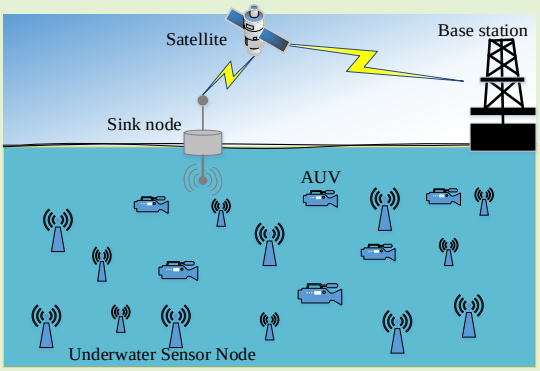
A Low-Delay Source-Location-Privacy Protection Scheme with Multi-AUV Collaboration for Underwater Acoustic Sensor Networks

Xiaojing Tian, Xiujuan Du, Xiuxiu Liu, Lijuan Wang, Lei Zhao

***Abstract*— In recent years, to protect source-location-privacy (SLP) in underwater acoustic sensor networks (UASNs), some schemes through the collaboration of multi-autonomous underwater vehicle(AUV) have been proposed. However, the long end-to-end delay in these schemes leads to untimely data delivery. To address this issue and enhance SLP protection, a low-delay source-location-privacy protection scheme with multi-AUV collaboration for UASNs (LDSLP-MA) is proposed in this paper. In the LDSLP-MA scheme, a multipath technique including multipath routing as well as multi-AUV collaboration is employed to enhance SLP protection. Additionally, through strategically assigning dwelling and target areas for AUVs, the delay taken by multi-AUV scheduling is minimized while the diversity of data transmission paths and SLP protection is enhanced. Specifically, the optimal target area is selected through grey relational analysis. Simulation results demonstrate that the LDSLP-MA scheme achieves an extended safety period, decreased energy consumption, and reduced delay compared to other schemes. Notably, in comparison to multi-AUV collaboration-based SLP protection schemes like the push-based probabilistic method for SLP protection (PP-SLPP) and stratification-based SLP (SSLP), LDSLP-MA increases the safety period by over 100%, reduces delay by over 82%, and lowers average node energy consumption by over 65%.**



***Index Terms*— SLP, UASNs, Low-delay, Multi-AUV collaboration, Multipath routing**

I. Introduction

UNDERWATER acoustic sensor networks(UASNs) play a critical role in fields such as national defense and security, resource exploration, tsunami warning systems, and marine habitat monitoring [1]–[4]. Due to the absorption of water, radio signals attenuate heavily when propagating in water and can only propagate over long distances at ultralow frequencies (3-30 kHz), which requires a large antenna and high transmission power. Optical signals have large scattering in water. Therefore, acoustic waves are the most effective carriers for long-distance information transmission in water, and acoustic signals are used for communication in UASNs [5], [6]. UASNs present many challenges, such as low bandwidth, long propagation delay, dynamic network topology, energy limitation, and node mobility [7].

UASNs usually comprise underwater sensor nodes, AUVs, a surface sink node, and a ground-based base station [8]. UASNs operate as source-driven networks, so the network may fail if the source node is attacked[9]. Consequently, several researchers have begun investigating source-location-privacy (SLP) protection in UASNs. Most SLP studies in UASNs rely on multi-AUV collaboration, which is challenged by significant end-to-end delays caused by AUVs. Compared to ordinary underwater nodes, AUVs are autonomous, flexible, and adaptable to complex environments, making them indispensable in underwater scenarios [9], [10]. This paper proposes a low-delay source-location-privacy protection scheme with multi-AUV collaboration for UASNs (LDSLP-MA), focusing on protecting SLP and minimizing end-to-end delay. In our study, an area division algorithm based on the KD-Tree, a multi-constraint-based multipath routing (MCMR) algorithm, and a method for minimizing delay in multi-AUV scheduling are the main contributions, which are summarized as follows.

(1) The MCMR algorithm is proposed to enhance SLP protection, optimize network performance, and avoid the void area routing problem. It constructs an objective function to

This work was supported in part by the Natural Science Foundation of Qinghai Province of China under Grant No. 2024-ZJ-929, in part by the National Natural Science Foundation of China under Grant No. 61962052. (Corresponding author: Xiujuan Du.)

Xiaojing Tian, Xiuxiu Liu, Lijuan Wang, and Lei Zhao are with the College of Computer and the Qinghai Provincial Key Laboratory of IoT, Qinghai Normal University, Xining 810008, China (e-mail: 1984159821@qq.com; 1154894860@qq.com; 1041517271@qq.com; leizhao0515@163.com).

Xiujuan Du is with the College of Computer, Qinghai Normal University, Xining 810008, China, and with the Qinghai Provincial Key Laboratory of IoT, Qinghai Normal University, Xining 810008, China, and also with the State Key Laboratory of Tibetan Intelligent Information Processing and Application, Xining 810008, China(e-mail: dxj@qhnu.edu.cn).

generate diverse transmission paths for SLP protection, while multi-constraints are incorporated to form a penalty function to penalize the nodes that could degrade network performance. The candidate node that ensures SLP security and better network performance is chosen as the best next-hop based on the cost function from the objective and penalty functions.

(2) Existing SLP protection schemes with multi-AUV cooperation suffer from significant delays. To address this, a multi-AUV scheduling method is proposed to enhance SLP security and minimize the delay caused by inefficient multi-AUV scheduling. This method divides the 3D UASN network into several sub-areas and rationally allocates the dwelling and target areas of AUVs, thereby dispersing data transmission paths and preventing long-distance AUV cruising.

(3) The LDSLP-MA scheme is designed based on the MCMR algorithm and multi-AUV collaboration to achieve more decentralized multipath routing, extending the adversary's search range. In addition, delays caused by packets waiting to be collected and AUVs cruising are eliminated.

The rest of the paper is organized as follows. Section II reviews the traditional SLP protection schemes that utilize multi-AUV collaboration for UASNs. Section III discusses the system models and assumptions. The LDSLP-MA scheme is described in detail in Section IV. Section V evaluates the performance of the LDSLP-MA scheme. Finally, Section VI presents conclusions and future work.

