Energy-efficient intrusion detection system for secure acoustic communication in under water sensor networks

N. Nithiyanandam[1*], C. Mahesh[2], S.P. Raja[3], S. Jeyapriyanga[4] and T. Selva Banu Priya[5]
[1*]Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamilnadu, India
[e-mail: nnithi81@gmail.com]
[2]Department of Artificial Intelligence and Machine Learning, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu, India
[e-mail: chimahesh@gmail.com]
[3]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamilnadu, India
[e-mail: avemariaraja@gmail.com]
[4]Department of Information Technology, St.Joseph's Institute of Technology, Semmenchery, Chennai, India
[e-mail: priyankashanmugam16@gmail.com]
[5]Department of Artificial Intelligence and Data Science, Panimalar Engineering Collège, Poonamalle, Chennai, Tamilnadu, India
[e-mail : priya8517@gmail.com]
[*]Corresponding author: N. Nithiyanandam

Received July 15, 2022; revised September 26, 2022; revised December 20, 2022; revised April 2, 2023; accepted May 9, 2023; published June 30, 2023

Abstract

Under Water Sensor Networks (UWSN) has gained attraction among various communities for its potential applications like acoustic monitoring, 3D mapping, tsunami detection, oil spill monitoring, and target tracking. Unlike terrestrial sensor networks, it performs an acoustic mode of communication to carry out collaborative tasks. Typically, surface sink nodes are deployed for aggregating acoustic phenomena collected from the underwater sensors through the multi-hop path. In this context, UWSN is constrained by factors such as lower bandwidth, high propagation delay, and limited battery power. Also, the vulnerabilities to compromise the aquatic environment are in growing numbers. The paper proposes an Energy-Efficient standalone Intrusion Detection System (EEIDS) to entail the acoustic environment against malicious attacks and improve the network lifetime. In EEIDS, attributes such as node ID, residual energy, and depth value are verified for forwarding the data packets in a secured path and stabilizing the nodes' energy levels. Initially, for each node, three agents are modeled to perform the assigned responsibilities. For instance, ID agent verifies the node's authentication of the node, EN agent checks for the residual energy of the node, and D agent substantiates the depth value of each node. Next, the classification of normal and malevolent nodes is performed by determining the score for each node. Furthermore, the proposed system utilizes the sheep-flock heredity algorithm to validate the input attributes using the optimized probability values stored in the training dataset. This assists in finding out the best-fit motes in the UWSN. Significantly, the proposed system detects and isolates the malicious nodes with

http://doi.org/10.3837/tiis.2023.06.010 ISSN : 1976-7277

tampered credentials and nodes with lower residual energy in minimal time. The parameters such as the time taken for malicious node detection, network lifetime, energy consumption, and delivery ratio are investigated using simulation tools. Comparison results show that the proposed EEIDS outperforms the existing acoustic security systems.

Keywords: Intrusion Detection System, Under-Water Sensor Networks, Energy-Efficient Standalone Intrusion Detection System, Wireless Sensor Network.

1. Introduction

Marine research is an ever-inspiring paradigm in the oceanographic studies for the past few decades. Many innovations have been brought in military applications, surveillance, and resource exploration by harnessing acoustic communications [1, 2]. Due to the advent of sensor networks and digital technology, monitoring the ocean ecosystem equips biological observations to make better decisions needed for coastal environments [3]. Besides, Under Water Wireless Sensor Networks (UWSN) provides a better solution by exploring a vast ocean environment. It helps analyze the data underneath the water surface by deploying a network of self-powered autonomous sensor motes. Typically, the surface sink nodes are intended to gather and transfer the under-water phenomena to the control station for further analysis (**Fig. 1**).

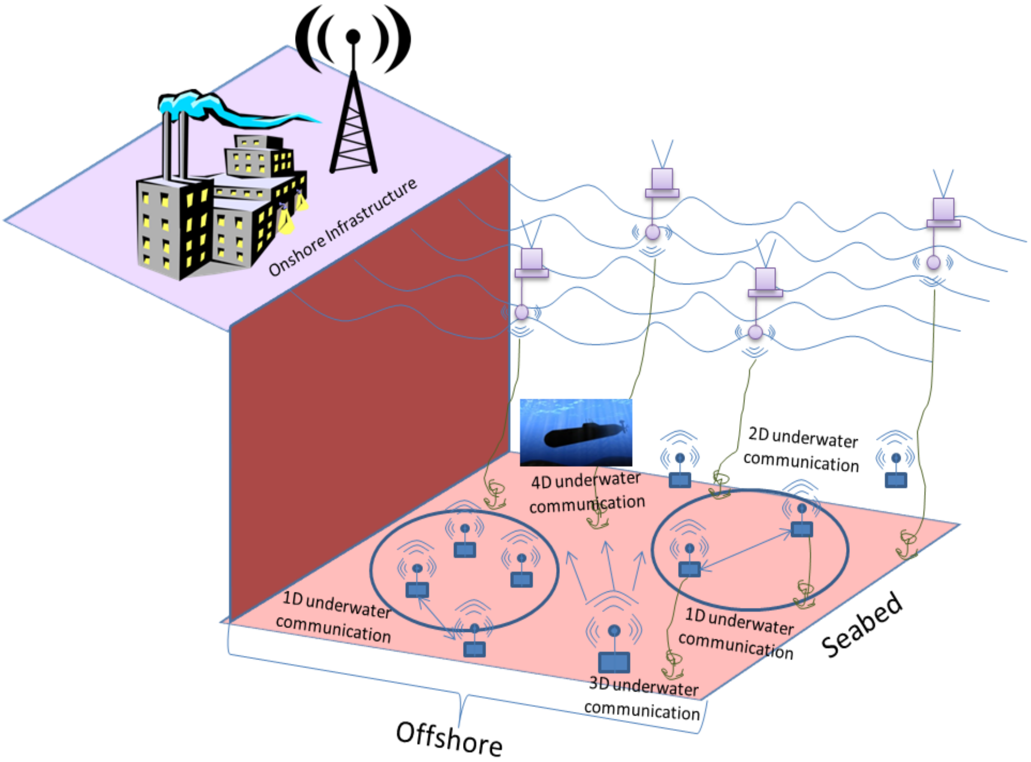
Onshore Infrastructure
4D underwater communication
2D underwater communication
1D underwater communication
1D underwater communication
3D underwater communication
Seabed
Offshore

Fig. 1. Under Water Sensor Networks

UWSN effectively does the exploration of ocean environments. Genuinely, UWSN helps in performing intelligent tasks such as disaster prediction, smart sensing, marine creatures monitoring, navigation, and target tracking. Despite this, some of the incompetence in carrying out long-haul communication persists. It is mainly due to high bit-error-rate, lower bandwidth, and node mobility. Consecutively, reduced dissemination of the radio waves, passive node mobility, and fading are some of the existing challenges. Battered by these factors, UWSN is now becoming a primary target of malicious attacks.

Customarily, the attacks in UWSN [4] are classified into two major categories: adversarial attacks on sensors and attacks on network protocols. The dominant intruder's influx to compromise the sink node is often encountered in UWSN. Since tampering the underwater sensor nodes is a complex task for the intruders due to its sparse deployment. On the other hand, puzzling the network protocols is occurring deliberately to halt acoustic communication and ruin the UWSN. Existing research for combating the sinkhole attacks [5, 6] majorly faced in the underwater environment is still sparse. Alternatively, the frequent replacement of batteries is more tedious due to the harsh aquatic environments. UWSN seeks abundant power requirements due to the exemptions like node battery backup, energy consumption, and replacement cost. Hence, the mechanism to patronize the stabilization of the energy levels needs to be addressed. To provide better energy efficiency and security, a novel IDS is modeled. The contributions of this proposed work comprise of two parts:

a) Firstly, the sheep-flocky heredity algorithm [7] for IDS is propounded to optimize the authenticated nodes. Here, validation of the nodes is performed for secure communication in the UWSN by fizzling out the malicious nodes, b) Secondly, the nodes' residual energy and depth information of individual nodes are gathered and validated in order to comply with the energy balancing targeted at enhanced network lifetime [8].

Initially, the information such as Node ID, Residual energy, and depth information of each node is collected and broadcasted. The score value is calculated for each node based on the authentication ID, high residual energy, and smaller depths by utilizing the collected information. Upon every transmission, the score values get validated, and new values are determined. In the proposed system, the sensor nodes retain the data packet for a considerable time. After ensuring the score of the neighboring node, the data packets are allowing for multi-hop communication. Hence, the sensor motes with high scores participate in the network, and bared sensors are ignored due to the reduced likelihood of participation.

The rest of the paper is organized as follows. In section 2, various existing approaches that address energy constraints, security vulnerabilities in UWSNs, and countermeasures are explored. In section 3, the proposed EEIDS for secured underwater communication is described in detail. Section 4 presents the performance evaluation of the proposed system, and finally, the conclusion and future works end the paper.

