Privacy Prevention and Nodes Optimization, Detection of IoUT based on Artificial Intelligence

Rajkumar Gaur (rajumargaur@gmail.com)  
Madan Mohan Malaviya University of Technology  https://orcid.org/0000-0003-2792-6535

Shiva Prakash  
Madan Mohan Malaviya Engineering College: Madan Mohan Malaviya University of Technology

Research Article

Keywords: Underwater, IoUT, optimization, ECC, dynamic graph network, Swarm optimization, PSO.

Posted Date: March 16th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2117622/v1

License: ☕️ This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
Abstract
Transportation, temperature control, and the production of pharmaceuticals all rely on 71 percent of the Earth’s surface, which is covered by water. Valuable things, including minerals, metals, corals, and coral reefs, can be identified with the help of the IoUT, among other applications. One of the crucial uses is in preventing damage caused by natural disasters. The IoT boosted concepts for a new undersea network (IoUT). Underwater networks have many drawbacks, including a lack of dependability, limited bandwidth, long propagation delays, high processing demands, high energy costs, and node detection with secure communication. Real-time, secure data communication is a significant area of research for us, along with node identification and dynamic network configuration. IoUT faces severe obstacles in the form of these issues. Our strategy involves a dynamic graph for network design, an AFA algorithm based on AI for node recognition, and ECC for a secure communication mechanism. In order to increase discretion and provide the undersea network with adequate robust security.

Keywords: Underwater, IoUT, optimization, ECC, dynamic graph network, Swarm optimization, PSO.
1 Introduction

Internet of Things (IoT) and Cloud Computing are fundamental communication systems in a digital world. Cloud and Internet of Things (IoT) have evolved as conscience technologies that enable the next generation of network communication domains. The IoUT has smart interconnected underwater objects that enable to monitor vast unexplored water areas and the use of significant resources with capabilities [1]. A Cloud will be mitigate this technological restriction, such as storage and process of communication. On the other hand, Cloud increase its future direction and includes the natural world. The Internet of Things is a more collaborative and attractive way for the IoUT network to construct innovative services in real-time [2]. IoUT-based sensible objects and cloud integration are used for storage with a secure data process with conceptual frame for transmit several smart applications. Researchers have found many challenges concerning IoUT applications and cloud-based services, such as privacy and heterogeneity of networks [3].

The IoUT application uses the mathematical model of particle swarm optimization (PSO) technique for node detection of networks. The suggested mathematical model reduces the cost of the network system for a dynamic node movement and the mobility of inadequate nodes for a destroyed network system. The swarm optimization algorithm and EC-based cryptology design and stable a dynamic network connection for the IoUT network.

The air-water network system uses a wireless sensor network (WSN). It shares information from node to node of IoUT with a similar network with various nodes. The security assistance in a network secures and transmits information to the network and prohibits attackers. The attacker exploits data and misbehaves with other nodes. Our techniques provide different services such as data confidentiality, integrity, availability, self-organization, safe geolocation, synchronization, and authentication for IoUT networks and are effective for security capability to wireless networks. The capabilities incorporate into the IoUT network.

The underwater devices and networks are unsafe from various attack. The attacks classify into the following categories:

- Identity verification and secrecy challenges: Eavesdropping, packet replay attacks, and packet spoofing external assaults can damage nodes’ privacy and integrity in transmission networks.
- Denial-of-Service: These attacks interrupt communication availability at any level of an underground network and harm the network devices.
- The personal attack on service reliability: The attacker modifies the network nodes to gain a node’s information value. For example, an attacker potentially injects a message, and a sensor node compromises a malicious message.

Our scheme uses the signatures scheme to identify the nodes and create hybrid encryption/decryption to messages; the sign allows a third-party verifier to confirm the accuracy of data sharing in the cloud without taking back
the entire bit of data. This approach is enhanced security mechanism for the privacy and protection of underwater networks during information communication.

This approach involves the signer’s identity and authentication of each node and the transfer of information by the secret and public key verifier. The following are the key assumptions and identify.

- The user’s identity who signed on to the bit stream will remain private.
- The third-party observer will not have any access to the message’s contents.
- It is also possible to successfully verify dynamic data.
- Concurrently performing several audit activities will improve their efficacy.

1.1 Problem definition of the IoUT Network

As an example of how to build a secure IoUT network that can be searched and acquire AI-enabled apps in the underwater network, this part focuses on establishing a secure IoUT network. The undersea network detects and assigns responsibility for mechanical aspects of tracking devices as part of their preservation strategy. Protecting the IoUT network is essential because it stops malicious investigators (i.e., attackers) from messing with the network’s dependability settings.

1.2 Objectives and contributions

An authentic system based on IoUT, used in intelligent villages and towns, was proposed by us, along with a safe method for cloud-based real-time monitoring. Concerns including dynamic network architecture, node detection, and legitimate communication are all tackled by this issue. Both land-based and marine IoUT protection models can significantly benefit from the proposed method. The primary content in the publication is broken up into three sections:

- First, In order to implement IoUT applications, it is necessary first to develop a network and algorithm that can function in the water.
- Second, using the mathematical model as a guide, develop node optimization and detection techniques using a manner influenced by natural algorithms.
- Third, for IoUT applications, improve the ECC-based signature technique and hybrid encryption/decryption mechanisms.

Applications utilizing the IoUT typically employ the ID-Based scheme for transmitting ciphertext data and identifying nodes. Quicker processing time, smaller key sizes, and increased security are all hallmarks of asymmetric cryptosystems (ECC) protocols. The objectives above can be attained by utilizing IoT protocols in IoUT applications.

The remaining part of the paper is structured as the Section 2 related work and illustrates the research activities of covered heterogeneous networks that extend network lifespan and protect IoUT against attacks with the related
work. Section 3, our proposed scheme for air-water communication and securing data transmission in underwater systems by utilizing dynamic techniques for sensors. Section 4, simulation and results, a discussion of security schemes. Section 5 is the analysis and research concerns of underwater network security. Section 6 encountered the conclusion of the paper.

2 Related work

This section compares the practical limitations of IoUT applications and information responsibilities to analyze the different concerns that persist. IoUT’s nodes are dynamic, moving things and connect with collaborative approaches. This scenario is responsible for movable tasks and creating a collective control system. IoUT aims to build a sensible network for intelligent underwater things [4]. These all relate to the ocean, lakes, and streams. These applications include climate management, nautical animals, monitoring underwater oil rigs, intruder detection, and crewless operations. The feasible underwater wireless communication architecture is shown in Figure 1.

The underwater network consists of sensible things such as underwater sensors and independent unnamed underwater vehicles (AUVs) [5]. Optical base stations (OBS) attach bright underwater things to the surface station by applying visible connections [6]. The architecture shows that the sensors devices communicate with each other.