II. Related Works

A. Source Location Privacy

SLP refers to the locations of source nodes are protected through some hiding or obfuscating methods which can prevent adversaries from inferring these positions through traffic analysis or path tracing. In wireless networks, such as wireless sensor networks(WSNs) and UASNs, the source nodes hold critical data. Once the source nodes are captured by some adversaries, sensitive information will be leaked and the adversaries can launch physical attacks. Therefore, SLP security is crucial.

The goal of SLP research is to make it difficult for adversaries to accurately determine the source's location, even through network traffic monitoring and path analysis, which means the probability of an adversary identifying the actual source node tends to zero, this can be depicted by fomula (1).

$$P\left(\hat{L}_{\mathrm{s}} = L_{\mathrm{s}}\right) \rightarrow 0 \tag{1}$$

where $\hat{L}_{\mathrm{s}}$ indicates the adversary's inferred source location, and L_{s} denotes the actual source location.

Typically, an adversary monitors traffic or traces packets to infer potential source nodes. The security of SLP depends on the amount of information about node locations gathered by the adversary. Therefore, entropy serves as a measure of the security of SLP. When the adversary believes that every node in the network has an equal probability of being the source node, the entropy value reaches its maximum, indicating the strongest SLP security. The entropy for SLP is defined by Eq. (2).

$$S(p_i) = -\sum_{i=1}^{n} p_i \log(p_i) \tag{2}$$

where n represents the total number of nodes in the network, and p_i denotes the probability that the ith node is the source node.

B. SLP in WSNs

Ozturk et al. provided firstly the concept of SLP in WSNs [11], and sparked extensive research into SLP protection. Current common techniques of SLP protection in WSNs include fake packet injection, ring routing, phantom routing, random walk, and multipath routing.

Fake packet injection is a privacy protection technique proposed originally by Kamat et al. for SLP. Fake packet injection is designed to deceive adversaries by injecting fake packets into the network, and mask the real data flow as well as the source node's location. With fake packet injection, when a node receives a real packet, it generates a fake packet with a certain probability to mislead its adversaries [12] . He et al. [13] proposed a scheduling mechanism to guide fake packets to be transmitted near the backbone path and confuse adversaries. The above technique enhances SLP by increasing traffic complexity and obscuring the communication path. However, it results in high energy consumption, thus it is unsuitable for energy-constrained UASNs.

Ring routing is a privacy-preserving technique through which packets are transmitted along a loop path, and adversaries are guided into the ring, thus SLP is protected. Wang et al. [14] proposed a ring routing technique through which real and fake packets are transmitted along a loop path, thus the adversaries are confused and hard to discover the source's location. Long et al. [15] proposed a ring-based routing scheme in which packets are sent to the nearest ring and routed along it. The ring path is changed periodically and irregularly to enhance location privacy and thwart attackers'tracking attempts. Frankly, while ring routing effectively protects SLP, routing packets along the ring significantly increases energy consumption and delay, thus it is unsuitable for UASNs.

Phantom routing is a privacy-preserving technique in which phantom nodes are introduced into the routing path to obscure the source node, and it is difficult for adversaries to distinguish the real source from the phantom nodes. Ozturk et al. [11] presented flooded phantom routing, which operates in two phases. During the first phase, packets are randomly transmitted from the source to a phantom node using unicast. During the second phase, packets are flooded from the phantom node to the sink. Subsequently, to reduce energy consumption by flooding, Kamat et al. [12] proposed single-path phantom routing, which uses the shortest path in the second phase. This reduces energy consumption as well as SLP security. Additionally, to address the low SLP security resulting from the centralization of phantom nodes, Chen et al. [16] provided an SLP protection scheme based on virtual sector routing, and improved the dispersion of phantom nodes as well as SLP security. However, it introduces the issue of long detours. To summarize, single-path phantom routing is more suitable

for UASNs, however, the selection of phantom nodes is a challenging problem.

Random walk is a privacy-preserving technique through which packets are forwarded along paths chosen randomly, and it is difficult for adversaries to determine the source's location. Tang et al. [17] investigated a random walk technique through which packets are delivered randomly and unpredictably, thus enhancing SLP security. However, the random walk technique leads to significant energy consumption and delays since the packets may reach the sink via extensive detours. To address these issues, Gu et al. [18] presented a new random walk technique that utilizes short or long random walks to enhance SLP protection. Although the new random walk technique reduces energy consumption and latency, these challenges remain significant compared to other methods, rendering it unsuitable for UASNs.

Multipath routing is a privacy-preserving technique through which different packets from the same source are routed along different paths. Multipath routing enhances SLP protection by expanding the adversary's search range. Wang et al. [19] put forward a Random Parallel (RP) routing algorithm, which implements multipath routing. However, the presence of parallel paths facilitates the adversary's inference of the source node direction. To address the issue, Mutalemwa et al. [20] presented a proxy node-based decentralized multipath routing method, though the method suffers from high latency due to long detours, it is suitable for SLP protection in 3D UASNs. Nevertheless, issues such as high latency and other performance challenges still need to be addressed.

C. SLP in UASNs

SLP protection in UASNs is a precondition for underwater acoustic reliable communication. Currently, research on SLP protection in UASNs is in its infancy, with most studies focusing on multi-AUV cooperation. Multi-AUV cooperation refers to the collaborative operation of multiple AUVs, utilizing their flexibility and cooperative capabilities in underwater environments to collect and transmit data packets. The following are existing SLP protection schemes for UASNs that utilize multi-AUV collaboration.

Han et al. proposed a stratification-based source location privacy (SSLP) scheme for UASNs [21]. The scheme divides a UASN into two layers, a static layer and a dynamic layer, each equipped with an AUV that has a random initial position. The source nodes are deployed in the static layer to sense underwater data, and the movement trajectories of the AUV are influenced by the wake-up states of all the nodes in this layer. In the dynamic layer, sensor nodes are clustered using the K-means algorithm, and the AUV in this layer utilizes the Q-learning algorithm to plan its motion trajectories. Data transmission between different layers is done through the AUVs in the two layers. Additionally, fake data sources are established in the network, and the data collected and transmitted by the AUVs include real and fake packets.