2. Related Works

This section investigates some of the existing mechanisms that address the security concerns and energy constraints in UWSN. We surveyed exploring enhanced security approaches and energy conservation practices for UWSN. In [9], the authors addressed the problem of applying security during the deployment stage itself. They have suggested that efficient protocols be designed in the network architecture to defend the UWSNs. Also, they have put forth some analysis impact of various attacks in wired underwater sensor networks. Followed by them, an experimental approach done by Habib et al. [10] provides a better analysis of the effects of active attacks in UWSN using OPNET simulator. As a useful measure, various security mechanisms are designed by various researchers. However, those approaches need some particularities such as coverage, residual energy, authentication, and depth values are taken into consideration. A node coverage mechanism for UWSN in a 3D space is formulated in [11]. The authors suggest a stochastic and probabilistic approach for determining the coverage area of k nodes. The feature of network coverage as per the study lags due to the dense deployment of nodes. Generally, energy is a measure that plays a significant role in UWSNs as it is a primary factor for every data transmission.

Various approaches have been suggested for reducing the energy consumption in networks. The authors have proposed a practical framework in [12] to limit the duplicate and redundant transfers to save energy in the underwater sensor network. In [13], a 3D based clustering model is designed for minimal energy consumption and reduced resource utilization in the event of target tracking performed in underwater environments. Consecutively in [14], energy harvesting mechanisms are designed focusing on energy-efficient acoustic communication. Many depth adjustment strategies are made in previous researches. In [15] algorithm for adequate depth-adjustment is explored using the dominating node as the depth node. It effectively sends the data to the sink with a reduced packet loss. Likewise, a moving node algorithm is suggested in [16] in which exploits water force to conserve power. It also acts as a recycle measure to get back the fatal nodes. Later [17] presents a joint approach for providing optimality in determining the depth node. Some IDS schemes proposed [18-20] provides the effective detection of malicious nodes for defending the underwater sensor networks.

A novel floating three-dimensional sensor network for ocean monitoring and surveillance application is proposed [34] which leverage nodes restricted movement to enlarge the monitoring area. Due to harsh ocean environment. it is difficult to deploy ocean sensor networks for ocean monitoring and surveillance. A new cost-efficient scheme is proposed [35] that claims, compared with deployments requiring self-adjusted nodes. Sanjana palisetti et.al [36] discusses about the application of UWSN on the area such as costal defense, pollution monitoring and secure communication. The scenario of multiple applications [37] sharing the same physical infrastructure is presented which allows the infrastructure to fully exploit the network resources. PengSun et.al discussed the challenges associated [38] with underwater wireless networking. UWSN enables new opportunities [39, 40] for exploration of the oceans. Military and security forces see the potential of using UWSN for mine reconnaissance, intrusion detection and surveillance.

3. Energy-efficient intrusion detection system (IDS) for secure communication in UWSN

Bemusing attacks in the UWSN are increasing exponentially due to the lack of security mechanisms to deal with 3D space and a plethora of deployment strategies [21]. Also, in most of the marine applications, USWN is neither indemnifying due to the replacement cost and sparse deployment [22]. Also, underwater sensor nodes are randomly anchored either statically or dynamically, and the portion of to-be-monitored remains unclear. To meet the challenges, the proposed system outlooks a strategy to perform the Intrusion Detection System greener and securer. In this paper, we address the increasing number of transmissions and unfortunate disruptions due to attackers often encountered in UWSN. We have divided the proposed system into three subdivisions: Node Deployment, Attacker detection using a sheep-flock algorithm, and Data forwarding via a secured energy-efficient path.

3.1 Node deployment

In the node deployment phase, the nodes take their positions in x, y, and z axes in 3D space in where they are anchored. The deflection in the nodes' position mostly occurred due to the dynamism with the waves while observing the underwater phenomenon. Hence, each sensor's depth is assumed to the length of the wire in which it gets anchored from the surface. The depth values are then stored and broadcasted among the neighboring nodes and finally inform the surface sink for further analysis. Typically, the depth value is required for the sink node to achieve the coverage ratio of the UWSN [27]. Let us consider that the sensor nodes are deployed in a cuboid region with the volume of $l \times b \times h$. Then the discrete nodes m and n are sharing a common link. Hence, the probability p of the likelihood of the nodes m and n in the deployment region is calculated as in equation 1.

$$p = \frac{1}{l^2 b^2 h^2}((-\frac{1}{6}s^6 + \frac{8}{5}s^6(l+b+h) - \frac{1}{2}\pi s^4(bl+hl+bh) + \frac{4}{3}\pi s^3 lbh) \tag{1}$$

And coverage density φ of each node is calculated by (2)

$$\varphi = \frac{1}{lbh}((-\frac{1}{6}s^6 + \frac{8}{5}s^6(l+b+h) - \frac{1}{2}\pi s^4(bl+hl+bh) + \frac{4}{3}\pi s^3 lbh) \tag{2}$$

Then the coverage volume C_v for the t number of nodes is given by (3)

$$C_v = \left[1 - (1 - \frac{\varphi}{h})^t\right] h \tag{3}$$

Where h is the intended density to be covered, and t is the total number of nodes. The following are the assumptions that made to achieve the coverage ratio:

a) All the nodes are treated as liable nodes and able to communicate with the sink node. Here the mode of communication is treated as acoustic among the underwater nodes. Consecutively, the ground node to the monitoring system is by radio wave communication.

b) At the deployment stage, the isomorphic nodes are allowed to adjust their sensing radius Ramin and Ramax upon the minimum and maximum coverage, respectively, as shown in **Fig. 2**.

c) Due to the factors such as drift in water currents and waves, the positions are changed of some corresponding nodes. At each round, the deployment readjusts the radius to achieve the coverage ratio, as made in equation 3.

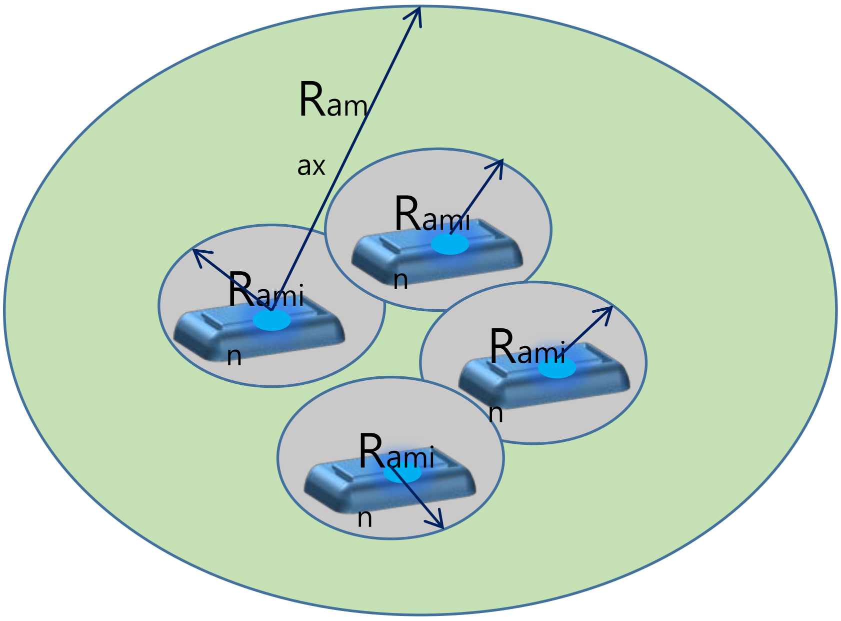

Fig. 2. Node deployment on sensing radius

Also, several node deployment strategies are prevalent for better coverage [23] prediction and self-adjusting [24] adoption. **Fig. 3** shows the random scattering of underwater nodes in a 3D plane simulated using the GNU plot [25] by taking coverage ratio as a measure.