The static construction of the network is the fixed-line, and the dynamic construction of the network is a dotted line. However, the node position will be changed for some reason and generate events with a further underwater network design, which is shown in Figure 2.

The transmission path of nodes to nodes and nodes to AUVs devices communication is shown in Figure 3. These reviews are divided into various subsections as follows:

2.1 Underwater network

The IoUT application is more used in submarine services, improves intelligence services for wide-sea and deep-sea liveliness, and encourages ocean analysis behaviors. Another advantage is the detection of disaster management. Moreover, an underwater network can be artificial appropriate for underwater communication. It includes submarine, uncrewed surface vehicle (USV), sensor devices, and constructs an underwater synergetic network development for secure communication insecure channels from various networks [3]. The self-organizing map (SOM) method is a centralized neural network (NN) based technique, which is used in collaborative approaches for movable device authorization. Cichocka et al. [23] First, the SOM technique was analyzed for the multi-agent authorization mechanism. This technique signifies a system dynamically managing the group-based humanoids to numerous locations’ movement. Mirsadeghi et al. [24] utilized the SOM to develop and control the decision system for township humanoids. The technology enables devices to obtain dynamic
<table>
<thead>
<tr>
<th>Ref</th>
<th>Platform Used</th>
<th>Key Features</th>
<th>Application</th>
<th>Implementation Tools</th>
<th>Attacks</th>
<th>Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>[9]</td>
<td>AI based scheme</td>
<td>Environment model, key degree, reinforcement learning</td>
<td>Marine scenarios</td>
<td>MATLAB</td>
<td>Global attacks, varying attack</td>
<td>2020</td>
</tr>
<tr>
<td>[12]</td>
<td>ECC-based BP</td>
<td>ECC based scheme without BP</td>
<td>Analysis of scheme with different assumptions</td>
<td>ECDLP based</td>
<td>-</td>
<td>2019</td>
</tr>
<tr>
<td>[13]</td>
<td>ECC based</td>
<td>Hierarchy-based cluster key agreement (HCECKA)</td>
<td>ECC based</td>
<td>system cluster key</td>
<td>Analysis different attacks</td>
<td>2021</td>
</tr>
<tr>
<td>[15]</td>
<td>IoT Cloud</td>
<td>ECC based Techniques</td>
<td>Card level security</td>
<td>Mega Matcher On Card SDK 3.5</td>
<td>-</td>
<td>2018</td>
</tr>
<tr>
<td>[16]</td>
<td>Pairing free scheme</td>
<td>By using DHA and DLP for BP</td>
<td>WSN</td>
<td>Mathematical Analysis</td>
<td>Adaptive Chosen Message Attack</td>
<td>2017</td>
</tr>
<tr>
<td>[17]</td>
<td>Autonomous Underwater Vehicles (AUV)</td>
<td>AUVs to the escorting positions safely escort the moving object</td>
<td>Underwater Internet of Things (UoT) applications</td>
<td>Cooperative-Control-Based</td>
<td>Attack Analysis</td>
<td>2020</td>
</tr>
<tr>
<td>[18]</td>
<td>Cloud based</td>
<td>HCECKA Methods</td>
<td>Efficient and dynamic group key synchronization</td>
<td>-</td>
<td>Active and Passive Attacks</td>
<td>2021</td>
</tr>
<tr>
<td>[20]</td>
<td>Optical wireless</td>
<td>Hyper-exponential fitting technique</td>
<td>Find out average bit error rate (ABER)</td>
<td>-</td>
<td>-</td>
<td>2022</td>
</tr>
<tr>
<td>[21]</td>
<td>Visible light communication (VLC) system</td>
<td>Reduce the signal strength (attenuation) and transmission distance of the signals</td>
<td>Wireless Optical Communication</td>
<td>Oscilloscope measuring device</td>
<td>-</td>
<td>2022</td>
</tr>
</tbody>
</table>
### Table 2: Computationally comparison between RSA and ECC schemes key size with Signature schemes [22]

<table>
<thead>
<tr>
<th>Key Size</th>
<th>RSA Scheme</th>
<th>ECC based DL</th>
<th>Algorithms</th>
<th>Signature</th>
<th>Key Exchange</th>
<th>RTBK</th>
<th>S L</th>
<th>R ECC/RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>56</td>
<td>n bits: 512</td>
<td>p bits: 512</td>
<td>q bits: 112</td>
<td>RSA-1024</td>
<td>304</td>
<td>10^{12}</td>
<td>10^{80}</td>
<td>1/6</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>1024</td>
<td>160</td>
<td>112</td>
<td>Verify 11.9</td>
<td>15.4</td>
<td>304</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ECCDSA-160</td>
<td>22.82</td>
<td>45.09</td>
<td>22.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>112</td>
<td>2048</td>
<td>244</td>
<td>224</td>
<td>ECCDSA-1024</td>
<td>2302.7</td>
<td>57.2</td>
<td>2302.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RSA-1024</td>
<td>61.54</td>
<td>121.98</td>
<td>60.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>3072</td>
<td>256</td>
<td>256</td>
<td>ECDSA-160</td>
<td>53.7</td>
<td>22.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7680</td>
<td>384</td>
<td>384</td>
<td>ECDSA-224</td>
<td>22.3</td>
<td>22.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>192</td>
<td>7680</td>
<td>384</td>
<td>384</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>15360</td>
<td>512</td>
<td>512</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comparison of Protocol Decryption, Assumption, Security and Efficiency

<table>
<thead>
<tr>
<th>Coordinate System</th>
<th>ECC Points Addition</th>
<th>ECC Point Doubling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affine</td>
<td>S + 2M + I</td>
<td>2S + 2M + I</td>
</tr>
<tr>
<td>Jacobian</td>
<td>4S + 12M</td>
<td>6S + 4M</td>
</tr>
<tr>
<td>Modified Jacobian</td>
<td>6S + 13M</td>
<td>4S + 4M</td>
</tr>
</tbody>
</table>
responsibility authorizations based on numerous original positions. The enhancement applies in statics 2D scenarios and is inactive in three-dimensional configurations. To handle authorization issues in multi-AUV systems based on
Figure 3 Underwater dynamic network and event detection