Wang et al. proposed a push-based probabilistic method for source node location privacy protection (PP-SLPP) for UASNs [22]. The scheme protects SLP in UASNs through fake packet injection mechanisms, multipath techniques, and multi-AUV collaboration to combat passive attacks. The scheme uses the mean shift algorithm for clustering in the dynamic layer and the K-means algorithm for clustering in the static layer, and it calculates the value of information (VoI) for each cluster. Each cluster pushes its VoI to the leader AUV using the VBF routing protocol. The leader AUV ranks the VoIs using the KNN algorithm and dispatches two follower AUVs to successively collect packets from the clusters with higher VoI. In addition, this scheme injects fake packets into the network to confuse the adversary.

Wang et al. proposed a source location privacy protection (BNCSLP) algorithm for UASNs based on backbone network construction and multi-AUV collaboration [23]. A backbone network is constructed to select fake sources from these backbone nodes and calculate the probability of fake packet transmission to address the high energy consumption issue. Simultaneously, to reduce the delay in data collected by the AUVs, the scheme divides the network into different areas based on thiessen polygons. A merge and update area mechanism was incorporated into the data collection phase of the AUVs. This dynamic merging process makes it more difficult for the adversary to locate the source node and shortens the AUVs' traveling paths, which balances network security and delay.

Wang et al. proposed a network coding-based scheme called the stratified source location privacy protection scheme (SSLP-NC) to resist decodable adversaries [24]. The SSLP-NC scheme provides different fake source selection mechanisms for shallow and deep water layers. The scheme encodes a mixture of real and fake packets to enhance the privacy of the packet content and counteract adversaries to initiate proactive attacks through decoding. For passive attack adversaries, multiple paths are established through nodes and AUVs to deliver encrypted real and fake packets, making it difficult for the adversary to trace the packets. Therefore, this scheme effectively protects the SLP from both active and passive attacks.

The aforementioned schemes achieve SLP protection, however, they come at the cost of long delays or high energy consumption. Specifically, these schemes use fake packets to mask real traffic, protecting SLP but significantly increasing energy consumption, which is unacceptable for energy-limited UASNs. Additionally, AUVs usually move at a speed of about 8 m/s in water, which is significantly slower than the speed of in underwater sound(1500 m/s) [22], [25]. This discrepancy leads to a significant increase in delay, thus existing SLP protection schemes with multi-AUV collaboration for UASNs suffer from excessive energy consumption and delays.

Table I lists the qualitative comparison of current SLP techniques. From Table I, it can be seen that multipath routing has good adaptability in UASNs considering SLP protection level, energy consumption and delay. Consequently, based on multipath routing, we propose a low-delay SLP protection scheme with multi-AUV collaboration (LDSLP-MA) for UASNs. Significantly, multipath routing faces two challenges. Firstly, it decreases the network performance, including increased delay and energy consumption. Secondly, centralized

TABLE I
PERFORMANCE COMPARISON OF SLP PROTECTION TECHNIQUES AND APPLICABILITY FOR UASNS.

Techniques	SLP protection level	Delay	Energy consumption	Applicability for UASNs
Fake packet injection [12], [13]	High	Low	High	No
Ring routing [14], [15]	High	High	High	No
Phantom routing [11], [12], [16]	Moderate	Moderate	Moderate	Yes
Random walk [17], [18]	High	High	High	No
Multipath routing [19], [20]	Moderate	Moderate	Moderate	Yes
Multi-AUV collaboration [21]–[24]	High	High	Low	Yes

transmission paths limit SLP security[20]. To address the first challenge, we propose a MCMR algorithm, which imposes a set of selection criteria on candidate nodes based on a multi-constraint mathematical model, and avoids the nodes that may degrade network performance to be chosen as the next hop node. To address the second challenge, our scheme utilizes multi-AUV collaboration to enhance the diversity of transmission paths as well as SLP security. Nevertheless, multi-AUV collaboration leads to long delays. To optimize the multi-AUV cooperation method and decrease the delay, we present a data transmission method by combining multi-hop routing with AUV transmission. The packets not collected by AUVs are delivered via multi-hop routing, while those collected by the AUVs are transmitted to the target area via the shortest path, eliminating the delays caused by waiting for collection and AUV cruising. Finally, in Section V, we demonstrate the superiority of our proposed scheme in terms of SLP security, delay, and energy consumption through simulation experiments.

III. SYSTEM MODEL AND ASSUMPTIONS

In this section, we describe the network model, the adversary model, as well as the assumptions.

A. Network model

The network model in this paper is shown in Fig. 1, which comprises the panda-hunter model [26] as well as the traditional underwater acoustic sensor network model [27], which includes a surface sink node, underwater source nodes, common underwater sensor nodes, and underwater AUVs. Packets are routed to the sink node through a combination of multi-hop routing and AUV transmissions. Notably, the panda-hunter model describes the pattern that the hunter (adversary) attempts to locate the panda (source node) by tracking the data transmission path. In our network model, the initial location of the hunter is near the sink node. The panda is located near the source node, and the location of the panda changes with the source node.

B. Adversary model

Existing SLP protection schemes for UASNs adopt the adversary model outlined in Algorithm 1 [21], [23]. In this paper, we also use the same adversary model described in

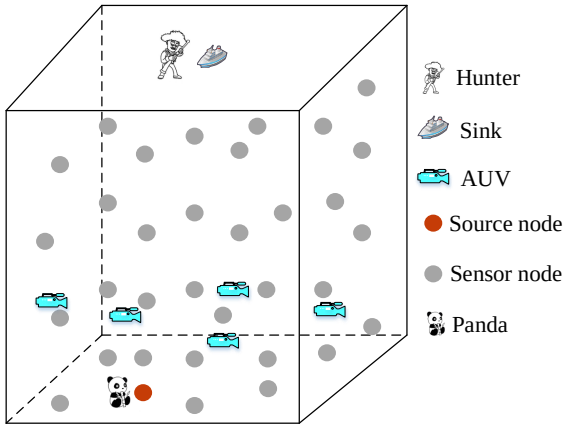


Fig. 1. Network model including panda-hunter and traditional underwater acoustic sensor networks.

Algorithm 1, which involves one adversary who gains access to the source node's location through passive attacks such as eavesdropping and backtracking. The adversary moves toward the sender's location only when it intercepts a packet. Otherwise, the adversary remains stationary. The adversary continuously monitors packets and moves toward the sender until it successfully determines the source's location.

