Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.022126
Article

Tech Science Press

Secured Route Selection Using E-ACO in Underwater Wireless Sensor Networks

S. Premkumar Deepak* **and M. B. Mukeshkrishnan**

SRM Institute of Science and Technology, Kattankulathur, Chennai, 603203, India
*Corresponding Author: S. Premkumar Deepak. Email: premkumardeepak@gmail.com
Received: 28 July 2021; Accepted: 30 August 2021

Abstract: Underwater wireless sensor networks (UWSNs) are promising, emerging technologies for the applications in oceanic research. UWSN contains high number of sensor nodes and autonomous underwater vehicles that are deployed to perform the data transmission in the sea. In UWSN networks, the sensors are placed in the buoyant which are highly vulnerable to selfish behavioural attack. In this paper, the major challenges in finding secure and optimal route navigation in UWSN are identified and in order to address them, Entropy based ACO algorithm (E-ACO) is proposed for secure route selection. Moreover, the Selfish Node Recovery (SNR) using the Grasshopper Optimisation Algorithm (GOA) is used to minimize the packet loss in the UWSN. The performance of the proposed E-ACO method is compared with existing routing methods such as Secure Authentication with Protected Data Aggregation (SAPDA), Secure Energy Efficient and Cooperative Routing (SEECR), Fault Resilient Routing using Moth Flame Optimization (FRR-MFO) and Improved ACO (IACO) method. The packet delivery ratio of the proposed E-ACO with 500 nodes is 0.89 which is higher than other existing methods such as SAPDA, SEECR, FRR-MFO and IACO.

Keywords: Entropy based ant colony optimization; grasshopper optimisation algorithm; packet loss; secure routing; selfish node recovery; underwater wireless sensor network

1 Introduction

An underwater wireless sensor network is a technology that empowers and facilitates the exploration of natural resources in oceanic areas. Underwater sensor systems are a combination of wireless advancements with little micro mechanical sensor innovation having features such as smart identifying, intelligent computing, and communication capabilities [1,2]. Sensors are anchored to the base of sea and are furnished with a drifting buoyant that-can be swelled by strings. The buoyant controls the sensor towards the sea area [3]. The profundity of the sensor is managed by modifying the length of wire that associates the sensor to the stay, by means of an electronically controlled motor that resides on the sensor. The utilization of submerged sensors system is to investigate the regular assets in the oceanic conditions. Now a day, underwater applications are utilised to investigate and check the maritime conditions, such as

environmental observations, habitat monitoring, seismic detection, acoustic recognition, mechanical procedure checking, military observation, and terror threat identification [4–6]. The communication between the sensor nodes is highly preferred for use in acoustic communication. Generally, this sensor system gathers information from their environment and sends information to the shore base station or a ship by means of satellite communication or submerged links [7,8].

The transmission capacity of the acoustic channel is low [9]; subsequently the data rate is lower than the communication rate by transmitting the information to buoyant sensors nodes that hand-off the information to close by coastal observing and control station called remote station [10]. Here we use buoyant systems to place the sensors in the ocean. The buoyant nodes will be vulnerable to selfish behavioural attacks because of the high bit error rates, large and variable propagation delays, low transmission capacity of acoustic channels and the development of sensors with water flows. Selfish Nodes keep switching between good and bad behaviour over time, due to on and off attack [11,12]. The selfish behavioural node uses the complete system assets and the framework properties like vitality, and information transmission, for its own advantage [13]. When the networks fall into selfish behaviour attack, the data forwarding loss may occur which creates the problems in routing process. Considering the characteristics and applications of the acoustic networks, many algorithms have been developed to ensure the secure functioning of these underwater wireless sensor networks [14,15]. Moreover, the energy efficiency of the UWSN is considered as a main issue, because of the sensor nodes with limited battery capacity. The batteries of the sensor nodes are can't be replaced, since it is deployed in the harmful environment. So, it is required to develop a secure and energy aware routing protocol to obtain a reliable data transmission over the UWSN.

In the proposed method, the E-ACO is used to discover the secure route for secure data transmission. Moreover, the important contributions of this proposal using E-ACO are presented as follows: In E-ACO, the selection of secure path is performed by using five various fitness function values which are trust value, distance between sender and receiver, temperature of the ocean, depth of the ocean, and wind speed. The packet delivery of the E-ACO is effectively improved by considering the environmental factors of UWSN such as temperature of the ocean, depth of the ocean, and wind speed. Because these environmental factors are generally affects the communication over the UWSN. By considering these parameters, an effective data transmission path is obtained from the source to the destination. The secure routing path selection using E-ACO is achieved by considering the trust value for the fitness function. The energy consumption and average packet drops are minimized by considering distance as a fitness function value in E-ACO method. Next, the entropy value calculated in the UWSN is used to avoid the redundant data transmissions which additionally helps to minimize the energy consumption of the nodes. Moreover, the GOA based SNR is used to replace the selfish nodes with normal nodes to minimize the packet drop and increase the overall performance of the network.

The organization of the paper is mentioned as follow: Section 2 presents the literature review about the recent works related to secure routing technique in UWSN. From the literature review, the problem statement is identified which is presented in Section 3. Section 4 describes the basic information of the network. The secure path selection process by using E-ACO algorithm is described in Section 5. The performance analysis of the proposed E-ACO is detailed in Section 6. Lastly, the conclusion of the paper is presented in Section 7.