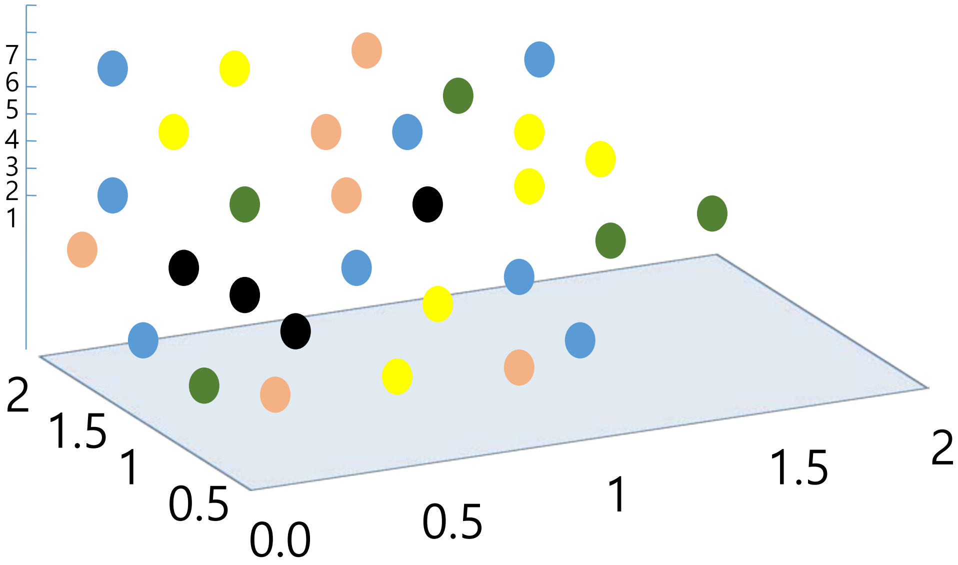

Fig. 3. Node Deployment in 3D plane

3.2Attacker detection using sheep-flock heredity algorithm

In this proposed work, three agents are considered for performing standalone IDS that run on each node for secured data transfer. It further isolates the malicious nodes, both internally and externally. First, ID agent verifies the authentication of the node, EN agent checks for the residual energy of the nodes, and D agent substantiates the depth value of each node. We have assumed that the agents are responsible for the data aggregation and forwarding. It behaves like a central authority for further validation of the nodes by utilizing the training data. ID agent reads the encrypted data. In the authentication process, the encryption is initiated by each node and perused by the sink node. It legally checks each node for ensuring secure acoustic communication. ID agent consists of attributes and keys.

Node_A	: Source node
Node_B	: Receiver node
Sink	: Surface sink
Key_A	: Private Key of Node_A
Key_sink	: Private Key of the sink node
K_sym	: Symmetric Key

Initially, NodeA starts the communication after obtaining the credentials from the surface sink through a message request, ReqM containing the ID and IP address. Further, it encrypts the intended data with a private key followed by the symmetric key, and passes it to Node_B.

$$NodeA \rightarrow sink:\ encrpyt_{Ksym}\,(encrypt_{KeyA}(ReqM), NodeA))$$

Surface sink deciphers the Req_M with the private key belongs to it. It then verifies the Node_A and deciphers the Req_M using the public key of Node_A. If the match is found, Node_A is considered as the authenticated node. After successful verification, the Node_A enciphers the incoming message with its private key and sink's private key, and then authentication credentials are sent to Node_A.

$$sink \rightarrow NodeA: encrpyt_{Ksym}\,(encrypt_{KeyB}(ReqM)))_{//}\,score{=}1$$

Upon every communication, Node_A sends its credentials to the node it intended to transfer the data. For example, if Node_A wants to communicate with the Node_B, it has to send the credentials to Node_B.

$$NodeA \rightarrow NodeB: encrpyt_{Ksym}\,\left(encrypt_{KeyB}(ReqM)\right), NodeA$$

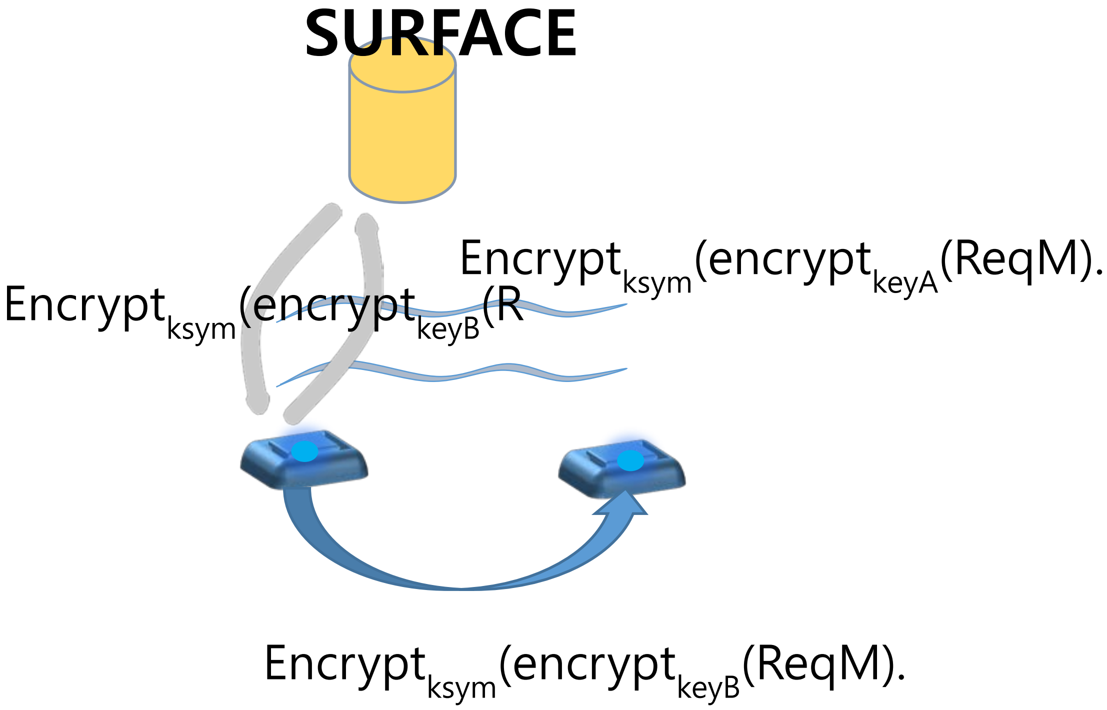
SURFACE
Encrypt_ksym(encrypt_keyA(ReqM).
Encrypt_ksym(encrypt_keyB(R
Encrypt_ksym(encrypt_keyB(ReqM).

Fig. 4. Node verification and authentication

After receiving the credentials from NodeA, the message is deciphered using the public key of the sink node and NodeA. The procedure is then followed by all nodes that take part in acoustic data transfer. The idea of node verification and authentication is shown in **Fig. 4**.

The score value for each node is expressed as the number of false-positive and false-negative obtained after the authentication process. If the node is authenticated, then the score value for an authenticated node ($Node_{auth}$) is one. otherwise, it is set as 0.

Later, EN agent compares the obtained energy with the desired energy and determines the matching value as a score for each sensor node. Additionally, the agent is responsible for fetching both the neighbor's energy value and its energy information. The energy of the node is the total amount of joules that are spent for sensing and communicating. Hence the energy consumption measure requires the distance of neighboring nodes where it is deployed. The underwater sensors communicate through acoustic mode [26]. it uses the sound wave as the medium of transfer [27].

Hence, the signal loss (S_{loss})is calculated as in equation 4.

$$S_{loss} = distance^{\lambda} . ɵ^{distance} \tag{4}$$

Distance is the measure taken for transmitting a data packet
λ is the factor of energy diffusion
ɵ denotes the coefficient parameter equals to $10^{COA(fc)/10}$, in which COA is the coefficient of

absorption and f_c is the frequency of carrier signal expressed in kHZ units and COA is calculated by the following equation 5.

$$COA(f_c) = 0.11\frac{10^{-3}{f_c}^2}{1+{f_c}^2} + 44\frac{10^{-3}{f_c}^2}{4100+{f_c}^2} + 2.75\,X\ 10^{-7}{f_c}^2 + 3\,X\,10^{-6} \tag{5}$$

Hence the energy consumption of individual node for transmitting the received packet ($P_{received}$) over the distance D at the time $T_{P_{received}}$is measured as in equation 6.

$$I_{energy}(D) = P_{received}\,X\,T_{P_{received}}\,X\ \text{Sloss} \tag{6}$$

After calculating the energy consumption value, the neighboring node's energy data is collected by sending an $\text{Energy}_{\text{req}}$ to its adjacent nodes. Upon receiving the neighboring data, the nodes are allowed to participate in the acoustic communication. The genuine energy value C_{energy} is set and stored in the training data. The score value for the energy of an individual is obtained by equation 7.

$$\left\{score = 1\ \ or\ 0 \qquad \sum_{i=1}^{i=k} \begin{matrix} if\ I_{energy} == C_{energy} \\ if I_{energy} \neq\ \ C_{energy} \end{matrix}\right\} \tag{7}$$

Likewise, the D agent is responsible for verifying the depth value of the node. The random root node starts to determine the depth of each node that lies within the coverage range, as discussed in section III (i). Let us assume the depth value of each node is 0 initially in the same horizontal plane. The distance between the two nodes is expressed as $\text{H}_{\text{distance}}$. All the nodes are intended to maintain the distance table having distance information of the neighboring nodes that exist in the coverage region. The root node selected the farthest node as a second root and marked it as root 1 using the distance information. Consecutively, root 1 determines root 2, and the process gets continued for the entire network. The vertical distance of the node from the root node is expressed in equation 8. And equation 9 indicates the final depth of the node which is expressed as $\text{Node}_{\text{depth}}$.

$$\text{V}_{\text{distance}}(\text{Node}_{\text{A}},\ \text{root}) = \sqrt{{C_v}^2 - \text{Hdistance}^2} \tag{8}$$

$$\text{Node}_{\text{depth}} = \text{V}_{\text{distance}}(\text{Node}_{\text{A}},\ \text{root}) + \text{Root}_{\text{depth}} \tag{9}$$

Here, C_v is the value obtained from equation 3.