Algorithm 1 The adversary model

```
Adversary_location = Sink_location
while Adversary_location ! = Source_node_location do
    When a adversary overhears a packet
    Adversary_location = Immediate_sender_node_location
end while
// Source_node_location found
```

C. Assumptions

1) All sensor nodes, except for the sink node, share uniform functions and parameters, including initial energy levels, monitoring range, fixed transmission power, gain, and other related characteristics.
2) Multiple AUVs are deployed in the network, each moving at a velocity of 8 meters per second.
3) The adversary is limited to performing local attacks rather than global attacks, and all other functions and parameters

remain consistent with those of the sensor nodes, with the exception that the adversary has unlimited energy.

IV. THE LDSLP-MA SCHEME

This section provides a detailed description of the LDSLP-MA scheme, including network initialization, the MCMR algorithm, the method of minimizing delay for multi-AUV scheduling, multi-hop transmission with multi-AUV collaboration, and an analysis of the LDSLP-MA scheme with a focus on delay, security, and void area routing avoidance.

A. Network initialization

1) Area division based on the KD-Tree algorithm: This paper aims to protect the SLP and optimize end-to-end delay by rationally planning the dwelling and target areas of AUVs. The 3D UASN is divided into well-stratified 3D sub-areas in this paper using the KD-Tree algorithm [28], which is as follows.

Step 1: A 3D coordinate system is established with the sink node as the origin. A data set containing n coordinates (x_i, y_i, z_i) in the 3D UASNs is generated using the Monte Carlo method.

Step 2: The variance of all data in each dimension was calculated according to Eq. (3).

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(d_i - \bar{d}) \tag{3}$$

where d_i refers to the ith data point of the dimension in the data set, and $\bar{d}$ refers to the average of all data points in the dimension. After calculating the variance of the three dimensions, the dimension with the maximum variance is selected as the split axis, denoted as L.

Step 3: The node with the median value in the dimension of the split axis is selected as the current node.

Step 4: In the dimension of the current split axis, the data points less than the median are allocated to the left branch, while those greater than the median are allocated to the right branch.

Step 5: When the split axis is the x-axis, L is set to 1; when the split axis is the y-axis, L is set to 2; and when the split axis is the z-axis, L is set to 3. Then, update the split axis according to Eq. (4). In fact, the x, y, and z axes take turns as the split axes.

$$L = (L+1)\%3. \tag{4}$$

Step 6: Repeating steps 2 to 5 to identify the left and right child nodes until all data points have been allocated. Consequently, the 3D UASN is randomly divided into hierarchical sub-areas in the form of 3D cubes.

2) Obtaining the layer information of the sub-areas: To ensure bottom-up data transmission by AUVs and reduce end-to-end delay, we assign the layer information to each sub-area and rationally plan the dwelling and target areas of the AUVs. The layer of the sub-area containing the sink node is assigned to "1". The layer for each sub-area is determined according to the minimum number of sub-areas that are subject to be traversed from the current sub-area to the sub-area with the sink node, including both the current sub-area and the sub-area containing the sink node.

3) Obtaining the neighbor information: To establish effective communication between neighboring nodes, each node maintains a neighbor table. The sink node periodically broadcasts hello packets which are flooded by other nodes, thus each node connected to the sink node can acquire the information of neighbor nodes through the received hello packets. During subsequent data transmissions, each node can update its neighbor table by listening to packets from neighboring nodes.

B. The MCMR algorithm

To design multipath routing for UASNs and protect SLP during multi-hop transmission in the LDSLP-MA scheme, a MCMR algorithm is proposed. It consists of two main components: constructing a mathematical model for multi-constraint routing and selecting the best next-hop.

To achieve multipath routing, the same sender transmits different packets via different next-hops as much as possible. However, pursuing diverse next-hops may lead to poor network performance, such as increased end-to-end delay and energy consumption, and even may affect the normal transmission of packets. Therefore, this paper proposes a multi-constraint-based multipath routing algorithm that establishes multiple constraints to avoid the selection of the next hops that would result in poor network performance.

In the face of UASNs with severe void area routing problems, this paper defines candidate nodes in a way different from the depth-based greedy routing algorithms. In the depth-based greedy routing algorithms, the neighbor nodes whose depth is less than that of the sender are considered candidate nodes. However, all the neighbor nodes in our algorithm can be defined as candidate nodes, and the candidate nodes are classified into two categories: preferred candidate nodes and normal candidate nodes. Preferred candidate nodes are the neighbor nodes whose depths are less than that of the sender. In contrast, normal candidate nodes are the neighbor nodes whose depths are equal to or larger than that of the sender. When there are preferred candidate nodes, the normal candidate nodes are not considered in determining the best next-hop. The normal candidate nodes are considered only when there are no preferred candidate nodes.

1) Mathematical model for multi-constraint routing: To enhance SLP security and optimize network performance, a mathematical model for multi-constraint routing is constructed. In this model, multi-constraints are established based on forwarding angle, depth difference, overhead, and the number of preferred candidate nodes. These constraints are then transformed into a penalty function to penalize the candidate nodes that lead to poor network performance. Simultaneously, to create multipath routes for SLP protection, an objective function is designed based on the residual energy and selection frequency of candidate nodes. Lastly, a cost function that combines the penalty and objective functions is developed to ensure the selection of the optimal next-hop node, balancing both SLP security and network efficiency.

Given the sender i, a candidate node j, the set of candidate nodes A, the set of preferred candidate nodes A_1, and the set of normal candidate nodes A_2. When there is a preferred

candidate node, the normal candidate nodes do not participate in the selection of the best next-hop node. When there is no preferred candidate node, the normal candidate nodes participate in the selection of the best next-hop node to address the void area routing problem. Thus, $A = A_1$ when set A_1 is not empty, and $A = A_2$ when set A_1 is empty. During the process of selecting the best next-hop, the MCMR algorithm imposes constraints on network parameters, such as forwarding angle, depth difference, overhead, and the number of preferred candidate nodes, as described below.