2 Literature Review

The existing approaches are divided into two types such as classical and swam intelligence based approaches which are described as follows:

2.1 Classical Approaches

Goyal et al. [16] presented the Secure Authentication with Protected Data Aggregation (SAPDA) method in order to improve the secure data transmission and Quality of Services (QoS) in the UWSNs. The SAPDA method also increases the data reliability in the UWSN by using the delay time and energy consumption of the network. The design of the SAPDA method was divided into two modules that are secure authentication and protected data aggregation which makes SAPDA method more complex. Saeed et al. [17] presented Secure Energy Efficient and Cooperative Routing (SEECR) Protocol to prevent the UWSN from the malicious attack. The SEECR protocol deals with energy consumption and security mechanism of the UWSN to protect the UWSN from the attacker. Cooperation method was used in the presented SEECR protocol order to utilize the multi-hop networking in UWSN. In the performance analysis, the SEECR protocol was compared with Adaptive Mobility of Courier Nodes in Threshold-optimized DBR (AMCTD) routing protocol. In SEECR technique, the increment of the node consumes high energy compared to AMCTD, which is an important issue of SEECR method.

Murgod et al. [18] presented cluster based wormhole attacks detection and reduction technique in UWSNs environments. Energy Efficient Hybrid Optical-Acoustic Cluster Based Routing (EEHRC) Protocol was used to detect the presence of wormhole attack and prevent the UWSN from the attack. As per the comparison of the performance, the EEHRC protocol did not reduce the considerable amount of energy consumption of the UWSN which is the main disadvantage of the EEHRC protocol. Prasanth [19] presented the Energy-efficient Fault detection and Recovery Management (EFRM) method for selfish node detection and recovery of the secure data transmission in UWSNs. The EFRM method utilized the hidden poisson markov model to improve the performance of the fault node detection. After selection process, the recovered sensor node is selected by analytical based network model that enables to restore the large number of sensor nodes from malicious environment. While transmitting the data, the EFRM did not address the error control technique which became a drawback of the EFRM method. Ali et al. [20] presented cooperative, reliable, and stability-aware routing protocol for secure data transmission in UWSNs. The author presented two different types of protocol which are (i) stability-aware and stability based routing protocol and (ii) co-operative reliable with stability- aware based routing protocol. These two methods perform proper energy optimization of the transmission as well as define the secure routing. The presented routing protocol had more amount of alive nodes for finding the secure and energy optimized path for data transmission.

Muthukkumar et al. [21] presented dynamic Bayesian game based on trust strategy for secure data transmission in underwater acoustic sensor networks. The author introduced the trust strategy based dynamic Bayesian game (TSDBG) technique to identify the secure path among the nodes in the underwater acoustic sensor networks. In the data transmission, the packet dropping and malicious activities of the network were calculated by trust and payoff of each sensor node. Every normal node frequently monitors the activity of their neighbor node based on payoff and trust value. Energy consumption of the network was not properly optimized by the TSDBG method which became a drawback in this paper. Katya et al. [22] introduces the GEDAR steering convention for secure path detection in UWSNs. Moreover, some of the buoyant nodes may be in void area which is identified by the GEDAR to change the geographical location for transmitting the information packets to the destination hubs. The execution speed of the network was improved by using GEDAR conventions which is compared with conventional submerged defeating convention in terms of various parameters such as energy efficiency and packet data compression. The focus was only on the void node detection and secure path detection. The important performance parameters such as QoS, life time of network, arrival time from source to destination were not sufficiently handled and this became a disadvantage for the method.

2.2 Swarm Intelligence Based Approaches

Kumari et al. [23] presented Moth Flame Optimization (MFO) technique based on fault resilient routing protocols for the UWSNs. These problems made the network more vulnerable to security threats. To solve this problem, the MFO based fault resilient routing method transfers the information from sensor node to base station by using Autonomous Underwater Vehicles (AUV). The performance of the proposed model was compared with various types of algorithms such as AUV based method, and EECOR. The energy consumption of the network was not reduced enough, which is a disadvantage of the MFO based fault resilient routing protocols. Xiao et al. [24] presented the Improved ACO (IACO) method to develop energy-efficient clustering routing algorithm. Accordingly, the network was separated into many clusters where an each cluster has one Cluster Head Node (CHN) and numerous cluster member nodes. The selection of CHN was optimized by considering the distance factor and residual energy of the nodes. Further, the IACO was used to generate the transmission path from the CHN to the destination. Hence, the combination of single and multi-hop transmission were used to minimize the energy consumption. However, there was a lack in appropriate fitness function selection which affects the routing performances. Khan et al. Reference [25] developed the Dragon Fly Optimization (DFO) to accomplish the routing optimization. An optimal amount of clusters were obtained by using the DFO in the adaptive node clustering protocol. The fitness functions considered in the cluster head selection were load balance and average distance of the sensors. This work was failed to analyze the residual energy and packet delivery ratio of the UWSN. However, this DFO was performed only single hop routing which leads to increase the energy consumption of the nodes.

3 Problem Statement

Recent problems faced in UWSN are described in this section which also explains how the proposed E-ACO technique presents the way to solve the problems of UWSN.

The path selection for data transmission in the underwater sensor network is an important function which must be considered while developing UWSNs. Similarly, in SAPDA [16], more priority was given to design a secure network by using clustering based structure. Moreover, the SAPDA method consumes high energy to perform the transmission operation due to its highly complex structure. The SEECR [17] method did not perform the recovery operation of the node from the malicious node. The fault resilient routing–MFO [23] technique executed secure path selection in the UWSN by using optimization technique. The energy consumption and selfish node recovery was not considered as an important factor while designing the network which is a problem of the MFO technique.

Solution

This study shows that the malicious node detection and malicious recovery is an important problem in UWSNs. To avoid this, there are five fitness functions considered such as trust value, temperature of the ocean, depth of the ocean, distance between the nodes and wind speed. These fitness values are used to select a secure path for secure data transmission. The Entropy based ACO with the five fitness functions enables the selection of secure route for data package transmission. In this E-ACO, the SNR using GOA is used to improve the packet delivery ratio during the communication.

4 System Model

This section provides the basic information about the network and energy model to be taken in this E-ACO technique.