Fig. 5 shows the overall process of the depth value aggregation. Here red node is the member node, and the green node is the root node in the cluster. The depth information is aggregated in the sink and further transmitted to the surface station.

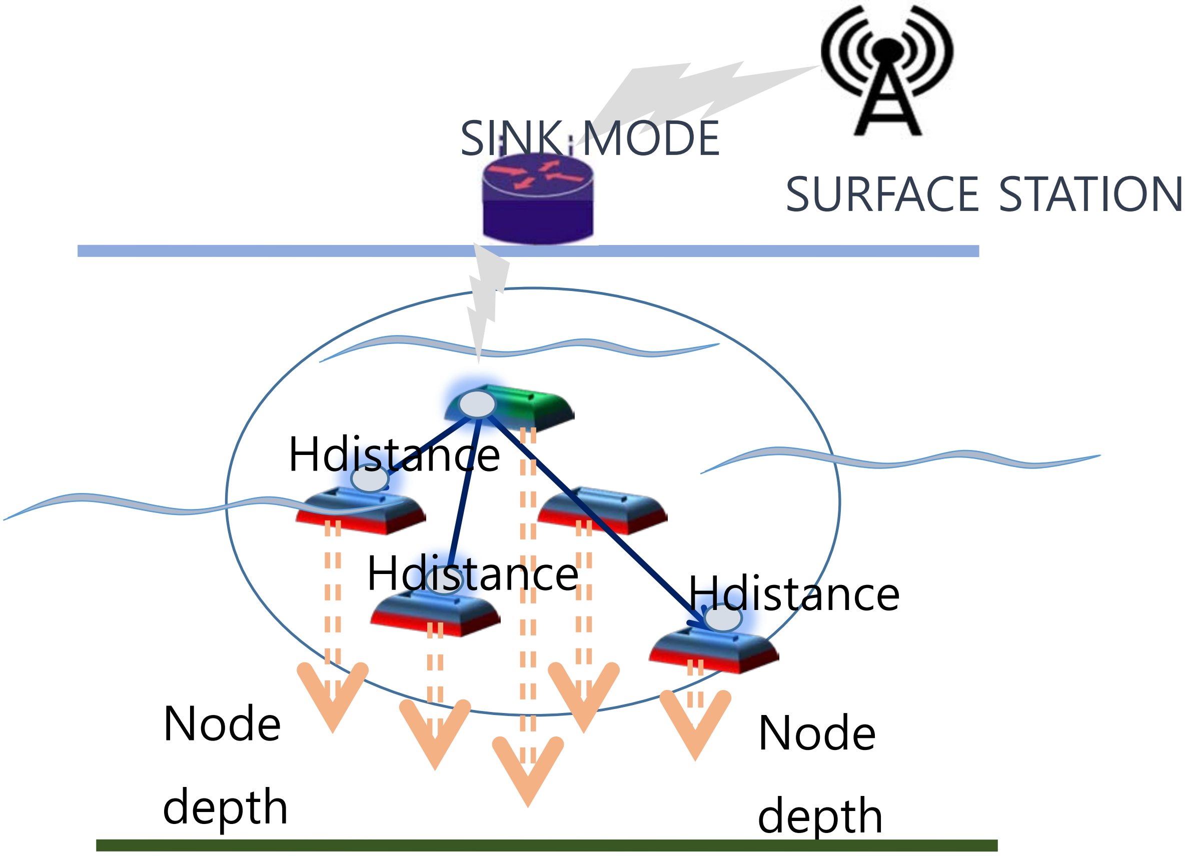

Fig. 5. Depth calculation by root node

The score value for depth is determined by the equation 10.

$$\left\{ score = 1\ \ or\ 0 \qquad \sum_{i=1}^{i=k} \begin{matrix} if\ Node_{depth} == C_{depth} \\ ifINode_{depth} \neq\ C_{depth} \end{matrix} \right\} \qquad (10)$$

Where, C_{depth} is the corrected depth value of the nodes stored in the training data.

All the fetched data collected from the agents are verified and validated using the sheep-flock heredity algorithm. The overall process of malicious node detection is given below (**Fig. 6**).

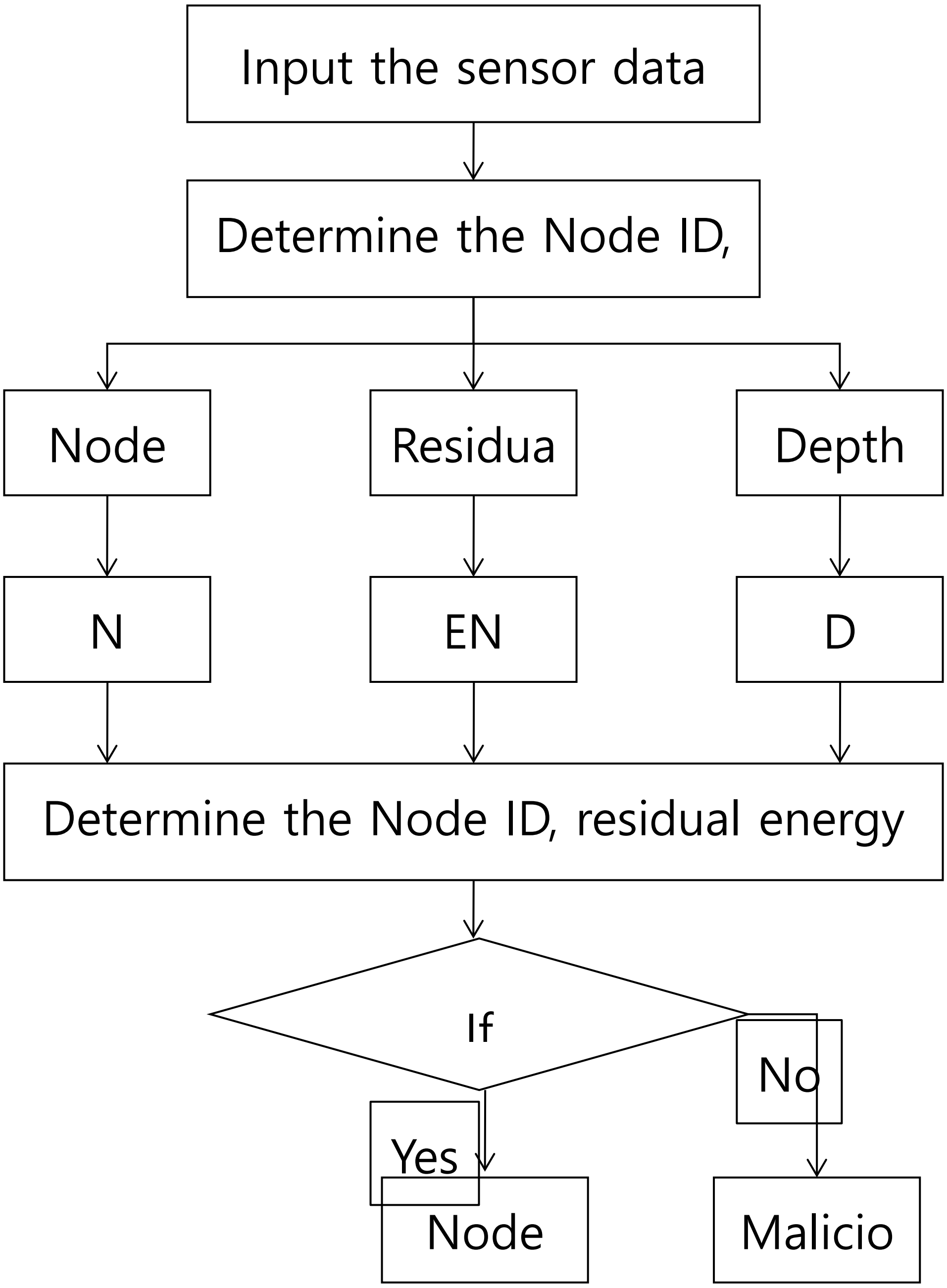

Fig. 6. Flowchart for Intrusion Detection using SFH

The sheep-flock heredity algorithm [28] states that the shepherd in the lowland controls the sheep. It is assumed that the maximum likelihood of the characteristics of sheep is inherited only within the farm. Rarely, some species can exhibit some other characteristics from another flock. In this context, the sheep are affected by the flock's features and from the nearest flock. The obtained features are considered to be the fitness characteristics assumed to breed the most as both the flock possesses it. The idea is adopted for performing the EEIDS to detect and isolate the malicious nodes. The fitness value FV is calculated as in equation 11.

$$FV_{node} = =TD-OV,\ \forall node=1,2,3\ldots\ldots\ldots.n$$

Here, TD denotes the training data, and OV represents the obtained value from the agents. FV_{node} is the threshold value set using the training data containing NodeID, depth value, and residual energy of all the nodes in the network. The step by step procedure for implementing the sheep-flock heredity algorithm is shown below.