Constraint 1: To prevent packets from being delivered along a direction away from the sink node and alleviate the long detour problem, the forwarding angle of the selected candidate node μ should satisfy the constraint given by Eq. (5).

$$\mu \leq \nu \tag{5}$$

whereμ is forwarding angle, defined as the angle between the line connecting the sender i and the sink node and the line connecting the sender i and the candidate node j. ν is the angle between the line from the projection of the sink node to the sender and the line from the sender to the sink node, as shown in Fig. 2. The angles μ and ν are shown in Fig. 2.

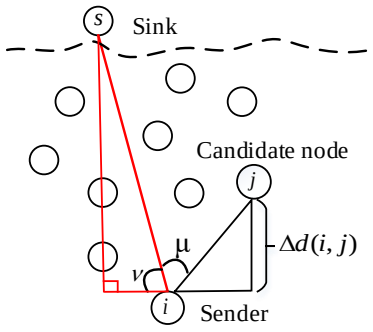


Fig. 2. Schematic of angles μ and ν in the MCMR algorithm.

Constraint 2: To avoid wasting energy, the communication overhead from the sender to the selected candidate node should satisfy the constraint given by Eq. (6).

$$cost(i,j) \leq \frac{\sum_{m=0}^{|A|} cost(i,m)}{|A|} \tag{6}$$

where m denotes the candidate node. $cost(i,j)$ represents the energy consumed by the sender i to transmit a packet with l bits to the candidate node j, which is defined by Eq. (7) [29]:

$$\begin{aligned} cost(i,j) &= E_t\left(l, dis\left(i,j\right)\right) + E_r\left(l\right) \\ &= lP_rT_d(A\left(dis\left(i,j\right), f\right) + 1) \end{aligned} \tag{7}$$

where $E_t\left(l, dis\left(i,j\right)\right)$ denotes the energy consumed by the sender to send the packet, $E_r\left(l\right)$ denotes the energy consumed by the receiver to receive the packet, P_r denotes power consumption and T_d denotes transmission delay. $A\left(dis\left(i,j\right), f\right)$ represents the attenuation of the sound signal with frequency f transmitted over the distance $dis\left(i,j\right)$.

Constraint 3: To effectively avoid the void area routing problem, the number of preferred candidate nodes for the selected candidate node should satisfy the constraint given by Eq. (8).

$$n(j) \geq \frac{\sum_{m=0}^{|A|} n(m)}{|A|}. \tag{8}$$

where $n(m)$ denotes the number of preferred candidate nodes for candidate node m.

Constraint 4: To ensure that data packet are not forwarded to the sink node by detour, the depth difference between the sender and the selected candidate node should satisfy the constraint given by Eq. (9).

$$\Delta d(i,j) \geq \frac{\sum_{m=0}^{|A|} \Delta d(i,m)}{|A|}. \tag{9}$$

where $\Delta d(i,m)$ denotes the depth difference between the sender i and the candidate node m.

In summary, the multiple constraints are given by Eq. (10).

$$\begin{cases} \mu \leq \nu \\ cost(i,j) \leq \frac{\sum_{m=0}^{|A|} cost(i,m)}{|A|} \\ n(j) \geq \frac{\sum_{m=0}^{|A|} n(m)}{|A|} \\ \Delta d(i,j) \geq \frac{\sum_{m=0}^{|A|} \Delta d(i,m)}{|A|} \end{cases} \tag{10}$$

To solve the multi-constraints problem, penalty functions are introduced in the MCMR algorithm. A penalty function is a method used to transform a constrained optimization problem into an unconstrained optimization problem [30]. A penalty is imposed according to the penalty function on candidate nodes that violate the constraints. The penalty function is defined as Eq. (11).

$$\begin{aligned} p(x) &= \alpha * \max\{\mu - \nu, 0\} \\ &+ \beta * \max\{cost(i,j) - \frac{\sum_{m=0}^{|A|} cost(i,m)}{|A|}, 0\} \\ &+ \lambda * \left|\min\{n(j) - \frac{\sum_{m=0}^{|A|} n(m)}{|A|}, 0\}\right| \\ &+ \gamma * \left|\min\{\Delta d(i,j) - \frac{\sum_{m=0}^{|A|} \Delta d(i,m)}{|A|}, 0\}\right| \end{aligned} \tag{11}$$

where α, β, λ and γ are weighting factors that satisfy $\alpha + \beta + \lambda + \gamma = 1$.

To implement multipath routing and balance the network's energy consumption, the objective function is defined as Eq. (12).

$$g(x) = \frac{E_{\text{init}}}{E_R(j)} + Num(j) \tag{12}$$

where E_{init} denotes the initial energy of a candidate node, $E_R(j)$ represents the residual energy of the candidate node, and $Num(j)$ denotes the selection frequency of the candidate node.

The cost function for the candidate node is given by Eq. (13).

$$f(x) = \eta g(x) + \xi p(x) \tag{13}$$

where η and ξ are the weighting coefficient used to adjust the influence of the penalty function and the objective function on the cost function, which satisfy $\eta + \xi = 1$. Since the sum

of η and ξ is a constant, when ξ is larger (η is smaller), candidate nodes with better network performance are more likely to be selected as the best next hop, while the diversity of transmission paths is reduced. Conversely, when ξ is smaller (η is larger), the candidate nodes that may promote the diversity in transmission paths are more likely to be selected as the best next hop, though this may reduce the network performance. By adjusting the weighting coefficients, candidate nodes can be dynamically selected to balance the network performance and the security of SLP, thereby achieving an effective trade-off.

The smaller the cost function, the higher probability that this candidate node is selected as the best next-hop. This mathematical model makes it easier to select the candidate nodes with higher residual energy, lower selection frequency, and those meet the constraints as the best next hop, thus implementing multipath routing and enhancing SLP protection, while also ensuring good network performance.

2) Selecting the best next-hop: The best next-hop is selected according to the mathematical model for multi-constraint routing. The specific process of selecting the best next-hop is as follows.

Step 1: Identify the set of candidate nodes available to the sender;

Step 2: Compute the value of the cost function for each candidate node based on the mathematical model for multi-constraint routing;

Step 3: Select the candidate node with the minimum value of the cost function as the best next-hop;

Step 4: Iterate through Steps 1 to 3 until the packet reaches the sink node.