4.1 Network Model

UWSN is a wireless communication system used to communicate in underwater environment. The UWSN system has some important parts which are sensor nodes in the underwater, water surface gateway and wireless base station. Each of the sensor nodes in the network has the ability to sense, compute and transmit the collected information. The collected data is transmitted to the surface gateway by using the multiple relay nodes that are just normal sensor nodes. The water surface gateways act as hub of the acoustic wireless communication network. The base station in the land remotely controls the sensor nodes by controlling the gateway on the surface of the water. Some of the sensor nodes in the network can be attacked by the malicious user whose motive is to drop the packets which are transmitted in the network. Fig. 1 shows the sample structure of the UWSN model.

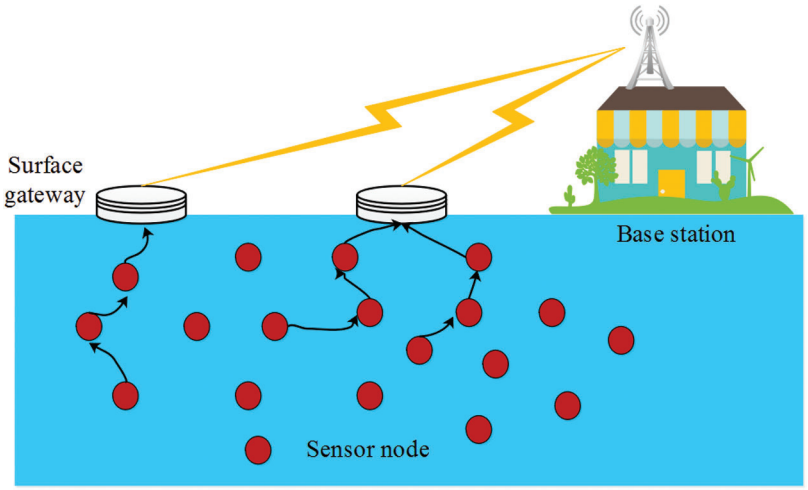

Figure 1: Illustration of the sample structure of UWSN

4.2 Energy Model

The energy consumption of the network is an important factor which to be considered in the process of wireless communication networks. Eq. (1) represents the energy model of the underwater communication networks. $E_1(m, d_1)$ denotes the energy of a node which transmits m bits of data to the d_1 distanced node. The energy consumption for the transmission in particular node is,

$$E_1(m, d_1) = mE_{elec} + mT_1 TL_{loss}(d_1) \tag{1}$$

where, T_1 represents transmission time of single bit information, TL_{loss} specifies the propagation loss and E_{elec} denotes the energy utilization of the transmitter circuit processing the single bit information.

The receiver node's energy utilization (E_r) and fusion energy utilization (E_m) for single bit data are calculated by using Eqs. (2) and (3).

$$E_r(m, d_1) = mE_{rece} \tag{2}$$

$$E_m(m, d_1) = mE_m \tag{3}$$

Here, energy utilization for receiver circuit processing of single data information is denoted as E_{rece}.

5 Proposed Work

In this proposed method, EACO is proposed for optimal route selection for the secure data transmission in UWSN. Entropy is calculated based on the information provided by the sensor nodes such as trust value, distance between two nodes, temperature, wind speed and depth in the ocean. By considering the trust value in the fitness function, the malicious nodes are avoided during path selection. The distance, wind speed, depth of the ocean are considered to select the shortest path to minimize the energy consumption for the operation of the network as well as to minimize the death rate of sensor nodes. Moreover, the GOA based SNR is used to minimize the packet loss by replacing the selfish nodes. The block diagram of the E-ACO technique is presented in the Fig. 2.

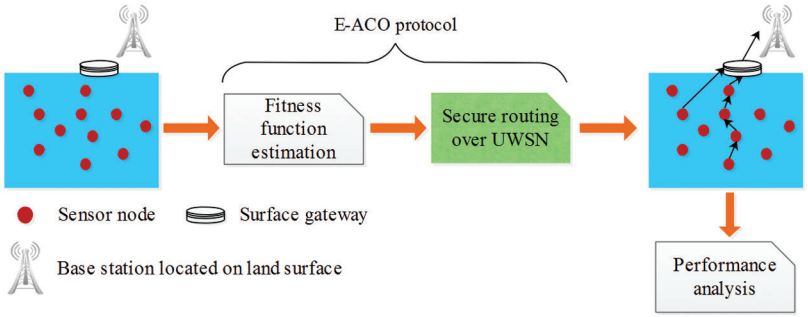

Figure 2: Block diagram for E-ACO protocol

5.1 Selfish Behavioural Analysis

Initially, the sensors are deployed in the underwater scenario, where the base station is located in the land surface which used to receive and analyze the data received from the sensor nodes. In UWSN directing the ship in right path is challenging due to lack of information provided by the sensor nodes for factors such as temperature, humidity, wind speed and wind direction, rainfall, depth and location etc. The E-ACO based routing is used to perform secure and effective data transmission under the constraints of selfish nodes. This information plays a vital role in ship navigation, detection in node failures. In UWSN, selfish behaviour attack is considered as one of the major issue. Due to selfish behavioural node, the data communication between remote station and ship is disrupted in the UWSN. Because the selfish nodes exist in the network may spoof the normal sensor nodes during communication. These selfish node causes the packet loss as well as it performs unauthorized access over the UWSN. Additionally, GOA is used to perform the selfish node recovery, where the selfish nodes are replaced by using the normal nodes. This helps to improve the packet delivery ratio.

5.2 Ant Colony Optimization

The Ant Colony optimization (ACO) is a routing algorithm which is developed by mimicing the behaviour of Ant colony to find the secure route to destination. Generally, an ant family finds the secure and shortest path to their food sources from the rest.