Algorithm 1 SFH algorithm

```
Input: Attributes of underwater sensor nodes ($att_1$, $att_2$,…….,$att_n$)
  1. Declare the initial random population N
  2. Assume some sub chromosome using the length l
  3. Fix some target value as threshold measure using the TD for all nodes in the N and
     represent as $FV_{node}$
  4. Implement interchange on sub chromosome
  5. Employ opposite mutation on sub chromosome
  6. Compute $FV_{node}$ for chromosome obtained from step 4 and differentiate with the $FV_{node}$
     of the intended chromosome and find out the chromosome based on the best fit $FV_{node}$
     value.
  7. Repeat step 4 for all levels until achieved a best $FV_{node}$ value
  8. Find the optimal path
```

The implementation of EEIDS using sheep flock heredity algorithm is shown in algorithm 2.

Algorithm 2 EEIDS using sheep flock heredity algorithm

```
1. Declare the number of underwater sensor nodes N={att1 …attn)
     Examine the conditions
          $\begin{Bmatrix} score = 1 \quad if\ (\ att\ satisfies\ the\ fitness\ value) \\ score = 0\ otherwise \end{Bmatrix}$

     if ($Node_{auth}$==1)&&($I_{energy} == C_{energy}$)&&($Node_{depth} == C_{depth}$) then
          $\boldsymbol{score = 1}$
     else
          $\boldsymbol{score = 0}$

2. Assume sub chromosomes as {{$att_1$…$att_m$}, {$att_m$……$att_p$}, {$att_p$…..$att_n$}}
3. Implement cross-over on nodes and calculate the score value and check with the obtained
   values and $FV_{node}$.
4. Employ inverted mutation on nodes and calculate the score value and check with the
   obtained values and $FV_{node}$
5. Repeat 2,3 and 4 until all the nodes meets the fitness conditions, then classify the nodes as
   malicious and trusted nodes
6. Allow nodes participation falls under trusted category else, reject the nodes
```

3.3 Data forwarding via secured energy-efficient path

In this phase, the data packets are transferred from the initiator node to the receiver node after getting verified with each node's score values. The nodes' score information helps identify the node's status, whether it is trusted or malicious. In EEIDS, every node is provided with the corresponding score value. the sender node selects the authentic node with a high score as its next hop. In this view, each node maintains a list of neighboring nodes possessing high scores to forward the data packets. The nodes with score 0 are considered the untrusted node and no longer allowed to participate in the network, as shown in **Fig. 7**. Let us assume the nodes a, b, c, and d are the trusted optimal nodes having satisfied all the parameters. Node e and f are considered as a malicious node as it fails to satisfy the parameters taken. Therefore, the nodes are not allowed to forward the data packets through the malicious nodes. In some cases, two neighboring nodes may be having a high score. It can be resolved by checking for the optimal energy value and the depth value of the neighboring nodes.

The nodes with higher residual energy and lower depth value are considered as optimal nodes. Since higher residual energy nodes can sustain for a long time and nodes with lower depth value can transmit the data packets to the sink node faster. Upon transmission in the network, while forwarding the data packets, three different scenarios are possible (a) if two neighboring nodes have the high score with same residual energy value, (b) if two neighboring having optimal score with the same depth value and (c) if two optimal neighboring nodes are having same energy and depth value. In case a) if the node possesses the same residual energy, the node checks for the depth value of the neighboring nodes. If the node has a lower depth value, then that node is considered the next hop. Likewise, in the case of b, if two liable neighboring nodes have the same depth value, the node checks for higher residual energy, the nodes which are having higher energy value is considered as the next hop. In scenario (c), when the neighboring nodes have the same depth and residual energy, any node may be considered the next hop.

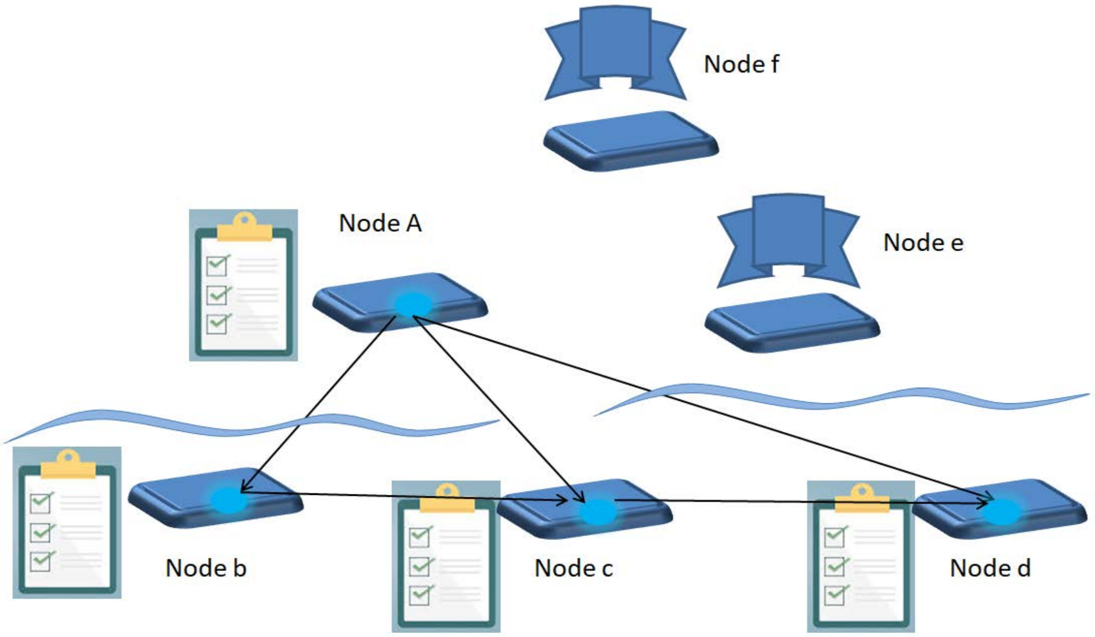

Fig. 7. Data transmission in a secured path

4. Performance evaluation of EEIDS

The simulation set up with 100 honest nodes and 20 malicious nodes is taken for consideration. The existing security approaches in UWSN such as ABC [29], SHD [30], TDM [31], MLS [32], and VBM [33] are chosen for analyzing the performance of EEIDS. Various parameters, such as time taken for malicious detection, network lifetime, energy consumption, and delivery ratio, are examined in this section.

4.1 Time taken for malicious detection

Counter value maintained by each node determines the time taken for the malicious node detection. Whenever a node receives the score value as 0, it increments its buffer size by one, and the sender node updates that the forwarded node as malicious. Once the node is detected as malicious, it broadcasts the information to all the nodes lies within the coverage region. It is evident when the number of nodes is increasing, the time taken for detecting the malevolent node getting increases. It is because a more significant number of neighbors involved in detecting and broadcasting, hence the time taken for predicting the node behavior also gets increased. The simulation starts with ten nodes, and the process remains continuing for all 100 nodes. **Table 1** provides the experimental results of the existing algorithms and EEIDS.

Table 1. Time taken for malicious node detection

Number of nodes	ABC (sec)	SHD (sec)	TDM (sec)	MLS (sec)	VBM (sec)	EEIDS (sec)
10	235	197	182	154	75	31
20	239	205	187	158	78	35
30	247	211	194	168	82	28
40	254	219	199	172	85	37
50	257	225	206	176	88	42
60	264	230	214	179	92	45
70	275	236	219	188	107	48
80	285	243	223	193	110	54
90	290	245	225	195	116	56
100	295	255	230	200	120	60

For a network consisting of 100 nodes, the average time taken by EEIDS for malicious node detection is around 43 seconds. The obtained values are plotted in the Gnu plot, as shown in **Fig. 8**, and it is clear that the proposed EEIDS consumes less time for vulnerability detection compared to other security systems.