In summary, the best next-hop is determined according to the mathematical model for multi-constraint routing in the MCMR algorithm, which achieves multipath routing extends the adversary's search range, and enhances SLP protection. Additionally, the residual energy and the number of preferred candidate nodes are considered to prevent the nodes from premature death due to energy exhaustion, avoid the packets to be delivered to the sparsely deployed areas thus solve the void area routing problem. Furthermore, to avoid the long detour problem, depth difference and forwarding angle are taken into account to ensure that packets are always forwarded by the nodes closer to the sink node. Lastly, residual energy and overhead are considered to extend the network's lifetime. In conclusion, the MCMR algorithm effectively protects SLP, avoids the void area routing problem, prevents long detours, and prolongs the network's lifetime.

C. Minimizing delay in multi-AUV scheduling

The utilization of AUVs in USANs brings about both advantages and disadvantages. On the one hand, AUVs can address the challenge of data transmission in complex underwater environments and enhance SLP protection by diversifying the transmission paths. On the other hand, their involvement in packet transmission leads to long end-to-end delays, rendering packets time-ineffective. To enhance SLP protection and minimize end-to-end delays, a method for minimizing the delay caused by multi-AUV scheduling is proposed. This method relies on a well-stratified area division and scientific planning of the dwelling and target areas of AUVs to enhance the diversity of transmission paths and disrupt the spatial and temporal correlation of data transmission between different areas. In this way, the security of SLP is improved, and high end-to-end delay due to AUV cruising is avoided. In the LDSLP-MA scheme, the dwelling area is where the AUV collects data packets, while the target area is where the AUV delivers packets. Currently, all SLP protection schemes with multi-AUV collaboration suffer from long end-to-end delays. In this subsection, a novel multi-AUV scheduling method is proposed to reduce end-to-end delays while protecting the SLP.

1) Determination of the dwelling areas: When an AUV follows a fixed path to or from a specific area, it is vulnerable to be tracked by the adversary. To prevent AUV from being tracked by the adversary, the dwelling area of each AUV is subject to change constantly. Furthermore, if the AUVs collect packets directly from the source nodes, the risk of exposing the source node's location increases. To prevent the disclosure of the source node's location and facilitate packet collection by AUVs, the dwelling areas of AUVs are strategically located close to but at a distance from the source node's area.

After network initialization, the 3D area of the UASN is divided into multiple sub-areas, and each sub-area is configured with a layer. The dwelling areas of AUVs are determined based on the layer L_{source} of the sub-area in which the source node is located. To protect SLP and reduce the delay, the layers of all the dwelling areas are the same. The layer of the dwelling areas of the AUVs should be smaller than the layer of the sub-area where the source node is located. When the layer of the sub-area where the source node is located is less than or equal to 3 (i.e., $L_{source} \leq 3$), the dwelling areas of AUVs should be adjacent to or the same as the sub-area where the sink node is located. In this case, using the AUV to relay packets from the source node does not provide diversity of transmission paths. On the contrary, it increases the risk of exposing the source location. Consequently, the AUVs do not participate in packet transmission when $L_{source} \leq 3$. In fact, the larger the value of L_{source} , the greater diversification of data transmission paths using AUVs. To further diversify the transmission paths, the set of dwelling areas of AUVs B is set as follows.

$$B = \begin{cases} \{b \,|L\,(b) = L_{source} - 1\}, 3 < L_{source} \leq 5 \\ \{b \,|L\,(b) = L_{source} - 2\}, L_{source} > 5 \end{cases} \tag{14}$$

where b denotes the sub-area, $L\,(b)$ denotes the layer of the sub-area b, and L_{source} denotes the layer of the sub-area containing the source node. Eq. (14) ensures that the routing path of packets from the source node to the sink node passes through the designated dwelling areas, thus facilitating the AUVs to collect data. Additionally, Eq. (14) ensures the dwelling areas are away from the sub-area containing the source node at a specified distance, thus avoiding leakage of the source location.

The number of AUVs is related to the size of $|B|$, one AUV is assigned to one dwelling area to collect packets in that area. In addition, each dwelling area is numbered. To reduce end-to-end delay, the AUV travels through one or several nodes

with the least depth in that dwelling area until some packets are collected. After that, the AUV cruises along the shortest path and delivers the collected packet to the target area. If the AUV collects multiple packets, the AUV travels and delivers them to their respective target areas in the order from near to far. Upon completing the delivery of the packets, the AUV travels to a new dwelling area.

Assuming that the serial number of the current dwelling area is Num (where $1 \leq Num \leq |B|$), the serial number of the new dwelling area which the AUV is gong to is given by Eq. (15).

$$\mathrm{New}Index(Num) = (Num \bmod |B|) + 1. \tag{15}$$

From Eq. (15), it is seen that the dwelling area of each AUV in the LDSLP-MA scheme changes continuously to prevent the AUV from being tracked by the adversary. Upon reaching a new dwelling area the AUV starts to collect packets.

2) Determination of the target areas: Grey relational analysis (GRA) is a method used for correlation analysis when the data volume is small, and information is incomplete or uncertain [31], [32]. By comparing the correlation degrees of each sequence with the reference sequence, the method identifies the sequence with the highest correlation, thereby enabling corresponding decisions and optimizations.

To address uncertainty in the optimal target area, the source node specifies an optimal target area for each packet based on the GRA. Reasonably assigning a target area to each packet is an effective way to achieve path diversification and mitigate long delays. The specific process to determine the target area is as follows.

Step 1: Identifying the evaluation object and evaluation criteria.

To achieve the goals of high SLP security and low delay, it is crucial to determine the evaluation objects and criteria for GRA. The evaluation objects include all sub-areas that are smaller in layer than the dwelling area, excluding the sub-area where the sink node is located. The evaluation criteria include the layer of the sub-area, $L(b)$, the number of times the sub-area has been designated as a target area, N, the closest distance from the sub-area to the sink node, $\min(d_{\mathrm{s}})$, the farthest distance from the sub-area to the sink node, $\max(d_{\mathrm{s}})$, the closest distance from the sub-area to the source node, $\min(d_{\mathrm{source}})$, and the farthest distance from the sub-area to the source node, $\max(d_{\mathrm{source}})$. There are m evaluation objects, n evaluation criteria, a reference sequence of $x_0 = \{x_0(k) \,|k = 1, 2, \cdots, n\}$, and a comparison sequence of $x_i = \{x_i(k) \,|k = 1, 2, \cdots, n\}, i == 1, 2, \cdots, m$.