5.2.1 Initialization

The ACO algorithm can be applicable for discrete problems which can be a network with N number of nodes and L number of links. In the network, each and every node has a minimum number of artificial ants and every link in the network is related with a weight. The distance between nodes or random number is considered as the initial weight of network's link. The node transition rule is presented in Eq. (4), which is used to calculate the probability of choosing minimum distanced node (j) as a next node from current node (i). The node transition formula is,

$$P_{ij}^{k}(t) = \begin{cases} \frac{[\tau_{ij}(t)]^{\alpha}[\eta_{ij}]^{\beta}}{\sum len_k [\tau_{ij}(t)]^{\alpha}[\eta_{ij}]^{\beta}} & if\ j \in \mathcal{N}_k \\ 0 & otherwise \end{cases} \tag{4}$$

Here, τ_{ij} is denoted as intensity of pheromone and η_{ij} is denoted as heuristic value. α and β are called as parameters which are used to control the τ_{ij} and η_{ij}. $\mathcal{N}_k$ is defined as the set of nodes, that ant k consumes not yet visited.

5.2.2 Pheromone Update Rule

The artificial ants are developed which are inspired by the nature ants and their food searching technique. If a sensor node needs to send the information to a particular endpoint, the artificial ants select the next node to be used for transmission, by using the node transition formulae and store the visited node's information in their storage. When the information or the ant successfully reach the destination terminal, the pheromone update formula is used to update the pheromone value of the link to retrace the same route to its source node. This rule contains reinforcement of pheromone and evaporation of pheromone which are used to increase or decrease the pheromone values of the link to make the ant travel front and back, respectively. Hence, the ant discovers the shortest route from the source node to the destination. The formula for the pheromone update rule is given in Eq. (5).

$$\tau_{ij}^{new} = (1-\rho)\tau_{ij}^{old} + \sum_{k=1}^{m} \Delta_{ij}^{k} \tag{5}$$

where, m denotes total number of ants, coefficient of the pheromone decay is represented as $\rho \in (0,1)$. $\Delta\tau_{ij}^{k}$ is total number of pheromone laid by ant k in between links i, j. The expression for $\Delta\tau_{ij}^{k}$ is shown in Eq. (6).

$$\Delta\tau_{ij}^{k} = \begin{cases} \frac{Q}{f_k} & if\ the\ kth\ ant\ traversed\ link\ (i,j) \\ 0 & otherwise \end{cases} \tag{6}$$

Here, Q is denoted as constant value, f_k is defined as cost function.

The process of routing using E-ACO is stated as follows:

1. For an each sensor node, the ant is allocated and the route is generated from the source node to the sink. The source node generates some route setup packets which are denoted as forward ant packets.
2. The generated forward ant packets are randomly broadcasted to the successive node by using the probability matrix. This process is sustained until the forward ant packets collected by the sink.
3. Each packet has the information about the node which they visited, trust value, distance between sender and receiver, temperature of the ocean, depth of the ocean, and wind speed.
4. If the path is extended to sink, the forward ant's database creates the backward ant packet. Next, the backward ant broadcasts in the same path that is used for forward ant packet transmission.
5. Next, the pheromone value is updated for an each path by using the fitness function such as trust value, distance between sender and receiver, temperature of the ocean, depth of the ocean, and wind speed which are defined in the following section.
6. Finally, the node selects the next hop for data transmission based on the node transition rule given in the Eq. (4).

5.3 Fitness Function Derivation

The fitness factor is important factor to find the secure path for secure communication in the UWSN. The fitness factor improves the efficiency and integrity of the wireless communication network. In the proposed

method, the fitness function is formulated depending on trust values and distance between sensor nodes to destination node is selected to enable secure data transmission.

5.3.1 Trust Value Calculation

The general expression for the trust value calculation is given in Eq. (7).

$$F(t) = F_1(t) + F_2(t) + F_3(t) + F_4(t) \tag{7}$$

Here, $F_1(t)$ represents the direct trust which is based on deviation in the estimated time and actual time. The expression to calculate direct trust value is represented in Eq. (8). $F_2(t)$ is defined as indirect trust value which is given in Eq. (9). (t) represents the recent trust which is calculated by taking the node regression of $F_1(t)$ and $F_2(t)$ of the sensor node in the UWSN. The mathematical notation for recent trust is given in Eq. (10). $F_4(t)$ represents the trust value based on data bytes which is calculated based on total amount of data bytes transmitted from the source node to the total amount of the data bytes received by the terminal node. The mathematical notation for the trust based data bytes is represented in Eq. (11).

$$F_1(t) = \frac{1}{3}\left[F_1(t)(t-1) = \left[\frac{T^{key} - E^{key}}{T^{key}}\right] + w\right] \tag{8}$$

$$F_2(t) = \frac{1}{N}\sum_{i=1}^{N} F_2(t)(x) \tag{9}$$

$$F_3(t) = \alpha \times F_1(t) + (1-\alpha) \times F_2(t), \quad \text{where, } \alpha = 0.3 \tag{10}$$

$$F_4(t) = \frac{1}{2} \times \left[\frac{\partial_{i,j}^{i}}{d} + \frac{\partial_{i,j}^{j}}{d}\right] \tag{11}$$

where, T^{key} is the appropriate time needed to transmit the key, E^{key} is the predictable time to receiving the key, x is the jth destination witness factor, N is the total number of neighbour nodes, $\partial_{i,j}^{i}$ is the Total amount of transmitted data bytes by the source node, $\partial_{i,j}^{j}$ is the total amount of received bytes by the receiver node and d is the information packet limit for transmitting and receiving the data.

5.3.2 Temperature

The temperature of the node is considered in the fitness function of ACO routing. Because the UWSN environment was affected because of the high temperature gradient. Specifically, the temperature of the upper surface of the sea is higher than the bottom surface.

5.3.3 Distance Between Two Nodes

The Euclidean distance between the two nodes is used as a one of the fitness functions which helps to find the data transmission path with less distance. This helps to minimize the energy consumption of the nodes. The distance between the transmitter and receiver node is calculated by using Eq. (12).

$$D = \sqrt{(x_1 - y_1) + (x_2 - y_2)} \tag{12}$$

where, the position of node '1' is (x_1, y_1); the position of node '2' is (x_2, y_2). D is considered as a fitness function.