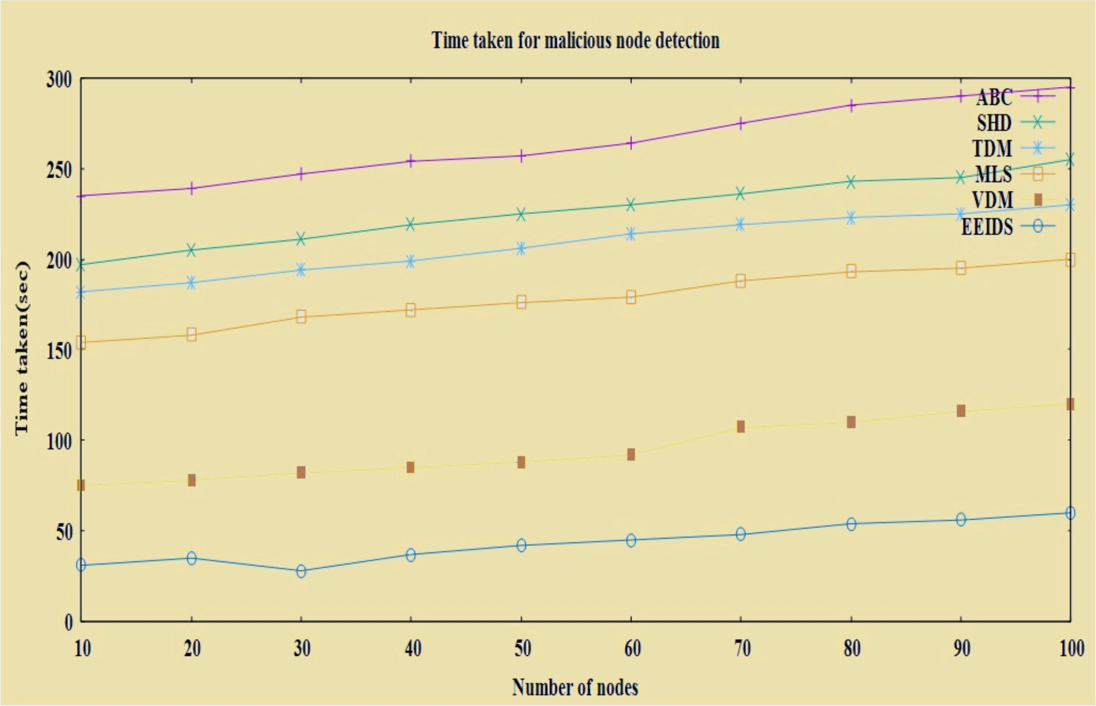

Fig. 8. Time taken for malicious node detection

4.2 Network life time

It is calculated by evaluating the number of exhausted nodes in the network. When the nodes start transmitting the data for a long time, it might die due to the low power backup and some drifts in current. The existing systems always designed for choosing the nodes with lower depth value for data transmission. Due to the over usage of the same nodes may turn the lower depth nodes to halt at times. However, EEIDS designed for choosing the node in terms of residual energy. Hence the designed system enhances the network lifetime by performing data transmission in a balanced way. **Table 2** shows the different instances of network lifetime when increasing the number of nodes in certain intervals.

Table 2. Network life time of UWSNs

Number of nodes	ABC	SHD	TDM	MLS	VBM	EEIDS
10	5	7	8	9	10	1
20	8	10	11	12	13	1
30	9	11	12	13	14	2
40	11	13	14	15	16	2
50	14	16	17	18	19	2
60	16	18	19	20	21	3
70	17	19	20	21	22	3
80	19	21	22	23	24	3
90	16	18	19	20	21	4
100	20	22	23	24	25	4

Based on the obtained values, we perform the Gnu plot to visualize the proposed system performance (**Fig. 9**). It shows that EEIDS provides enhanced network lifetime by sustaining a higher number of nodes.

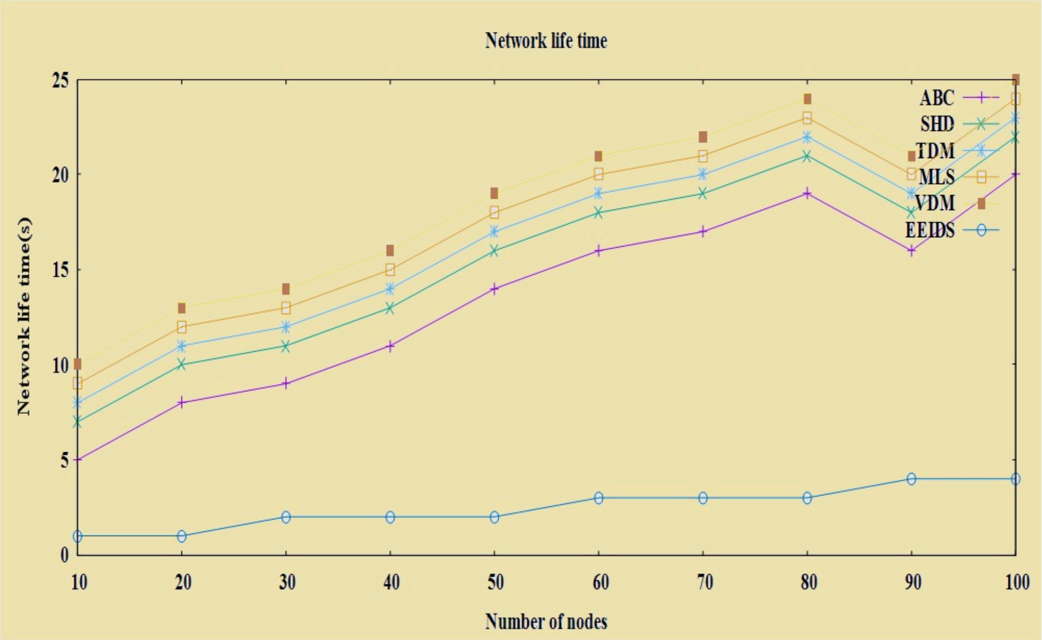

Fig. 9. Comparison of UWSN life time

4.3 Energy consumption

It is the amount of energy taken by the underwater sensor to forward the data packets from one end to another. Existing systems often encountered with repeated transmissions and high utilization of lower depth nodes. So, the energy consumption of them is high. Since EEIDS is designed to stabilize the energy levels, the amount of energy consumed by the sensors will be low compared to the previous studies. **Table 3** shows various energy values checked at different time intervals with a gradual increase of nodes.

Table 3. Energy consumption of sensor nodes

Number of nodes	ABC	SHD	TDM	MLS	VBM	EEIDS
	(joules)	(joules)	(joules)	(joules)	(joules)	(joules)
10	25	30	35	40	45	11
20	28	33	38	43	48	11
30	29	34	35	36	37	12
40	31	36	37	38	39	12
50	34	39	40	41	42	12
60	36	41	42	43	44	13
70	37	42	43	44	45	13
80	39	44	45	46	47	13
90	36	41	42	43	44	14
100	40	45	46	47	48	14

Using the above values, the Gnu plot (**Fig. 10**) is made, and we can infer that the proposed EEIDS provides reduced energy consumption when compared to the existing systems.

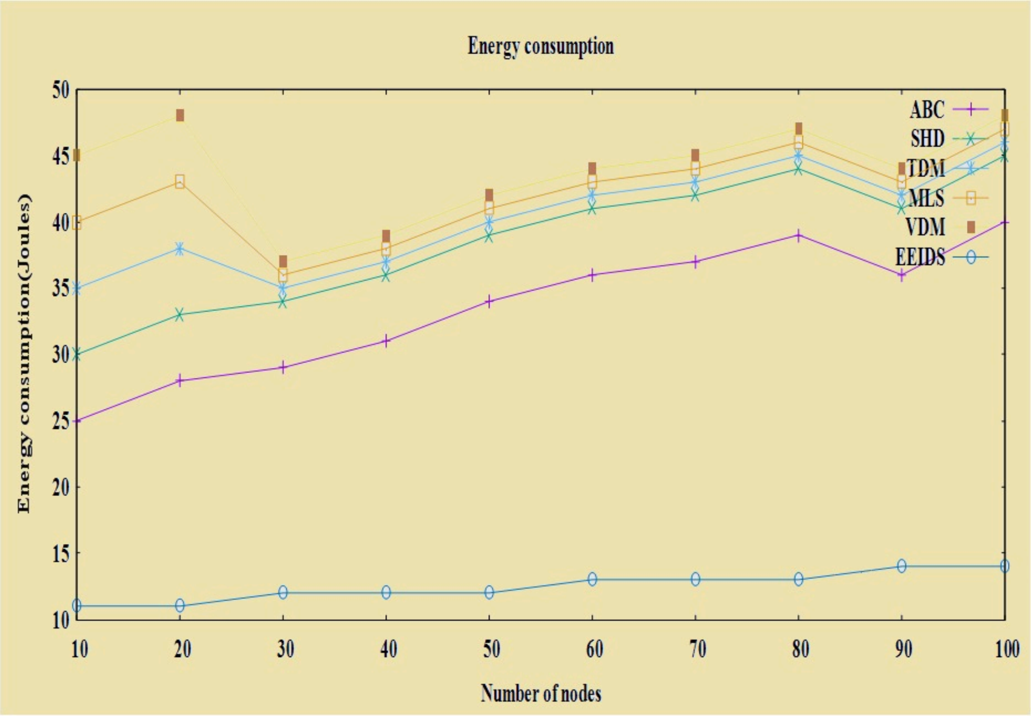

Fig. 10. Comparison of energy consumption in network

4.4 Delivery ratio

It is the measure of the successful delivery of packets from the source to the destination. Here the existing systems show a higher delivery ratio because it performs data transfer in all paths without considering the residual energy and depth measures. **Table 4** shows the delivery ratio of various schemes measured at a gradual increase in the number of nodes.