the SOM algorithm [24]. This procedure combines the speed combination and works assignment approach for the neighboring current’s status of the sea. It divides the job area into related regions and the obstacle delay, which may be reduced [25]. The algorithm assigns each latitude as output and creates paths from the AUVs to target locations. Wang et al. [26] proposed a correct improvement methodology based on an acceptable range of procedures. The technique allows the device to generate the necessary configuration and appear target under any primary condition. Rizqi et al. [27] proposed probable field function to aircraft configuration and control technique for path-planning approach. Batina et al. [28] discussed the concern of trust assurance in sensor interfaces and proposed reputation-based secure information. In the architecture, every node renews the status of nearest neighbors based on initial appearances and forecasts the predicted enforcement. The node’s siblings are based on multiple
advanced authentications and enhance the analysis performance of assurance management. Domingo et al. [29] created a secure architecture that relies on direct communication and certificate verification. The first performance of nearest neighbors authorized trust certification from independent nodes and identified when renewing trust certificates. Feng et al. [30] developed a trust-based altered approach for the authentication process to improve direct and indirect trust coupling. The various comparison of underwater communication systems’ security schemes and protection models is shown in Table 1 [13, 29]. Table 1 shows the various security strategies and how to preserve the information of IoT nodes while using client-server communication. These schemes have a basic setup, key generation, signature generation, and signature verification in wireless communication. Table 1 represents the different attacks, and the year approaches was published. The existing security-based schemes relief from some attacks. Ullah et. al. [11] use the DND techniques. the DND has some drawbacks as dynamic forwarding of the information and authentication, the integrity of data, and catching of data. Rao et al. [12] develop a scheme without the bilinear pairing technique. The scheme’s security level is lower than other existing schemes. Sharma et. al. [16] use only one-point multiplication in the signature algorithm and two-point multiplications in Pairing-Free Identity Based Digital Signature (PF-IBS) verification algorithm. The scheme does not support the Mutual authentication and session key computation. Yaduvanshi, R et al. [31] use more time to verify the scheme. Sharma, N. et al. [32] use the pairing based, which is more secure but uses some extra pairing in point-to-point hashing.

ECC-based and RSA-based techniques are used in [6,9,11,14,16]. The comparison between RSA and ECC scheme’s key sizes with different security schemes lengths are shown in Table 2. Table 2 shows a computational comparison of schemes based on ECC and RSA with different key sizes [15][19-21]. Compared to RSA-based schemes, the ECC-based scheme uses a minor key size and faster execution to improve security levels. Table II illustrates the different signature lengths (SL) and key ratios (RTBK) for ECCRSA. For pairing-based schemes, the security scheme performs operations such as multiplication (M), square (S), and inversion (I). The secret message encodes in the form of ciphertext. The ECC-160 and ECC-224 are equivalent to the RSA-1024 in terms of security. Consequently, the ECC-based scheme requires less space and speedy performance than RSA-based schemes.

2.2 Data Collection in IoUT
The IoUT application is a collection of sensor networks with insufficient bandwidth, power, and storage capacity. To enable sensor data collection and analysis is complex. So, incomplete sensor information can be classified into informational and non-informational from different organizations [33]. In IoUT, the fundamental data is transmitted or received from wireless technology [14, 33]. Abnormality information may arise from noise, crashes, violence and
may be effective in fault-tolerance schemes. Other procedures reduce and aggregate acquired information in the underwater network. After the survey found that the total is established, group-based aggregation systems produce more reliability than non-group-based in underwater networks. Security provocations are necessary for limited secure sensor devices and various attacks. One approach is to reduce the delay of information tampering and block assurance. The data is presented regionally or communicated end-to-end encrypted if that is non-feasible networks [34].

- Time-dependent: In the reportage kind, Sensors will be activated at a specific event, such as temperature sensing or a triggered event, to collect the planned points on a regular schedule.
- Location Dependent: IoUT nodes will gather the assigned information at the instant when they coast straight overhead a particular location. The Sensor detects the appropriate level of water vapor emissions in the area and notifies the situation of an environmental monitoring organization.
- Location & Period Dependent: The IoUT Nodes hover overhead the town during a hectic hour, sensing several factors, such as the amount & intensity of emission of H2o, plus record-keeping video to understand the condition of transportation and communications at the time.
- Event-Dependent: Every event occurs, such as ship monitoring or a water game competition relay. The air-water communication nodes with sensors directly gather the information.

2.3 IoUT Network Deployment

Sensor network distribution techniques are critical for IoUT, targeting node locations and directly accessing network services. A flexible deployment technique is necessary for performing the network performance in an underwater network. Typically, sensor deployment for WSN appropriates large sensors than the smallest required number for renewal schemes. The distribution of nodes management and energy efficiency required of IoUT [29]. Moreover, this determined that no special techniques could be efficiently used. The network deployment is minimum, probably because wired sensor networks’ node formation of locations and range is restricted to cable and predetermined positions. Similarly, node connectivity is not instantly associated with the location. The IoUT challenges can be broadly categorized into secure communication, identifying nodes events, and designing dynamic networks due to unexpected position changes of UAV devices [33, 35].

3 Proposed Work

The proposed architecture design for the air-water communication with different scenarios of IoUT, which is shown in Figure 4. AUVs are scattered initially at random around the working environment. When a moving object has to be removed, a certain number of AUVs are assigned to
monitor nodes from the services station. A network shape is formed with the moving object as the target. If one of the building’s AUVs restarts to monitor the malfunction, a new AUV will be assigned dynamically to the monitoring position. The remaining AUVs will maintain the structure by assuming a possible virtual point at the location. The AUV works as the patrol mission, drops malicious devices, and moves to consecutive positions. The AUVs create record continues of fail nodes, and the escort position will be allocated to a new AUV. The remaining AUVs will keep the formation together by specifying a possible virtual point at the location [5].

In Figure 4, the underwater network communicates ground layers and underwater layers by the nodes and AUV devices. The following techniques use the swarm-based AFA algorithm for dynamic node detection, a dynamic graph-based network construction, and ECC for security key size (180 bits). The UAV has direct communication with the trusted base station service provider. The instructions and messages communicate through ASU to AUV and AUV to nodes. So, the AUVs and Nodes communicate with each other in the water. The enhanced secure swarm-based genetics algorithm based on an Elliptic Curve ($S^2BGA – EC$) algorithms are used for node detection, node identification, and secure communications. The $S^2BGA – EC$ scheme is used for communication from the cloudlet. A cloudlet is a small-scale, mobility-enhanced cloud data center positioned at the Internet’s edge. The primary goal of the cloudlet is to serve resource-intensive and interactive mobile apps by offering vital computing resources to mobile devices with minimal latency. The security strategy provides safe communication as well as protection from attackers.

### 3.1 Secure System Model for IoUT

The IoT-based uses authorize nodes to participate in an outdoor consisting of cloud servers and supervise through trust base secure services providers. Fig 4 shows the service providers’ requests transmitted to the intelligent devices. We consider the following IoUT prototype model for analyzing different problems in underwater networks.