5.3.4 Wind Speed

The speed of wind (v) is considered as one of the fitness functions which is calculated by using Eq. (13). The performance of the sensor node may affected by the wind speed. Specifically, the sound velocity of the acoustic signal is affected, when the wind speed is higher than the 7 m/s.

Hence, wind speed is considered as one of the trust values.

$$V = \sqrt{\frac{2q}{p}} \tag{13}$$

Here, q defined as pressure of wind and p is defined as density of air.

5.3.5 Depth

Depth (H) is an important aspect that influences the overall performance of underwater network system. Hence, the depth of the ocean is considered for fitness function. The Depth of the ocean is denoted as H.

The overall fitness function is calculated by using weighted sum approach which is shown in Eq. (14)

$$f_k = a_1F(d) + a_2T + a_3D + a_4V + a_5H, \quad \text{here} \quad a_i \in (0, 1) \tag{14}$$

where, a_1, a_2, a_3, a_4, a_5 are considered as 0.3, 0.25, 0.15, 0.1, 0.2 respectively. The Eq. (14) is considered as cost function of ACO which is used to update Pheromone value shown in Eq. (6). In these fitness functions, the trust value is considered as primary factor as the sensor nodes are tried to spoof by selfish node. Therefore, the selfish nodes in the network are prevented while generating the data transmission path which leads to minimize the packet loss of the UWSN. Since, the essential environmental factors such as temperature, wind speed and depth creates the great impact over the underwater acoustic data transmission. Therefore, the E-ACO is considered these environmental factors to generate an optimal routing path according to the communication environment. Meanwhile, the distance is considered as one more fitness function in the E-ACO method to generate the transmission path with less distance. Because, the energy consumption of the sensor nodes are highly dependent on the transmission distance of the routing path.

5.4 E-ACO for Optimal Route Selection

In UWSN, the sensors nodes are placed in the buoyant based upon the geographical area. The geographical information about the active and inactive sensor nodes is reported to the nearby base station. Based on the collected information from the nodes, the ship is navigated through the optimized route.

In Eq. (6), the f_k is replaced by the Eq. (14), and amount of Pheromone deposited in the path is given in Eq. (15).

$$\Delta\tau k_{i,j} = \frac{Q}{a_1F(d) + a_2T + a_3D + a_4V + a_5H} \tag{15}$$

where, $\Delta\tau k_{i,j}$ is the amount of Signal which is received by the kth node. Q is a constant parameter (Consider $Q = 1$). The $\Delta\tau k_{i,j}$ is used to update cost function for updating the pheromone in Eq. (5). The pheromone updated value is used to find the routing path for the data transmission in the network. After identifying the transmission path, the entropy value is calculated during the data transmission. Further, the Entropy value is calculated for saving the energy from the redundant transmissions. Specifically, the entropy is the average amount of received data and the following Eq. (16) is used to calculate the entropy value.

$$Entropy = -\sum_{j=1}^{|I_j|} I_j \log_2(I_j) \tag{16}$$

where, the evaluation which monitor the redundant transmission is represented as I_j and the total amount of values received from the UWSN area is $|I_j|$.

E-ACO Algorithm

1. **Input:** Set pheromone and heuristic exponential weight.
2. Generate an initial ant population.
3. **for** j = Maximum number of iterations
4. **for** each ant in the ACO.
5. Repeat until *k*th ant finishes the tour to the sink node.
6. Use Eq. (4) for selecting the next hop ant.
7. Use Eq. (5) for updating the pheromone value.
8. **end for**
9. Update the optimal solution.
10. **end for**
11. **Output:** Secure and optimal route from the source to the sink node.
12. Entropy is calculated using Eq. (16) for avoiding the redundant transmissions.

5.5 Selfish Node Recovery Using GOA

In this E-ACO method, the GOA based SNR is used to replace the selfish nodes using the normal nodes for improving the data transmission over the UWSN. The GOA is used in this E-ACO, due to its high convergence performance. The replacement of selfish nodes with normal nodes is helps to improve the performance of the UWSN. Here, the grade diffusion algorithm is used to generate the grade value for all the nodes in the UWSN. In this SNR algorithm, the threshold value (ST) is computed for replacing the selfish nodes as shown in Eq. (17). The selfish nodes are replaced by using the functional nodes chosen by using the GOA, when the ST is higher than zero.

$$ST = \sum_{i=1}^{\max(Grade)} T_i T_i = \begin{cases} 1, & \frac{N_i^{now}}{N_i^{original}} < \beta \\ 0, & otherwise \end{cases} \tag{17}$$

where, the grade value of the sensor node is T_i; the number of nodes and number of functioning nodes with grade value i are represented as $N_i^{original}$ and N_i^{now} respectively. Here, the parameter β is selected between the value of 0 and 1. The ST is higher than zero and T_i becomes 1, when the amount of sensor nodes which function for an each grade is lesser than the β. This grade value is used to compute the amount of sensor nodes which required to be replaced using the GOA.

Generally, the GOA is inspired by the migration of grasshopper over the larger distance and it is designed by the Saremi et al. [26]. The important motivation of the GOA is the features of the two

swarming behaviours such as larval and adulthood. The process of replacement of malicious node using the GOA is mentioned as follows:

1. The nodes in the UWSN broadcasts the event data to the destination node. Subsequently, the threshold value is calculated by using the Eq. (17).
2. The initialization process of GOA is accomplished, when the value of ST is greater than zero. Then the population of the GOA is initialized with the sensor node ID along with its coordinates (x, y).
3. GOA is used to choose the normal nodes for replacing the selfish nodes found from the network.
4. The main aim of using GOA based SNR is to reuse the most data transmission path and replaces the selfish nodes. This GOA is used to calculate the number of selfish nodes which required to be changed in the UWSN. The fitness function derivation is shown in the Eq. (18).

$$Fit = \sum_{i=1}^{\max(Grade)} \frac{P_i \times TP^{-1}}{N_i \times TN^{-1}} \times i^{-1} \tag{18}$$

where, the amount of replaced sensors are N_i; the amount of re-usable routing paths from sensors with grade value i is P_i; total amount of sensors and routing paths in the UWSN are TN and TP respectively. The GOA provides the grasshopper (*i.e.*, respective selfish node ID) with the best fitness value. Further, the SNR replaces the selfish nodes using the normal nodes to minimize the packet drop in the UWSN.