Table 4. Delivery ratio of the sensor nodes

Number of nodes	ABC	SHD	TDM	MLS	VBM	EEIDS
10	15	25	25	30	35	21
20	18	28	28	33	38	21
30	19	29	25	26	27	22
40	21	31	27	28	29	22
50	24	34	30	31	32	22
60	26	36	32	33	34	23
70	27	37	33	34	35	23
80	29	39	35	36	37	23
90	26	36	32	33	34	24
100	30	40	36	37	38	24

Fig. 11 shows the comparison results of the delivery ratio of various security approaches. EEIDS shows less delivery ratio as it transmits the data via a secured energy-efficient path.

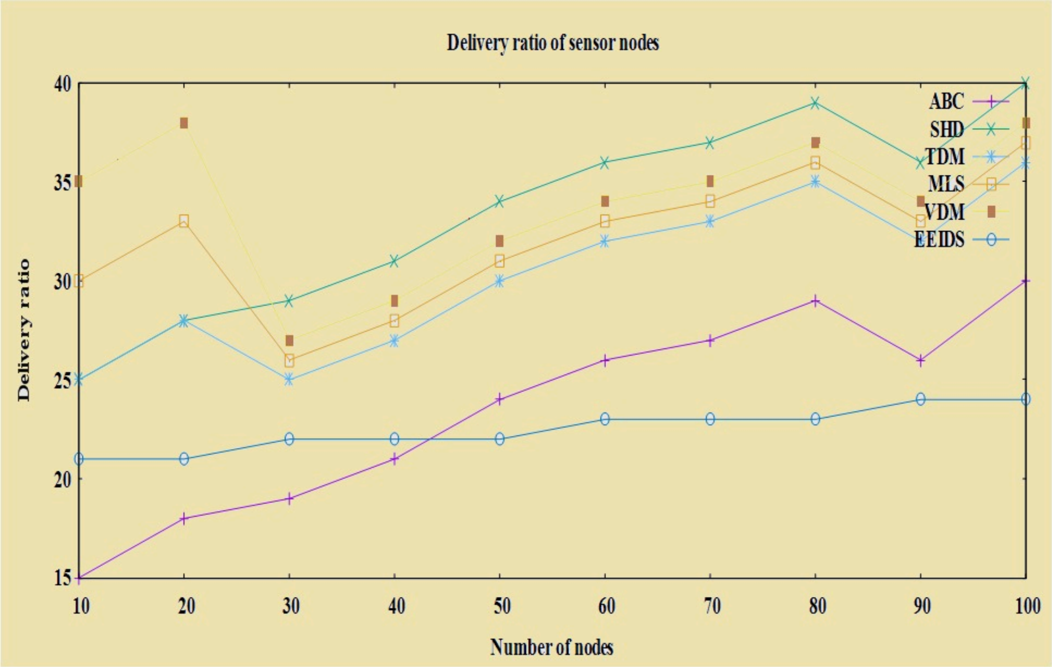

Fig. 11. Comparison of delivery ratio of sensor nodes

4.5 Discussion

The effectiveness and efficiency of the proposed security approach is evaluated by matrices like time taken for malicious node detection, network life time of UWSN, energy consumption of sensor nodes and delivery ratio of the sensor nodes. The proposed approach is compared with existing security approaches and it is proved that the proposed approach is more efficient. For evaluation of the proposed approach, number of nodes ranging between 10 and 100 with the interval of 10 each is taken into consideration. Form **Table 1**, the result shows that the time taken for malicious node detection of EEIDS approach is significantly less as compared to the existing methods. The time taken for detection of 10 nodes for EEIDS is 31 seconds which is more than half of the time taken by existing approaches. As shown in **Table 2**, life time of network in UWSN of EEIDS method is the shortest which is ranging from 1 to 4 seconds of time for the interval of nodes between 10 and 100. In **Table 3**, energy consumption of sensor nodes is evaluated in unit of joules. It is identified that EEIDS is the most energy efficient approach among the existing security approaches in UWSN with the minimum energy consumption of 11 joules and maximum of 14 joules for 100 nodes whereas, the minimum energy consumption for the existing approaches is 25 joules and maximum is 48 joules. **Table 4** is about delivery ration of sensor nodes and the delivery ratio of proposed EEIDS method is consistence ranging from 21 – 24 while increasing the number of nodes from 10 to 100 respectively. Hence, the simulation result confirms that the proposed method EEIDS achieves a reasonable performance under different routing scenarios.

5. Conclusion

Securing the underwater sensor network is quite complicated since it is constrained with high propagation delay, reduced bandwidth, and limited battery power. Hence, we provide an energy-efficient ID using a sheep flock heredity algorithm for establishing an optimal path. Here three agents are assigned for each node intended to perform authentication, residual energy calculation, and depth value measurement. Also, score values are determined for detecting the vulnerable node. Besides, EEIDS isolates the malicious and low energy nodes to avoid further participation in the network. The green and secure EEIDS is evaluated experimentally, and the comparison results are shown to infer that it outperforms existing security approaches.

References

[1] Climent, S., Sanchez, A., Capella, J.V., Meratnia, N., Serrana, J.J., "Underwater acoustic wireless sensor networks: Advances and future trends in physical, MAC and routing layers," *Sensors*, 14, 795–833, 2014. Article (CrossRef Link)

[2] Wang, Y., Liu, Y., Guo, Z., "Three-dimensional ocean sensor networks: A survey," *J. Ocean Univ. China*, 11, 436–450, 2012. Article (CrossRef Link)

[3] Bean Tim P., Greenwood Naomi, Beckett Rachel, "A Review of the Tools Used for Marine Monitoring in the UK: Combining Historic and Contemporary Methods with Modeling and Socioeconomics to Fulfill Legislative Needs and Scientific Ambitions," *Frontiers in Marine Science*, vol. 4, 15 August 2017. Article (CrossRef Link)

[4] Ahmad, B., Jian, W., Enam, R.N. et al., "Classification of DoS Attacks in Smart Underwater Wireless Sensor Network," *Wireless Pers Commun*, 116, 1055-1069, 2021. Article (CrossRef Link)

[5] Guang Yang, OrcID, Lie Dai andZhiqiang Wei, "Challenges, Threats, Security Issues and New Trends of Underwater Wireless Sensor Networks," *Sensors*, 18(11), 3907, 2018. Article (CrossRef Link)

[6] Guerroumi, M., Derhab, A., Saleem, K., "Intrusion detection system against sink hole attack in wireless sensor networks with mobile sink," in *Proc. of the 2015 12th IEEE International Conference on Information Technology-New Generations (ITNG)*, Las Vegas, NV, USA, pp. 307–313, 13–15 April 2015. Article (CrossRef Link)

[7] M. Saravanan, "Sheep flock heredity algorithm to solve the loop layout problem in flexible manufacturing system," *Int. J. Enterprise Network Management*, Vol. 7, No. 3, 2016. Article (CrossRef Link)

[8] Abdul Wahid and Dongkyun Kim, "An Energy Efficient Localization-Free Routing Protocol for Underwater Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, Vol. 2012, p. 11, 2012, Article ID 307246. Article (CrossRef Link)

[9] J. Kong, Z. Ji, W. Wang, M. Gerla, R. Bagrodia, and B. Bhargava, "Low-cost attacks against packet delivery, localization and time synchronization services in under-water sensor networks," in *Proc. of the 4th ACM workshop on Wireless security*, ACM, pp. 87–96, 2005. Article (CrossRef Link)

[10] Y. Dong, H. Dong, and G. Zhang, "Study on denial of service against underwater acoustic networks," *J. of Commun*, vol. 9, no. 2, pp. 135– 143, Feb. 2014. Article (CrossRef Link)

[11] Jiang, P., Ruan, B.F., "Cluster-Based Coverage-Preserving Routing Algorithm for Underwater Sensor Networks," *Acta Electron Sin.*, 2013(10), 2067–2073, 2013. Article (CrossRef Link)

[12] W. G. Seah and H.-X. Tan, "Multipath virtual sink architecture for underwater sensor networks," in *Proc. of the Mts/Ieee Kobe-Techno-Ocean (OCEANS '06)*, Singapore, May 2006. Article (CrossRef Link)

[13] Wang X, Xu M, Wang H, Wu Y, Shi H, "Combination of interacting multiple models with the particle filter for three-dimensional target tracking in underwater wireless sensor networks," *Math Probl Eng*, 2012. Article (CrossRef Link)

[14] Bereketli A, Bilgen S, “Remotely powered underwater acoustic sensor networks,” *IEEE Sensors J*, 12(12), 3467–3472, 2012. Article (CrossRef Link)

[15] Senel, F., Akkaya, K., Yilmaz, T., “Autonomous deployment of sensors for maximized coverage and guaranteed connectivity in underwater acoustic sensor networks,” in *Proc. of IEEE 38th Conference on Local Computer Networks (LCN)*, Sydney, Australia, pp. 211–218, 21–24 October 2013. Article (CrossRef Link)

[16] Zeng, B., Zhong, D.H., Yao, L., “Research of underwater mobile sensor network algorithm based on water flow,” *Appl. Res. Comput*., 10, 80–89, 2010.