1. At least one trustworthy base station service provider can be found on the edges (or seashore), and other AUVs scatter around the TBSSP in random positions.
2. The TBSSP provides an extended receiver using a technique that handles the complete escorting coverage from AUV devices. The AUVs’ devices’ long-range object observation sensors are proficient in observing limitations and protection targets within a specific limit.
3. The TBSSP carries a high information range to transfer messages and control every AUV device. These devices deliver a little notification when interacting with nearby AUVs with a slight transmission delay.
4. The dynamic or static AUV sends information to near AUVs’. It tracks information from sensor-based nodes, if any, altered positions.
5. The AUVs’ actions frequently change when the activities are done in the possible ways.
6. If any reason the nodes move, the network topology will be changed. That time sharing the information node to node or nodes to UAV or UAV to TBSSP generates events and requires authenticity because some malicious node or attacker tries to communicate and eradicates some essential pieces of information.

These all actions of IoUT are shown in Figure 4.

3.1.1 Nodes

A UAV is a standard sensor that gathers information from nodes. The TBSSP controls the whole operation and intimates the UAVs to monitor the node’s position and data. The TBSSP also controls the USVs through some techniques, and if any nodes want to join privately, they transfer information (Node ID) through the group’s public receiver key. The sensor-based nodes (ID) wait and establish a connection to the IoUT network. So, to handle these types of problems, use the Dynamic Particle-based Elliptic Curve cryptography (DPECC) mechanism to protect the network for secure communications.

3.1.2 Trusted Base Station Services provider (TBSSP)

The service provider is reliable for establishing the lower layer node from the public key and performs underwater security operations [36]. Meanwhile, a network group node produces the group key for synchronization. In the network,
each node receives the identical pair key from a terminal and secures information in the underwater network (earthward) communication. TBSSP manages the system key pairs and transactions of the IoUT network [29]. Every UAV receives the identical key pair for future reliable connections when the entire system performs the essential synchronization. TBSSP is the founder and manages UAVs, USVs, and nodes with connectivity security services. The TBSSP determines the system key pair and assigns data transfer from water upper and lower layers nodes from the nearest UAV service provider.

3.1.3 The method of unwavering data channeling

The subsection introduces how to deal with reliable information communications in underwater and ground layer station. Implementing the key exchange protocol through the elliptic curve-based Diffie-Hellman (ECDH) keys exchange approach. In various situations enhances reliable information transmission and increases node performance. This implementation is the key to protecting and establishing the nodes’ data security. The base station services provider and UAV system used the key performance security operations in an underwater network. The ECDH-based secure session key establishes sharing authentic information [28]. This key produces manageable, reliable information releases from the gateway to Base Station (BS) network.

- **Secure transmission process**: The method analyses the critical synchronization of the node’s key pairs in IoUT approaches and gives the most trustworthy, practical, and steady information for communications. This operational method is analogous to a private master key security technique in that the entire network claims the relevant key to collect information broadcasts. In the approach, underwater device uses key pairs to encrypt communication from nodes to UAVs [2, 34].

- **Base Station to Cloud**: To analyze the critical synchronization of the ground-based sensor nodes with TBSSP keys paired on the cloud server. The proposed approach usually provides dynamic and reliable communication transformation [8]. Since the whole network utilizes keys to secure data transmissions, this application method is similar to a private master key mechanism. The network communicates data using an identity-based procedure for nodes and UAVs descendingly.

- **Base Station to Cloud** To analyze the critical synchronization of the ground-based sensor nodes with TBSSP keys paired on the cloud server. The proposed approach usually provides dynamic and reliable communication transformation [8]. Since the whole network utilizes keys to secure data transmissions, this application method is similar to a private master key mechanism. The network communicates data using an identity-based procedure for nodes and UAVs descendingly.

- **USV to TBSSP**: To analyze the lower and upper layers’ actual synchronization of nodes to the base station. The wireless network has used the key agreement protocols. This technique provides dynamic, reliable information transmission in the underwater network. Since the entire network utilizes
key pairs to achieve secure transmission, the proposed method is similar to public and private key algorithms. The network executed the communication process of data security using the identity-based security scheme for UAV and trusted base station services provider (TBSSP) [4, 5].

- **Nodes to Nodes:** When nodes in various layers desire to convey, this analysis achieves the information transfers by using key nodes like public and private schemes. During transmission, nodes use the key and encrypt/decrypt the messages, using public and private keys to produce the ciphertext. The one-way function (hash functions) investigates the transferred information integrity by correspondence nodes. The fundamental approaches correspond to node information communication, which provides adequate security for nodes to nodes.

### 3.2 Design IoUT's Network

The PSO algorithm used to supervise event detection on the dynamic network consists of discovering and detecting events. An irregular recent graph snapshot used a sensor node and designed a new network, shown in Figure 3. The message transformation mechanism uses different techniques from source to destination nodes. The node uses handshaking protocols for contention-based, including adapting the classic Request-To-Send/Clear-To-Send (RTS/CTS) approach for an underwater method [37, 38].

**Definition 1: Dynamic Network**

The dynamic network based on the dynamic graph. Suppose a dynamic graph $G_{P}$ is dynamic graph of sequence of $p$ discrete sets $(G_{n_{1}}, G_{n_{1}}, G_{n_{1}}, \ldots, G_{n_{p}})$. where $G_{P}$ show the timestamp with $t$ and $G_{p}$ is set of some tuples $(V, E_{p}, W_{p}, X_{p})$.

- $V$: show the set of fixed graph vertices.
- $E_{p}$: is collection of $m_{p}$ b undirected edges.
- $W_{p}$: is edge weight and define function as $W_{p}: E_{p} \rightarrow \mathcal{R}_{+}$ and $X_{p}$ function define as $X_{p}: V \rightarrow \mathcal{R}^{n_{f}}$, Where $n_{f}$ feature of each node.

The tuples define as $V$ is member of the organization, $E_{p}$ created edges and timestamp of internal of messages transfer in network with difference time between nodes, $W_{p}$ is basically messages exchanges between nodes numbers, $X_{p}$ is position of node as static and total number message transfer between nodes time interval is dynamic with $p$ time.

**Definition 2: Dynamic Event Flag Function**

We define flag function $f(G_{p} - k.p) \in \{0, 1\}$ to be flag function of order $k$. Where $k$ is time order. where $(G_{p-k}, G_{p-k+1}, \ldots, G_{p})$

such that $f(G_{p} - k.p) = \begin{cases} 
1, & \text{if an event occurs at time } t \\
0, & \text{otherwise} 
\end{cases}$

The event might depend not only on the current graph snapshot $G_{p}$ but also on the $k$ the previous snapshot $G_{p-k}, \ldots, G_{p-1}$. This allows the function $f$ to model events that depends on the network changes. They define a similar function $\Delta$ for the early detection (or forecasting) of events $\Delta$ snapshots into
the future occurrence events in context. After nodes events occurrence, this occurrence used the PSO algorithm.