6 Experimental Results and Discussion

The implementation and simulation of E-ACO algorithm based path selection is performed by using Network simulation-2 (NS2) software which is operated on Windows 7 operation system with Intel core i3 processor and 4GB RAM. Here, 1000 m × 1000 m area is utilized to simulate E-ACO algorithm and 1000 sensor nodes are randomly placed in the area. The simulation parameters for NS2 software that were considered for performing E-ACO is given in the Tab. 1.

Table 1: Parameters used in E-ACO

Name of parameter	Values for parameters
Number of nodes	1000
Time span taken	100 s
Traffic Source	CBR
Traffic rate	50 Kbps
Attacker	1 to 10
Propagation	Two ray ground
Antenna	Omni Antenna
Initial energy	10000 J
Transmission power	2.0 W
Receiving power	0.75 W

The performance of the E-ACO based routing is calculated by means of the delay, Delivery ratio, average packet drop, average energy consumption, first node die and half node die. The E-ACO based

routing protocol is compared with four various methods such as SAPDA [16], SEECR [17], FRR-MFO [23] and IACO [24] in terms of the same parameters mentioned in Tab. 1.

6.1 Packet Delivery Ratio

Packet delivery ratio is defined as ratio between numbers of packages received by the receiver and number of packages sent by the source node. The packet delivery ratio directly represents the efficiency of the overall network which is given in Eq. (19).

$$Packet\ delivery\ ratio = \frac{number\ of\ packages\ received}{number\ of\ packages\ transmitted} \tag{19}$$

Fig. 3 represents the packet delivery ratio for E-ACO protocol and other methods such as SAPDA [16], SEECR [17], FRR-MFO [23] and IACO [24]. The packet delivery ratio of the E-ACO method is higher than the SAPDA [16], SEECR [17], FRR-MFO [23] and IACO [24]. Basically, the malicious node in the network drops the transmitting data packets from one node to another. In the proposed E-ACO, the secure path is selected by replacing the malicious node using GOA based SNR. The malicious node detection is performed by considering the trust value for the fitness function. Hence, the packet delivery ratio is increased when compared with other existing SAPDA, SEECR and FRR-MFO method.

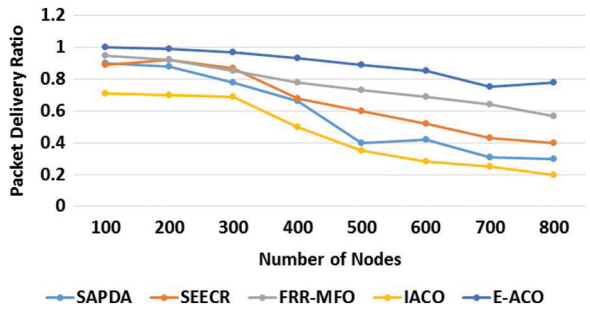

Figure 3: Performance analysis of packet delivery ratio for E-ACO method

6.2 Delay

Delay or End to End delay is defined as total number of time taken for the data package to be sent through a network from source node to destination node. The mathematical expression of the delay is given in Eq. (20).

$$D = \frac{\sum(received\ time - sending\ time)}{\sum number\ of\ links} \tag{20}$$

Here, D is defined as delay.

Fig. 4 represents the delay for E-ACO protocol with other methods such as SAPDA [16], SEECR [17], FRR-MFO [23] and IACO [24]. The delay of the E-ACO method is lower than the SAPDA [16], SEECR [17], FRR-MFO [23] and IACO [24]. The lower delay value is achieved by considering the distance of the node using fitness functions by which, the shortest path from source to destination is determined. The shortest path from the source sensor node to the destination decreases the delay time of the underwater network.

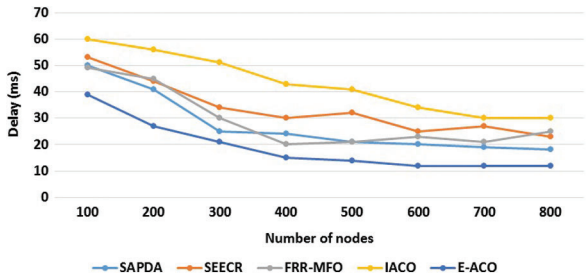

Figure 4: Performance analysis of delay for E-ACO method

6.3 Average Packet Drop

In the transmission, some of the data packets are dropped by routing nodes or sensor node due to the limitation of buffer or overflow of information in the network. The mathematical equation for average packet drop or loss is given in Eq. (21).

$$average\ packet\ drop = \frac{Z - Y1 - Y2}{Z} \tag{21}$$

Here, Z is represented as number of packet send by the sensor node, $Y1$ denoted as total number of received packets and $Y2$ represents total amount of recovered packets

Fig. 5 represents the average packet drop for E-ACO protocol with other methods such as SAPDA [16], SEECR [17], FRR-MFO [23] and IACO [24]. The average packet drop of the E-ACO method is lower than the SAPDA [16], SEECR [17], FRR-MFO [23] and IACO [24]. The E-ACO method consider the trust value in the fitness function which select secure path to transmit the information to the destination. The secure path or malicious free path obtained using the GOA based SNR decreases the packet loss in the transmission.