Step 2: Determining the weights of evaluation criteria.

To reasonably allocate the weights of these evaluation criteria, this paper employs the analytic hierarchy process (AHP) [33]. AHP is a multi-criteria decision-making method. By constructing a hierarchical structure model and performing pairwise comparisons of evaluation criteria, AHP helps the decision-makers to choose the best. According to the AHP, the weights of these evaluation criteria are as follows. N has a weight of 0.45, $L(b)$ has a weight of 0.24, both $\min(d_{\mathrm{s}})$ and $\min(d_{\mathrm{source}})$ have a weight of 0.11, while both $\max(d_{\mathrm{s}})$ and $\max(d_{\mathrm{source}})$ have a weight of 0.045. Thus the weights of the evaluation criteria ω are given by Eq. (16).

$$\omega = \{0.45, 0.24, 0.11, 0.11, 0.45, 0.45\}. \tag{16}$$

It is worth noting that, in the AHP, consistency checks on ω are required, which are not elaborated here.

Step 3: Determining the optimal reference sequence.

When determining a target area, the sub-areas that have not been designated as a target area (i.e., the sub-areas with $N = 0$) have the highest priority. A sub-area located in the middle of the two sub-area, the sub-area where the sink node is located and the dwelling area, is preferably determined to be the target area, i.e., $L(b) = L_d/2$, where L_d denotes the layer of the dwelling area. The optimal values of $\min(d_{\mathrm{s}})$ and $\max(d_{\mathrm{s}})$ are $D_{sd}/2$, where D_{sd} is the average distance from the sink node to the dwelling area. The optimal values of both $\min(d_{\mathrm{source}})$ and $\max(d_{\mathrm{source}})$ are $D_{ss} - (D_{sd}/2)$, where D_{ss} is the euclidean distance between the sink node and the source node. Thus, the optimal reference sequence is given by Eq. (17).

$$x_0 = \{0, L_d/2, D_{sd}/2, D_{ss} - (D_{sd}/2), D_{sd}/2, D_{ss} - (D_{sd}/2)\}. \tag{17}$$

Step 4: Data normalization

Due to the different dimensions of the evaluation criteria, it is necessary to normalize the original comparison sequence x_i. The commonly used data normalization fuctions are as follows.

a) : The cost-based normalization function is given by Eq. (18) (the smaller the evaluation criterion, the better).

$$x_i(k)' = \frac{\max x_i(k) - x_i(k)}{\max x_i(k) - \min x_i(k)} \tag{18}$$

where $x_i(k)'$ is the normalized value of the k-th criterion for the i-th object. $x_i(k)$ is the original value of the k-th criterion for the i-th object. $\max x_i(k)$ is the maximum value of the k-th criterion across all objects. $\min x_i(k)$ is the minimum value of the k-th criterion across all objects.

b) : The benefit-based normalization function is given by Eq. (19) (the larger the evaluation criterion, the better).

$$x_i(k)' = \frac{x_i(k) - \min x_i(k)}{\max x_i(k) - \min x_i(k)} \tag{19}$$

where all mathematical symbols are interpreted as in Eq. (18).

c) : The moderate-type normalization function is given by Eq. (20) (the closer the evaluation criterion to the optimal value, the better).

$$x_i(k)' = 1 - \frac{|x_i(k) - y(k)|}{\max\{|x_i(k) - y(k)|\}} \tag{20}$$

where $y(k)$ is the optimal value of the k-th criterion. $\max\{|x_i(k) - y(k)|\}$ represents the maximum difference between the k-th criterion across all objects and the optimal value. All the remaining mathematical symbols are interpreted in the same way as in Eq. (18).

Step 5: Calculating the grey relational coefficient

The formula for the grey relational coefficient is used to

measure the similarity between the comparison sequence and the reference sequence. The calculation formula is given by Eq. (21).

$$\xi_i(k) = \frac{\min\limits_i \min\limits_k |x_0(k) - x_i(k)| + \varsigma \max\limits_i \max\limits_k |x_0(k) - x_i(k)|}{|x_0(k) - x_i(k)| + \varsigma \max\limits_i \max\limits_k |x_0(k) - x_i(k)|} \tag{21}$$

where $\xi_i(k)$ represents the grey relational coefficient of the k-th criterion between the i-th object in the comparison sequence and the reference sequence. ς is the distinguishing coefficient, typically ranging from 0 to 1, with a common value of 0.5. $\min\limits_i \min\limits_k |x_0(k) - x_i(k)|$ is the minimum absolute difference between the value of the k-th criterion for all objects and the value of the k-th criterion in the reference sequence. $\max\limits_i \max\limits_k |x_0(k) - x_i(k)|$ is the maximum absolute difference between the value of the k-th criterion for all objects and the value of the k-th criterion in the reference sequence.

Step 6: Calculating the grey weighted relational degree and evaluation analysis.

The grey weighted relational degree is calculated according to Eq. (22).

$$r_i = \sum_{k=1}^{n} \omega(k)\xi_i(k) \tag{22}$$

where r_i represents the value of relational degree value of the i-th evaluation object. $r_1 \quad r_2 \quad \cdots \quad r_i$ is compared and the sub-area with the highest value of r_i is selected as the optimal target area.

D. Combining multi-hop transmission with multi-AUV collaboration

In the LDSLP-MA scheme, packets are forwarded through multi-hop or delivered through multi-AUV collaboration, aiming to protect SLP and reduce end-to-end delay. During packet transmission, the packet inevitably passes through one of the dwelling areas. When a packet is transmitted within a dwelling area within which there is an AUV, the AUV will collect the packet, then the AUV transports the packet to the target area. When a packet is unable be collected by any AUV, the packet is forwarded by the best next hop according to the MCMR algorithm. This combination of multi-hop forwarding and AUV transporting breaks the correlation between areas and creates more diverse data transmission paths and enhances the security of SLP.

The LDSLP-MA scheme eliminates the delays caused by packets waiting to be collected and AUVs cruising. By transporting different packets to different target areas, AUVs increase the diversity of data transmission paths. Therefore, this scheme not only achieves low delay but also enhances SLP security through the proposed MCMR algorithm and multi-AUV cooperation. The specific workflow of the LDSLP-MA scheme is shown in Fig. 3.