3.3 Optimization of IoUT Network

An intelligent artificial network is part of nature-inspired computing and uses nature algorithms to optimize nature-based problems. The fish swarm algorithm is mainly used for optimizing the global searching for neural networks. This algorithm improves the multi-layer network performance. The fish swarm-based algorithm was used in IoUT to optimize some problems. Searching for nodes is tricky because the node positioning changes with different causes underwater. To avoid this problem, use the swarm (AFA) process. However, the next problem is to design a dynamic network and its deployment underwater. To handle this problem used event detection techniques and designed a dynamic network with time respect (event detection processor). The PSO and dynamic network used in the underwater network consists of detecting events of nodes, what will be changing in position, what the energy label of nodes, and environment change conditions (natural disasters) [23, 24].

The events are generated underwater due to environmental changes, node position changes, or physical assaulter. These changes in different conditions to handle these events use the artificial swarm optimization algorithms [34]. This nature-inspired (NI) algorithm solves many global searching and events detection problems. The article is based on the social behavior of Fish based techniques. Li Xiao-Lei first proposed this concept in 2002. The Fish sense organ work on the dynamic change of environments. So, this concept is used in underwater network detection of sensor nodes and occurs the error of the network.

The optimization approaches are based on the relationship between swarm methods and ordinary movements of human classes. This technique produces real-world optimization obstacles. In the environment, the social behavior of fish links traversed to produce an algorithm called Fish Swarm Optimization Algorithm (FSOA), based on the performance of the fish swarm and searching for the meal.

These conditions mainly work based on Fish, first for searching, second for swarming, and third for following the path. The underwater network deployment assumes various functions based on an artificial fish algorithm (AFA). The swarm intelligence (SI) technique and called particle swarm optimization (PSO). The PSO solves the non-linear optimization problem. The algorithm also provides the random solution of the network optimization algorithms to solve with the population of random solutions and fitness values. However, the PSO algorithm has some disadvantages, such as parameter selection and slow convergences. These algorithm is implemented in python.

**Definition of AFA**

So, use the AFA to define three functions based on fish behaviors.

\[ AFA_p = \text{is food searching (nodes detection)} \]

\[ AFA_s = \text{Collection of fish (as like networks nodes)} \]
AFA\(_f\) — follow the path of the network and track the food locations.

Then define a function for optimization such as:

Let the \(i^{th}\) position of the network in N-dimensions vector define as \(X_i = \{X_1, X_2, X_3, ..., X_n\}\) where \(i = 1, 2, 3, ..., n\). and \(X_j = X^1_j, X^2_j, X^3_j, ..., X^n_j\) as random select visual points of selected of \(X_i\). Suppose:

\[
Y_i = F(x), \quad (1)
\]

\(F_i = \text{Fitness function of } i^{th} \text{ nodes position in populations.}\)

\[
\Delta_{ij} = x_{-i} - x_{-j} \quad (2)
\]

difference of time (event) nodes position and calculated as:

\[
X_j - X_i = \text{range.random()}, I(0,n) \quad (3)
\]

\[
S_r = \{X: X_i - X_j < \text{vision}\} \quad (4)
\]

\[
X_{next} = X_i + (X - X_i)/\text{X-X}_{-i}.\text{hop.random()} \quad (5)
\]

Where Num = The max iteration (steps counts), \(F_i = \text{Fitness function of node position } x, \Delta_{i,j} = \text{nodes distance between } i \text{ and } j \text{ positions, vision = fish visual range, random() = pick random number between } \{0, 1\}, \text{hop = moving steps length of fish algorithm, } S_r \text{ is the collection of AF range from current position (near nodes positions), } x \text{ is the types of fish behavior as } X_j \text{ for prey, AFA}_p \text{ food searching and } X_c \text{ for swarm.}\)

### 3.4 Security Model of IoUT

The IoUT security model is based on different security services as:

- **Authentication** is verification that a legitimate sender transmitted the information. Authentication and verification are entirely related because two or more things confirm each other’s authenticity. They produce secret keys over the open channel to transfer information securely. Conversely, an previously authorized key can be managed to perform authentication [14]. This security service is necessary for underwater network force and marine applications.

- **Confidentiality** means that data is not available to unauthorized third parties. Therefore, Confidentiality is significant applicability, such as naval monitoring, and the authorized device to transmit information should be confirmed.

- **Integrity** Ensures that no information has tampered from an opponent. Various sensors, such as water condition monitoring, soil monitoring, water’s ph value monitoring, node dynamic position changes monitoring, and message integrity, defend these problems in the underwater environment from IoUT application.
• **Availability** Availability of the information should be available when required by an authorized user. The absence of availability of some attackers, such as DoS attacks and DDoS, would significantly alter time and search applications. The availability ensure the forecasting of seaquakes.

The ID-Based digital signature scheme provides information integrity, message origin authentication, and non-repudiation services. The security scheme uses the ECC-based digital signature techniques to encryption/decryption messages. Based on cryptography analytical problems, these security algorithms construct and protect the IoUT based applications.

The proposed security algorithms are based on some complex problems and models (ROM) of cryptography, such as: [39–41].

1. First, the $S^2BGA - EC$ scheme is based on discrete logarithm problem (DLP) and Diffie-Hellman Assumptions (DHAs).
2. Second, the $S^2BGA - EC$ scheme uses Elliptic curve cryptography (ECC) and removes the interoperability and intractability problems of IoUT applications [31].
3. Third, the $S^2BGA - EC$ scheme uses the Random Oracle Model for the correctness and a hybrid encryption/decryption technique for privacy-preserving messages.

**Digital Signature Algorithm (DSA)**

The digital signature is based on elliptic curve cryptography algorithms and SHA-1 algorithm. The SHA-1 algorithm is a crypt-formatted hash function used in the field of cryptography and crypt analytics that takes a minor input and generates a string that is 160 bits, commonly known as a 20-byte hash value, long. The resultant hash value is a message digest and is commonly represented and created as a hexadecimal number with 40 digits. This digital sign has key setup, key generation, sign generation, and signature verification algorithms. This setup is based on DLP, DHA and SHA-1.