[17] Xia, N., Zheng, Y.C., Du, H.Z., Xu, C.N., Zheng, R., “Rigidity driven underwater sensor self-organized deployment,” *Jisuanji Xuebao (Chin. J. Comput.)*, 36, 494–505, 2014. Article (CrossRef Link)

[18] Y. Y. Al-Aboosi and A. Z. Sha'ameri, “Improved underwater signal detection using efficient time-frequency de-noising technique and pre-whitening filter,” *Applied Acoustics*, vol. 123, pp. 93–106, 2017. Article (CrossRef Link)

[19] M. Goetz, S. Azad, P. Casari, I. Nissen, and M. Zorzi, “Jamming resistant multi-path routing for reliable intruder detection in underwater networks,” in *Proc. of the Sixth ACM International Workshop on Underwater Networks*, ACM, pp. 1-5, 2011. Article (CrossRef Link)

[20] G. Ateniese, A. Capossele, P. Gjanci, C. Petrioli, and D. Spaccini, “SecFUN: Security framework for underwater acoustic sensor networks,” in *Proc. of OCEANS 2015 - Genova*, pp. 1–9, May 2015. Article (CrossRef Link)

[21] Zeng D., Wu X., Wang Y., Chen H., Liang K., Shu L. (2014) “A Survey on Sensor Deployment in Underwater Sensor Networks,” in *Proc. of CWSN 2013: Advances in Wireless Sensor Networks*, pp 133–143, 2014. Article (CrossRef Link)

[22] Guangjie Han, “A Survey on Deployment Algorithms in Underwater Acoustic Sensor Networks,” *International Journal of Distributed Sensor Networks*, Vol. 9, no. 12, 2013. Article (CrossRef Link)

[23] Anvesha Katti et. al, “Node Deployment Strategies and Coverage Prediction in 3D Wireless Sensor Network with Scheduling,” *Advances in Computational Sciences and Technology*, Vol. 10, No. 8, pp. 2243-2255, 2017.

[24] Akkaya, K., Newell, A., “Self-deployment of sensors for maximized coverage in underwater acoustic sensor networks,” *Computer Communications*, 32(7-10), 1233-1244, 2009. Article (CrossRef Link)

[25] Nagarajan, Balaji, “GNUPLOT for beginners,” in *Proc. of GSA Workshop*, 2016. Article (CrossRef Link)

[26] S Climent, A Sanchez, JV Capella, “Underwater acoustic wireless sensor networks: advances and future trends in physical, MAC and routing layers,” *Sensors*, 14(1), 795-833, 2014. Article (CrossRef Link)

[27] Ahmed, S., Javaid, N., Khan, F.A., Durrani, M.Y., Ali, A., Shaukat, A., Sandhu, M.M., Khan, Z.A., Qasim, Q., “Co-UWSN: Cooperative Energy-Efficient Protocol for Underwater WSNs,” *Int. J. Distrib. Sens. Netw*., 75, 59–72, 2015. Article (CrossRef Link)

[28] K. Mallikarjuna, N. G. Rao, G. S. Prasad, A. R. Reddy and A. Srikanth, “A sheep flock heredity algorithm for optimum design of ladder layout with integrated scheduling: An approach of metaheuristic,” in *Proc. of 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, pp. 2007-2012, 2017. Article (CrossRef Link).

[29] N. Nithiyanandam & Latha Parthiban, “An efficient voting based method to detect sink hole in wireless acoustic sensor networks,” *Int J Speech Technol*, 23, 343-354, 2020. Article (CrossRef Link)

[30] Ngai, Edith & Liu, Jiangchuan & Lyu, Michael, “On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks,” in *Proc. of 2006 IEEE International Conference on Communications*, 8, 3383–3389, 2006. Article (CrossRef Link)

[31] Ramesh S, Yaashuwanth C, “Enhanced approach using trust based decision making for secured wireless streaming video sensor networks,” *Multimedia Tools and Applications*, vol. 79, pp. 10157-10176, 2019. Article (CrossRef Link).

[32] Ramesh S, Yaashuwanth C, "Machine Learning Approach for secure communication in wireless video sensor networks against denial of service attacks," *International Journal of Communication Systems*, vol. 33, no. 12, pp. 1-12, 2020. Article (CrossRef Link)

[33] N. Nithiyanandam, Latha Parthiban, "An efficient voting based method to detect sink hole in wireless acoustic sensor networks," *International Journal of Speech Technology*, 23, 343–354, 2020. Article (CrossRef Link)

[34] Hanjiang Luo, Kaishun Wu, Feng Hong, "Ocean Barrier: a floating intrusion detection ocean sensor networks," in *Proc. of 2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*, December 2016. Article (CrossRef Link)

[35] Jiayi Sun and Gaotao Shi, "Cost-efficient node deployment for intrusion detection in underwater sensor networks," in *Proc. of 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS)*, December 2019. Article (CrossRef Link).

[36] Sanjana Palisetti and Akhilraj V. Gadagkar, "Intrusion detection of sinkhole attack in underwater acoustic sensor networks," *Journal of sensors*, 2015. Article (CrossRef Link).

[37] Hanjiang Luo, Xiumei Xie, Guangjie Han, Rukhsana Ruby, Feng Hong and Yongquan Liang, "Multimodal acoustic-RF adaptive routing protocols for underwater wireless sensor networks," *IEEE Access*, vol. 7, pp. 134954-134967, 2019. Article (CrossRef Link)

[38] PengSun, Winston K.G. Seah and Pius W.Q. Lee, "Efficient data delivery with packet cloning for underwater sensor networks," in *Proc. of 2007 Symposium on Underwater Technology and Workshop on Scientific Use of Submarine Cables and Related Technologies*, April 2007. Article (CrossRef Link)

[39] Juan Chang, Xiaohong Shen, Weigang Bai and Xiangxiang Li, "Energy-efficient barrier coverage based on nodes alliance for intrusion detection in underwater sensor networks," *IEEE Sensors Journal*, vol. 22, No. 2, pp. 3766-3776, January 2022. Article (CrossRef Link).

[40] Yanping Zhang, Yang Xiao, Kui Wu, Xiaojiang Du and Bo Sun, "Three dimensional intrusion objects detection under randomized scheduling algorithm in sensor networks," in *Proc. of 2008 The 4th International Conference on Mobile Ad-hoc and Sensor Networks*, December 2008. Article (CrossRef Link).

Dr. N. Nithiyanandam* has completed his B.Tech - Information Technology in Madras University in the year 2004 and completed his M.E - Computer Science and Engineering in Vels University 2013. He completed his Ph.D. in Computer Science in Pondicherry University 2021, Puducherry. His research area is Wireless Sensor Network. He has 15 years of experience in teaching and 3 years of experience in industry. He is working as Assistant Professor in in the department of Computing Technologies in SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamilnadu, India

Dr. C. Mahesh has completed his B.E – Electrical and Electronics Engineering in Madras University in the year 1998 and completed his M.E - Computer Science and Engineering in Anna University 2006. He completed his Ph.D. in Computer Science and Engineering in Vel Tech University 2016. His research area is Neural Network. He has 22 years of experience in teaching. He is working as Professor in in the department of Artificial Intelligence and Machine Learning in Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu, India

S. P. Raja is born in Sathankulam, Tuticorin District, Tamilnadu, India. He completed his schooling in Sacred Heart Higher Secondary School, Sathankulam, Tuticorin, Tamilnadu, India. He completed his B. Tech in Information Technology in the year 2007 from Dr. Sivanthi Aditanar College of Engineering, Tiruchendur. He completed his M.E. in Computer Science and Engineering in the year 2010 from Manonmaniam Sundaranar University, Tirunelveli. He completed his Ph.D. in the year 2016 in the area of Image processing from Manonmaniam Sundaranar University, Tirunelveli. Currently he is working as an Associate Professor in the School of Computer Science and Engineering in Vellore Institute of Technology, Vellore, Tamilnadu, India

S. Jeyapriyanga has completed her B.E – Computer Science and Engineering in Anna University in the year 2017 and completed her M.E - Software Engineering in Anna University 2019. Her research area is Wireless Sensor Networks. She has 6 years of experience in teaching. She is working as Assistant Professor in in the department of Information Technology in St. Joseph's College of Engineering, Chennai, Tamilnadu, India

T. Selva Banu Priya has completed her B.E – Computer Science and Engineering in Anna University in the year 2006 and completed her M.E - Computer Science and Engineering in Anna University 2010. Her research area is Computer Networks. She has 11 years of experience in teaching. She is working as Assistant Professor in Artificial Intelligence and Data Science in Panimalar Engineering College, Poonamalle, Chennai, Tamilnadu, India.