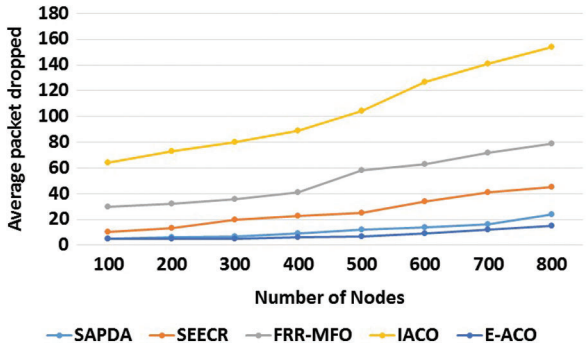

Figure 5: Performance analysis of average packet drop for E-ACO method

6.4 Average Energy Consumption

The energy consumption of the network is defined as the total energy utilized by the network to perform the data transmission operation. The mathematical expression for the average energy consumption is given in Eq. (22).

$$E = \sum_{i=1}^{N} energy\ for\ TX_i + Energy\ for\ RX_i + Idle\ energy_i \tag{22}$$

Here, N is denoted as total number of sensor nodes, transmission energy is defined as Tx, received energy is defined as Rx.

Fig. 6 represents the comparison for average energy consumption for E-ACO protocol with other methods such as SAPDA [16], SEECR [17], FRR-MFO [23] and IACO [24]. The average energy consumption of the E-ACO method is lower than the SAPDA [16], SEECR [17], FRR-MFO [23] and IACO [24]. The energy consumption of the sensor node is dependent on the distance between nodes, depth of the ocean, temperature of the ocean and wind speed of the ocean. In the E-ACO method, the distance, temperature, wind speed and depth are considered as fitness functions that decrease the energy consumption of the network.

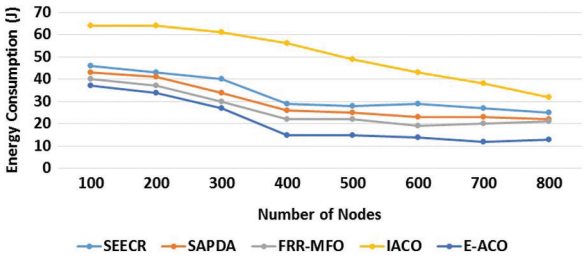

Figure 6: Performance analysis of average energy consumption for E-ACO method

6.5 Node Death Rate

There are two types of death nodes in the network known as First node die and half node die. Basically, the death node is defined as the ratio between energy exhausted sensor node and total amount of sensor nodes. The sensor node crossing the below 1% of the energy level in the battery is called as dead sensor node.

Fig. 7 represents the note death rate for E-ACO protocol and other methods such as SAPDA [16], SEECR [17], FRR-MFO [23] and IACO [24]. The death rate of the E-ACO method is lower than the SAPDA [16], SEECR [17], FRR-MFO [23] and IACO [24]. From Fig. 7, the E-ACO method based routing achieves low amount of death node by considering the distance between nodes, depth of the ocean, temperature, and wind speed as the fitness functions. Lower death rate improves the overall performance of the network.

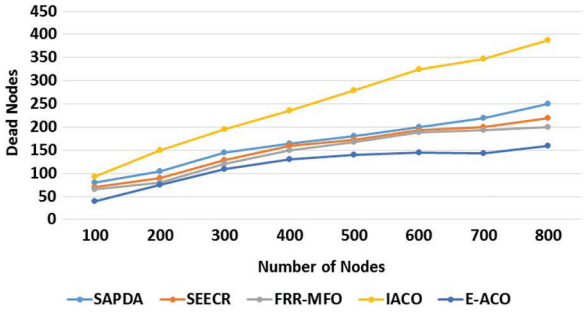

Figure 7: Performance analysis of node death rate for E-ACO method

The performance of the proposed E-ACO is better than the existing SAPDA [16], SEECR [17], FRR-MFO [23] and IACO [24] methods. The better performance of the E-ACO is achieved by considering the trust value, distance between nodes, death of the ocean, wind speed and temperature as the values of fitness function. By considering the trust value for fitness function, the packet delivery ratio and death

rate were minimized the most, by implementing the proposed method rather than the existing approaches. The secure, energy optimized and lower transmission time are all achieved using the proposed method by considering distance, temperature, depth, wind speed and trust value as the fitness functions. Moreover, the GOA based SNR is used to replace the selfish nodes with normal nodes for improving the PDR while transmitting the data packets over the UWSN. Hence, the overall performance of the network is increased in the proposed E-ACO method.

7 Conclusion

Analysing the optimal route path in underwater wireless sensor networks is a major challenge for the ships to get directions for a hazard free sea route. In the proposed method, the fitness functions considered for the E-ACO are five various factors known as trust value, distance between node, temperate of the ocean, depth of the ocean and wind speed. The main contributions are identification of the selfish node and providing optimal route selection mechanism to ships using E-ACO method. In order to find secure path for the data transmission, the trust value is considered in the fitness function which helps to identify the behaviour of the sensor node. The GOA based SNR is used to recover the selfish nodes by replacing the selfish nodes with normal nodes. The performance of the E-ACO method is compared with various methods that are SAPDA, SEECR, FRR-MFO and IACO. From the performance analysis, the proposed provides better result in packet delivery ratio, energy consumption, average packet drops and node death rate. The average packet delivery ratio of the E-ACO method is 0.90 which is very high compared with SAPDA, SEECR, FRR-MFO and IACO methods.

In future different approaches such as integration of numerous sink nodes and portability setting of sensors in dense environments should be examined, which are considered as an enormous challenge in remote sensor organize.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Roy and N. Sarma, "Effects of various factors on performance of MAC protocols for underwater wireless sensor networks," *Materials Today: Proceedings*, vol. 5, no. 1, pp. 2263–2274, 2018.