**Session Key Generation For sender and receiver**

**Algorithm 1 Parameter Generation**

**Require:** Pick p,q and g prime number parameters

**Ensure:** p, q and g

Let p is prime with 160 bit, q is large prime with 1024 bits as $q | p - 1$
Pick generator g from cyclic group with order $g \in Z_p^*$
Pick $h \in Z_p^*$ and compute $g = h^{p-1}/q$ mod n
1 to i
Repeat until $g \neq 1$
Parameter p,q and g
Let Sender Node A’s private key is: \( n_A \).
And public key of Node A is: \( p_A \).
To create a session key as: \( K = n_A \cdot p_B \).
Let Receiver Node B’s private key is: \( n_B \).
And public key of Node B is: \( p_B \).
To create a session key as: \( K = n_B \cdot p_A \).
To assign the Node id for sender node and send message to another nodes with assign value \( \hat{e}_1 \), the sender assign value by Hash function as \( e_m = \text{hash}(\text{msg}) \).
S. t. \( \hat{e} = \hat{e}_1 \oplus e_m \).
Where \( \hat{e}_1 = \hat{e}_{id} \cdot K \) and \( \hat{e}_{id} = \hat{e}_1 / K \).

In the, process the receiver receive the cipher message (msg) and eliminate the \( \hat{e}_{id} \) value from \( \hat{e} \). Then find the original message of node with ID. The ID show the identity of sender nodes.

**Algorithm 2** Key setup

**Require:** Let the domain parameters \((p, q, g)\)

**Ensure:** Key setup

Random integer for \( n_A \) such that \( 1 \leq n_A \leq q - 1 \).
Compute \( p_A = g^{n_A} \mod p \).
Public key is \( p_A \); private key is \( n_A \).

**Algorithm 3** Signature Generation

**Require:** Sign a message (msg)

**Ensure:** \((r, s)\) Signature generation for source node

Pick random integer \( k \) \( 1 \leq k \leq q - 1 \).
Compute \( X = g^x \mod p \) and \( r = X \mod q \).

if \( r = 0 \) then
    then step 1
end if

Execute value \( k^{-1} \mod q \)
Execute value \( \hat{e} = \text{SHA-1}(\text{msg}) \)
Compute value \( s = k^{-1}(\hat{e} + n_A r) \mod q \).

if \( r = 0 \) then
    then go to step 1
end if

Node signature \( \sigma = (r, s) \)

**Hybrid Encryption/Decryption of Messages**

The digital signature only checks the user’s identity but does not protect the
Algorithm 4 Signature Verification

Require: \((\sigma, r \text{ and } s)\)

Ensure: \(v = r\) To verify signature with message :

The receiver \((p, q, g)\) and public key

To verification the values \((r, s)\) with time interval \([1, q-1]\)

Compute \(\hat{e} = SHA - 1(\text{msg})\)

The value \(w = s^{-1} \mod q\)

Pick values as \(u_1 = \hat{e}w \mod q\) and \(u_2 = rw \mod q\)

Compute \(X = g^{u_1}y^{u_2} \mod p\) and \(v = X \mod q\)

If \((v = r)\) then accept otherwise reject

messages. The Encryption/ Decryption techniques only protect the messages in channels.

The characteristics of hybrid encryption are as follows:

- **Secrecy:** Nobody can get information about the encrypted plaintext (except the length) unless they have access to the secret key.
- **Asymmetry:** Encrypting the ciphertext can be done with the public key, but the secret key is required for decryption.
- **Randomization:** The encryption is randomized. Two messages with the same plaintext will not yield the same ciphertext. The scheme prevents attackers from knowing which ciphertext corresponds to a given plaintext.

This scheme uses hybrid encryption/decryption techniques to secure the messages.

Let the user choose the two values as \(a\) and \(b\) then

Compute no \(n = a\cdot b\); where \(n\) is large no

Choose random value \(t\) from \(0 \leq t \leq n\) with the value \(\zeta\)

Compute \(N = 127\);

By using the values \(N, \zeta, a, b\) and \(t\) to encrypt the messages \(M\).

\[
E_{nc} = (M + \zeta) \mod N
\]  \hspace{1cm} (6)

and decrypt the message use the key \(\zeta\) and \(E_{nc}\)

\[
M' = D_{ec} = (E_{nc} - \zeta) \mod N
\]  \hspace{1cm} (7)

Thus, the original message \(M = M'\)

Change every alphabet letter into plaintext \(M\) to an ASCII code. Apply encryption algorithm and obtain ciphertext. Convert ciphertext into the printable characters ASCII range (32 to 126) with modification ciphertext = mod \((C; 95) + 32\) in python 3.9.6 on each value of ciphertext.

Next, use the Elliptic curve encryption/decryption techniques based on a hybrid method to protect the message as:

\[
C = [(k.G), (M + kpN_A)]
\]  \hspace{1cm} (8)
and decrypt the message as:

\[ C = (C_1, C_2) \]  

(9)

**Correctness of Signature** If the Nodes wants to verify the received messages, then it performs the following computation as:

Let us suppose the signature scheme \((r,s)\) and \(v = r'\)

Then \[ X = X \mod q \]

\[ = (g^x \mod p) \mod q \]

\[ = (g^x \mod q) \mod p \]

\[ = X \mod q \]

\[ = r \]

**Example of First Encryption/Decryption Methods.** The character (value) \(= a*b \mod 127\) where \(N = 127\), if value less than 95 then add the 32 values and find the ASCII value’s of characters. The hybrid scheme has used the equation (6)(7)(8) and (9) to encryption/decryption the messages by elliptic curve cryptography is shown in Table 3.

<table>
<thead>
<tr>
<th>Table 3 Encryption and Decryption messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plaintext M</td>
</tr>
<tr>
<td>Ascles values</td>
</tr>
<tr>
<td>Encrypt: ((M + \zeta) \mod N)</td>
</tr>
<tr>
<td>Cipher text (C_i)</td>
</tr>
<tr>
<td>Decrypt: ((M - \zeta) \mod N)</td>
</tr>
<tr>
<td>Message</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>H e l p y o u</th>
<th>72</th>
<th>101</th>
<th>108</th>
<th>80</th>
<th>121</th>
<th>111</th>
<th>117</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt:</td>
<td>81</td>
<td>110</td>
<td>117</td>
<td>112</td>
<td>35</td>
<td>120</td>
<td>126</td>
</tr>
<tr>
<td>Cipher text</td>
<td>Q</td>
<td>n</td>
<td>u</td>
<td>p</td>
<td></td>
<td>#</td>
<td>x</td>
</tr>
<tr>
<td>Decrypt:</td>
<td>72</td>
<td>101</td>
<td>108</td>
<td>80</td>
<td>121</td>
<td>111</td>
<td>117</td>
</tr>
<tr>
<td>Message</td>
<td>H</td>
<td>e</td>
<td>l</td>
<td>p</td>
<td>y</td>
<td>o</td>
<td>u</td>
</tr>
</tbody>
</table>

3.5 Attacker model

In underwater networks, analyze the pair-based levels of attackers according to their expansive track information [9, 11, 12]. Whenever attackers offer the shortest path, their development costs progress by node discovery services. Meanwhile, the attackers admit the first-level attack to offer an unreliable address. The reputation values decrease from Node’s services. At that time, attackers admit a second-level attack, and nodes offer a correct address. However, their essential information is decreased from UAV nodes with a bypass. The Node assumes attackers and intermediary nodes do not modify their integrity during service. Reliability and authencity are essential in the scheme. So, attackers may continuously decrease the number of attacks, which tamper with their reliability preferences and enhance assistance possibilities[28].

