks”, *Software: Practice and Experience*, 2020.

[4] J. W. Lin, P. R. Chelliah, M. C. Hsu, and J. X. Hou, “Efficient fault-tolerant routing in IoT

wireless sensor networks based on bipartite-flow graph modelling", *IEEE Access*, Vol. 7, pp. 14022-14034, 2019.

[5] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand, and A. H. Gandomi, "An improved routing protocol for heterogeneous WSN for IoT-based environmental monitoring", *IEEE Internet of Things Journal*, Vol. 7, pp. 710-717, 2019.

[6] K. Thangaramya, K. Kulothungan, R. Logambigai, M. Selvi, S. Ganapathy, and A. Kannan, "Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT", *Computer Networks*, Vol. 151, pp. 211-223, 2019.

[7] B. D. Deebak and F. Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks", *Ad Hoc Networks*, Vol. 97, pp. 102022, 2020.

[8] S. S. L. Preeth, R. Dhanalakshmi, R. Kumar, and P. M. Shakeel, "An adaptive fuzzy rule based energy efficient clustering and immune-inspired routing protocol for WSN-assisted IoT system", *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-13, 2018.

[9] C. Lyu, X. Zhang, Z. Liu, and C. H. Chi, "Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of Things against DoS attacks", *IEEE Access*, Vol. 7, pp. 31068-31082, 2019.

[10] T. A. Alghamdi, "Convolutional technique for enhancing security in wireless sensor networks against malicious nodes", *Human-centric Computing and Information Sciences*, Vol. 9, pp. 1-10, 2019.

[11] I. Dohare and K. Singh, "PSO-DEC: PSO based deterministic energy efficient clustering protocol for IoT", *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 22, pp. 1463-1475, 2019.

[12] H. Farman, B. Jan, H. Javed, N. Ahmad, J. Iqbal, M. Arshad, and S. Ali, "Multi-criteria based zone head selection in Internet of Things based wireless sensor networks", *Future Generation Computer Systems*, Vol. 87, pp. 364-371, 2018.

[13] C. Miranda, G. Kaddoum, E. Bou-Harb, S. Garg, and K. Kaur, "A collaborative security framework for software-defined wireless sensor networks", *IEEE Transactions on Information Forensics and Security*, Vol. 15, pp. 2602-2615, 2020.

[14] D. Kim, J. Yun and D. Kim, "An Energy-Efficient Secure Forwarding Scheme for QoS Guarantee in Wireless Sensor Networks", *Electronics*, Vol. 9, pp. 1418, 2020.

[15] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand, and A. H. Gandomi, "Residual energy-based cluster-head selection in WSNs for IoT application", *IEEE Internet of Things Journal*, Vol. 6, pp. 5132-5139, 2019.

[16] K. Haseeb, A. Almogren, N. Islam, I. Ud Din, and Z. Jan, "An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN", *Energies*, Vol. 12, pp. 4174, 2019.

[17] P. F. Sheron, K. P. Sridhar, S. Baskar, and P. M. Shakeel, "A decentralized scalable security framework for end-to-end authentication of future IoT communication", *Transactions on Emerging Telecommunications Technologies*, p. e3815, 2019.

[18] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. N. Saqib, "Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key", *International Journal of Communication Systems*, Vol. 32, p. e4139, 2019.

[19] K. Haseeb, N. Islam, A. Almogren, I. U. Din, H. N. Almajed, and N. Guizani, "Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs", *IEEE Access*, Vol. 7, pp. 79980-79988, 2019.

[20] K. Haseeb, N. Islam, A. Almogren, and I. U. Din, "Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things", *IEEE Access*, Vol. 7, pp. 185496-185505, 2019.

[21] M. Srinivas and T. Amgoth, "EE‐hHHSS: Energy‐efficient wireless sensor network with mobile sink strategy using hybrid Harris hawk‐salp swarm optimization algorithm", *International Journal of Communication Systems*, Vol. 33, No. 16, p. e4569, 2020.

[22] M. Prasad and D. Reddy, "LWTSM-IoT: Light Weight Trust Sensing Mechanism for Internet of Things", *International Journal of Intelligent Engineering and Systems*, Vol. 14, No. 1, pp. 82-92, 2021.