[2] N. Javaid, S. Hussain, A. Ahmad, M. Imran, A. Khan *et al.,* "Region based cooperative routing in underwater wireless sensor networks," *Journal of Network and Computer Applications*, vol. 92, no. 2, pp. 31–41, 2017.

[3] W. Ge, K. Sun, Y. Yao, L. Liu, L. Luo *et al.,* "Numerical simulation on the deploying and recovering process for a node of underwater wireless sensor network," in *Proc. IEEE OCEANS*, Shanghai, pp. 1–4, 2016.

[4] R. M. Gomathi and J. M. L. Manickam, "Energy efficient static node selection in underwater acoustic wireless sensor network," *Wireless Personal Communications*, vol. 107, no. 2, pp. 709–727, 2019.

[5] R. Shakila and B. Paramasivan, "Performance analysis of submarine detection in underwater wireless sensor networks for naval application," *Microprocessors and Microsystems*, pp. 103293, 2020. https://doi.org/10.1016/j.micpro.2020.103293.

[6] G. Han, H. Wang, S. Li, J. Jiang and W. Zhang, "Probabilistic neighborhood location-point covering set-based data collection algorithm with obstacle avoidance for three-dimensional underwater acoustic sensor networks," *IEEE Access*, vol. 5, pp. 24785–24796, 2017.

[7] S. Rani, S. H. Ahmed, J. Malhotra and R. Talwar, "Energy efficient chain based routing protocol for underwater wireless sensor networks," *Journal of Network and Computer Applications*, vol. 92, no. 6, pp. 42–50, 2017.

[8] N. Kanthimathi, "Void handling using geo-opportunistic routing in un R. derwater wireless sensor networks," *Computers & Electrical Engineering*, vol. 64, no. 4, pp. 365–379, 2017.

[9] M. Faheem, R. A. Butt, B. Raza, H. Alquhayz, M. W. Ashraf *et al.,* "FFRP: Dynamic firefly mating optimization inspired energy efficient routing protocol for internet of underwater wireless sensor networks," *IEEE Access*, vol. 8, pp. 39587–39604, 2020.

[10] S. Sahana and K. Singh, "Cluster based localization scheme with backup node in underwater wireless sensor network," *Wireless Personal Communications*, vol. 110, no. 4, pp. 1693–1706, 2020.

[11] G. Yang, L. Dai, G. Si, S. Wang and S. Wang, "Challenges and security issues in underwater wireless sensor networks," *Procedia Computer Science*, vol. 147, no. 4, pp. 210–216, 2019.

[12] K. Vijayan, G. Ramprabu, S. S. Samy and M. Rajeswari, "Cascading model in underwater wireless sensors using routing policy for state transitions," *Microprocessors and Microsystems*, vol. 79, no. 3, pp. 103298, 2020.

[13] T. Dargahi, H. H. Javadi and H. Shafiei, "Securing underwater sensor networks against routing attacks," *Wireless Personal Communications*, vol. 96, no. 2, pp. 2585–2602, 2017.

[14] G. Han J.Jiang, L. Shu and M. Guizani, "An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network," *IEEE Transactions on Mobile Computing*, vol. 14, no. 12, pp. 2447–2459, 2015.

[15] X. Li, Y. Zhou, L. Yan, H. Zhao, X. Yan *et al.,* "Optimal node selection for hybrid attack in underwater acoustic sensor networks: A virtual expert-guided bandit algorithm," *IEEE Sensors Journal*, vol. 20, no. 3, pp. 1679–1687, 2019.

[16] N. Goyal, M. Dave and A. K. Verma, "SAPDA: Secure authentication with protected data aggregation scheme for improving QoS in scalable and survivable UWSNs," *Wireless Personal Communications*, vol. 113, no. 1, pp. 1–15, 2020.

[17] K. Saeed, W. Khalil, S. Ahmed, I. Ahmad and M. N. K. Khattak, "SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks," *IEEE Access*, vol. 8, pp. 107419–107433, 2020.

[18] T. R. Murgod and S. M. Sundaram, "Cluster based detection and reduction techniques to identify wormhole attacks in underwater," *Wireless Sensor Networks*, vol. 11, no. 7, pp. 58–63, 2020.

[19] A. Prasanth, "Certain investigations on energy-efficient fault detection and recovery management in underwater wireless sensor networks," *Journal of Circuits, Systems and Computers*, vol. 30, no. 8, pp. 2150137, 2020.

[20] M. Ali, A. Khan, H. Mahmood and N. Bhatti, "Cooperative, reliable, and stability-aware routing for underwater wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 15, no. 6, pp. 1550147719854249, 2019.

[21] R. Muthukkumar and D. Manimegalai, "Secured transmission using trust strategy-based dynamic bayesian game in underwater acoustic sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 2585–2600, 2021.

[22] E. Katya and S. R. Rahman, "Void node detection and packet re-routing in underwater wireless sensor network," *International Journal of New Practices in Management and Engineering*, vol. 9, no. 4, pp. 1–10, 2020.

[23] S. Kumari, P. K. Mishra and V. Anand, "Fault resilient routing based on moth flame optimization scheme for underwater wireless sensor networks," *Wireless Networks*, vol. 26, no. 2, pp. 1417–1431, 2020.

[24] X. Xiao and H. Huang, "A clustering routing algorithm based on improved ant colony optimization algorithms for underwater wireless sensor networks," *Algorithms*, vol. 13, no. 10, pp. 250, 2020.

[25] M. F. Khan, M. Bibi, F. Aadil and J. W. Lee, "Adaptive node clustering for underwater sensor networks," *Sensors*, vol. 21, no. 13, pp. 4514, 2021.

[26] S. Saremi, S. Mirjalili and A. Lewis, "Grasshopper optimisation algorithm: Theory and application," *Advances in Engineering, Software*, vol. 105, pp. 30–47, 2017.