The security algorithm is used in the IoUT network and analyzes the protocol’s security. Therefore, users adapted this model to estimate and validate the security in the network and stated authentication and key transfer protocol after identifying the successful asymmetric essential encryption/decryption
The inter-vehicle and AUVs information can be modified from denial-of-service (DoS) actions. So, review the standard attacks model, estimate their vulnerabilities, and acceptable private protection model to decrease the attacks. The proposed scheme perfectly defines an adversary reaction model as follow:

- An adversary can assume authentication protocol is definitely in the IoUT network. He/she can manage the public other way and join the protocol.
- An adversary can monitor, prevent, remove, or alter each message forwarded in a vulnerable medium but not use these unconfident mediums.
- An adversary can save the prevented information and re-transmit it to the added authorized nodes or forge information and communicate it to malicious Nodes.
- An opponent can obtain a node’s information (Node identity) in the network and remove messages collected in specific objects (nodes).

The following attacks and issues may be present in the IoUT application.

### 3.5.1 Replay Attack

A replay attack occurs when a cyberpunk monitors reliable network transmission. The attacker prevents messages and then illegal blocks or resends them to misinform the nodes and appended nodes’ danger replay attacks. A hacker does not require high-level abilities to convert the ciphertext of a message after carrying it from the underwater network. The attacker may be victorious single and resend the message to the entire device in the IoUT application and the replay attack shown in Figure 5 [13].

### 3.5.2 Jamming Attack

In the IoUT network, underwater communications over acoustic channels are numerously weak to hateful aggression—the typical notable malicious attack in the mechanical layer. A spiteful connection that explores interrupting the
connections between source nodes to destination nodes, the middle nodes are like a jammer in a jamming action. A jammer conflicts with the busy waterways of standard nodes by assigning various signs on the identical wavelength connection. However, the wavelength frequency of audial information is limited (from Hertz to kilohertz), underwater sensor nodes do unprotect from jamming attacks. The jamming attack makes a group of sensor nodes into consecutive, pulsed, and reactive jamming. In successive jamming initiatives, the radio transmitter constantly delivers numerous unusable messages and thus consumes its energy instantly. Therefore, reliable nodes can change to hibernation mode and perform wake-up continuously. The radio transmitter can rearrange inactive and powerful performance conventions in pulsed jamming attacks. In the illustration, the radio transmitter can preserve its energy failure and randomly fraudulent the network. Consequently, valuable links can communicate during the jammer’s rest time and notify the attacks TBSSP. According to authorized connections performance restrictions, the radio transmitter can turn to rest or work mode in reactive jamming attacks if communication identifies the jammer starts approaching in IoUT. Differently, it will convert empty receptacles in that position. The underwater network confirms connections and utilizes multi-frequency sensory approaches to convey messages.

### 3.5.3 Warmhole Attack

A wormhole is an out-of-network connection between physical locations in an application with lower latency with more capacity than regular connections. This connection uses high-speed radio or electric connections to reduce propagation time drastically. In a wormhole attack, the malicious node distributes specifically selected messages acquired at one node end to another node, and the wormhole attack is shown in Figure 6. The IoUT network nodes use the external communication link node before being inserted. As a result, spurious neighborhood creates relations when nodes are out of range from initial nodes. In the wormhole’s build, the nodes are inaccurate and considered close to one another.

### 3.5.4 Sybil Attack

Due to its multiple applications, the underwater network has grown in distinction and reduced the improvement of sensor technologies. However, this sensor network is vulnerable to various cyber-attacks due to its essential properties. The Sybil assault damaged the network, and it is the most harmful of the numerous cyber-attacks [42]. The Sybil attacks illustrate in three primary forms, which is shown in Figure 7. Some nodes choose to convey the message to the destination node in the first example, but the malicious node leaves the network. The sender sends data through another node in case two, and the connection routes to a malicious node [43–45]. In case three, node information transfers the source node to the destination node, and this attack is shown in Figure 7.
Figure 6 Warmhole Attack in Internet of Underwater Network

4 Simulation Results

The proposed approach $S^2BGA-EC$ methods for IoUT-enabled networks, which use low energy for the underwater network. The execution of the $S^2BGA-EC$ method is similar to traditional methods. This security scheme is implemented in Python 3.8.10 64-bit with pbc library and crypto based library by visual studio code 1.63.2. The proposed approach enhance the performance of ID-Based DSA and encryption/decryption of messages using key pairs. All analyses are conducted on a workstation with an Intel(R) Core(TM) i3-6100 CPU @ 2.30GHz 2.30GHz and 4 GB RAM. The public key, private key, and encryption/decryption are shown in Figure 8.

The comparison of message encryption/decryption and private key generation times (ms) with numbers of nodes results is shown in Figure 9.

As shown in figure 9, the node encryption time and node decryption time increase as the number of nodes increases. The computation times increase according to encryption/decryption messages. The key generation times also increase as the no of nodes increases simultaneously according to encryption/decryption performance with the messages transferred in bits shown in Figure 10.

Table 4 compares the computational cost of signer, verifier, and ciphertext [42-44]. The different schemes use the various values for signature generation and verification depending on the message’s length. However, our scheme uses short-time signature generation and verification of messages and the hybrid encryption/decryption techniques to provide more security than existing schemes.
The comparison includes the significant mathematical operations, such as bilinear pairing operation (B), elliptic curve point multiplication (M), and elliptic curve divisor doubling (DD), that are involved in both the proposed and existing schemes. Minor operations such as addition, division, subtraction, encryption, decryption, and hashing are used here because they require less processing time.
Table 4 compares the six existing schemes. While our approach requires a little more time than the scheme [11], the scheme provides better security. By applying hybrid approaches, the $S^2BGA − EC$ scheme contains a less 128-bit key size. Our proposed work is performed better than six existing schemes against signer, verify, total time, and ciphertext encoding times. The scheme is performed better than Ref [11] against the verifier, that value is (0.95 ms), which is (0.02ms) smaller. Our scheme is more efficient and secure than other
Figure 10 Message Encryption/Decryption with nodes

Table 4 Comparison of various schemes computation cost [11, 12, 16, 31, 32, 46]

<table>
<thead>
<tr>
<th>Ref</th>
<th>Signer</th>
<th>Verifier</th>
<th>Total</th>
<th>Cipher-text</th>
</tr>
</thead>
<tbody>
<tr>
<td>[11]</td>
<td>0.97</td>
<td>0.97</td>
<td>1.97</td>
<td>340</td>
</tr>
<tr>
<td>[12]</td>
<td>1.94</td>
<td>0.97</td>
<td>2.91</td>
<td>420</td>
</tr>
<tr>
<td>[16]</td>
<td>14.90</td>
<td>14.90</td>
<td>29.8</td>
<td>3172</td>
</tr>
<tr>
<td>[31]</td>
<td>14.90</td>
<td>29.8</td>
<td>44.7</td>
<td>2148</td>
</tr>
<tr>
<td>[32]</td>
<td>1.94</td>
<td>0.97</td>
<td>2.91</td>
<td>760</td>
</tr>
<tr>
<td>[46]</td>
<td>4.85</td>
<td>3.88</td>
<td>8.73</td>
<td>580</td>
</tr>
<tr>
<td>Our Scheme</td>
<td>0.97</td>
<td>0.95</td>
<td>1.92</td>
<td>340</td>
</tr>
</tbody>
</table>

schemes because the $S^2 BGA–EC$ approach provides more security within the same security levels. Further, it represents the scheme’s signer times and verification time in ciphertext, shown in Figure 11. (To use a small size of ciphertext values (ciphertext values*50) from 0 to 80 compute as histogram and OS represent our scheme).

5 Analysis and open research concerns

The section, to achieve an effective and responsible security model for underwater vehicles. The alteration order of nodes (e.g., add nodes automatically in applications) and key management are significant issues. The security services and simulation security services is shown in Table 5. Table 5 compares and contrasts the various IoUT security services presented by different schemes. As a result, our technique is trustworthy for forwarding
Figure 11  Comparison of various signature schemes used times in signing, verifying, total time and ciphertext values (OS = Our scheme)

Table 5  Comparison of various security services schemes

<table>
<thead>
<tr>
<th>Security Services</th>
<th>[6]</th>
<th>[9]</th>
<th>[12]</th>
<th>[15]</th>
<th>[16]</th>
<th>[17]</th>
<th>[31]</th>
<th>[46]</th>
<th>Our scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impersonation attack</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Replay attack</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sybil attack</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Jamming attack</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Warmhole attack</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Perfect forward/backward security</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Mutual authentication</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Session key agreement</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Traceability</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Anonymity</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

and backward security, traceability, and anonymity. In the underwater network, this secure technique defends against possible threats. These approaches [6],[9-10],[12],[14],[15-18] address some security concerns and counteract some assaults, but our improved scheme validates every security requirement.

- **Security:** To design a reliable transmission protocol, IoUT should initially execute the security node or destination sensor node in the network, and it is necessary. Whenever the network resists and represents the protocol that confirms the required information is fair and achievable. At the same time, users can confirm while not possible to access unapproved nodes.

- **Energy performance:** In IoUTs, energy performance becomes an essential metric because IoUT network power is limited. A power-efficient, reliable
communication protocol in an underwater network means that the protocol consumes a little potential energy on stable message transmission. Further, the reliable alteration of the protocol should be healthy for the associated movement of nodes in the network. Still, generally, not automated systems consider succeeding the difficulties.

- **Lightweight Protocol:** A reliable message protocol of IoUTs should be as flexible as possible for underwater sensor nodes that are resource-limited with low power, lacks memory, and low broadcast. So, design reliable protocols for IoUT networks to be secure and feasible for all applications.

- **Robustness:** On the other hand, the IoUT network effectively identifies the malicious links and secures the information from attackers. IoUT network is valuable and operational under multiple offenses and uses the proposed framework for solving all issues.

- **Space Complexity** The amount of space (memory) required to operate a cryptographic algorithm as a function of the input length is known as the algorithm’s space complexity. The complexity of space depends on the size of any input. The complexity is referred to as the worst-case complexity if the input size for the for loop is specified. The complexity is taken as the maximum complexity over all inputs of that size. Additionally, the complexity is known as the expected complexity if it is considered as the average complexity over all inputs of a given size.

- **Computational Complexity** A measure of the amount of computing resources (time and space) that a particular algorithm consumes when it runs and Computational complexity may refer to any cost models. The computation cost compute by the formula as
  \[
  \text{computation cost} = \left(\frac{(\text{existing scheme} - \text{proposed scheme})}{\text{existing scheme}}\right) \times 100 \quad [11]
  \]

### 6 Conclusions

Our enhanced mechanism is more efficient and prevents the information from various possible threats in IoUT applications. First, solve the dynamic network problem with a dynamic graph. Second, solve the node detection and optimization problems with an AI-based AFA algorithm and the last secure connections between devices. So, we established a realistic application scenario for the underwater network.

For future research, we will extend our research to create protocols to solve the key management of the network’s nodes and reduce communication secure data size and enhancement of the exploration capability of PSO based algorithms by incorporating ECDSA scheme exploration and a hybrid scheme the offsetting mechanism, and protecting the information of the air-water communication system.
Declarations

Some journals require declarations to be submitted in a standardised format. Please check the Instructions for Authors of the journal to which you are submitting to see if you need to complete this section. If yes, your manuscript must contain the following sections under the heading ‘Declarations’:

• Funding (Not applicable)
• Ethics approval (Not applicable)
• Consent to participate (Not applicable)
• Consent for publication (Not applicable)
• Availability of data and materials (Not applicable)
• Code availability (Not applicable)
• Authors’ contributions
• Conflict of interest/Competing interests (check journal-specific guidelines for which heading to use)

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in the paper.

☐ The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

If any of the sections are not relevant to your manuscript, please include the heading and write ‘Not applicable’ for that section.

References


Zhang, J., Sha, J., Han, G., Liu, J., Qian, Y.: A cooperative-control-based underwater target escorting mechanism with multiple autonomous underwater vehicles for underwater internet of things. IEEE Internet of Things Journal 8(6), 4403–4416 (2020)

Lin, H.Y.: Integrate the hierarchical cluster elliptic curve key agreement with multiple secure data transfer modes into wireless sensor networks. Connection Science 34(1), 274–300 (2022)


Mirsadeghi, E., Khodayifar, S.: Hybridizing particle swarm optimization


Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- Bibliography.docx