E. Analysis of the LDSLP-MA scheme

1) Low delay analysis: Current SLP protection schemes based on multi-AUV collaboration result in significant delays.

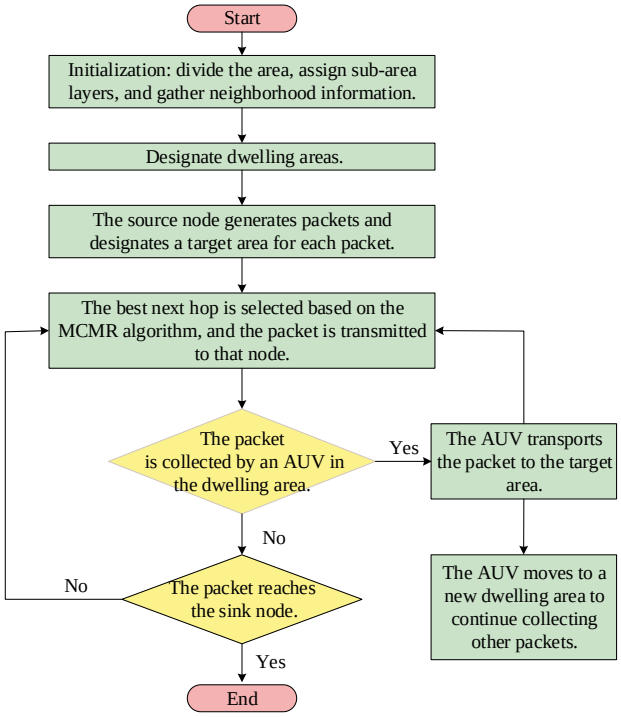


Fig. 3. The flowchart of the LDSLP-MA scheme.

The reason is that the AUVs are subject to navigating long paths to reach the cluster head and collect packets. Some schemes integrate multi-hop transmission and AUV delivery to alleviate long delay issues. However, packets transmitted to the cluster head in current schemes have to wait for the AUV to collect, which introduces additional delay, while inefficient scheduling of AUVs also increases the delays.

In the LDSLP-MA scheme, not all the packets in the dwelling area are collected by the AUV. Only some packets forwarded by the nodes with the least depth are collected by the AUV, significantly reducing delay. Additionally, the scheduling method of AUV is optimized by strategically planning dwelling and target areas to mitigate delays associated with AUV cruising. Despite AUV delivery taking longer delay than that by multi-hop transmission, our proposed AUV scheduling method substantially reduces end-to-end delay. Furthermore, in our proposed MCMR algorithm for multi-hop transmission, depth difference and forwarding angle are taken into account, effectively avoiding long detours of packets and further reducing end-to-end delay in multi-hop transmission.

2) Security analysis: In shortest-path routing and single-path phantom routing, consecutive packets from the same source node can be easily intercepted by the adversary, thereby reducing the challenge of discovering the source node's location by the adversary. In multipath routing, different packets from the same source node reach the sink node via different paths, extending the adversary's search range and making it more challenging for the adversary to discover the source node's location. Nevertheless, in the scenarios with parallel paths, consecutive packets are still easy to be intercepted by the adversary, which poses a threat to SLP.

The above challenges are addressed in our proposed

LDSLP-MA scheme. With the MCMR algorithm in this scheme different packets from the same source node are routed to the sink node through different paths, while the novel AUV scheduling method enhances the diversity of paths. When selecting a target area for a packet, the source node gives preference to the sub-area that has been designated as the target area fewer times, which not only resolves the issue of parallel path but also disrupts the spatio-temporal correlation of packets in the sub-areas. Consequently, this scheme utilizes more dispersed multiple paths for packet delivery, making harder the adversary to track the source location and thereby enhancing SLP security.

Furthermore, the AUVs following fixed trajectories between specific areas in other studies are vulnerable to being tracked by the adversary. To mitigate this risk, in our scheme, after an AUV delivers a packet to its target area, it travels to a new dwelling area instead of returning to the original dwelling area, which further hinders the adversary's tracking.

3) Void area routing avoidance: In UASNs, the void area routing problem significantly degrades the performance of routing algorithms [34]. With the depth-based greedy routing algorithms, if a sender lacks neighbor nodes with shallower depths, it may encounter packet loss because the packets are unable to be relayed continuously. To address this issue, in this paper neighbor nodes are categorized into preferred candidate nodes and normal candidate nodes. If the sender has preferred candidate nodes, only one of the preferred candidate nodes can be selected as the best next-hop. If the sender has no preferred candidate node, one of the normal candidate nodes (neighboring nodes with greater depth than that of the sender) is selected as the best next-hop.

Furthermore, the MCMR algorithm considers the number of preferred candidate nodes and avoids delivering packets to areas with sparse nodes, thereby mitigating the void area routing problem.

Uneven energy consumption causes some nodes premature death, which exacerbates the void area routing problem. To address the void area routing problem, in this scheme, the residual energy and selection frequency of candidate nodes are taken into account. In addition, packets are delivered to the sink node via diverse multiple paths, minimizing the likelihood of node death due to energy depletion, which helps to avoid the void area routing problem caused by the premature death of nodes.

Therefore, our scheme effectively addresses the void area routing problem from multiple aspects.

V. Simulation Evaluation

To evaluate the performance of the proposed LDSLP-MA scheme, we use MATLAB 2022 as a simulation tool. The LDSLP-MA is compared with SSLP [21], PP-SLPP [22], LSLPR [29], 2hop-AHH-VBF [35], CS [36] and HAMA [37] in terms of safety period, end-to-end delay, average energy consumption of nodes, and average energy consumption of AUV. Among these schemes, both SSLP and PP-SLPP are multi-AUV cooperation-based SLP protection schemes for UASNs,while CS and HAMA are multi-AUV-based schemes designed for underwater data collection. LSLPR, our previously proposed routing protocol, is designed to protect SLP in UASNs. 2hop-AHH-VBF is an energy-efficient underwater routing protocol. The comparison results for LDSLP-MA and LSLPR are based on our simulation experiments, whereas the results for other schemes are taken from [22]. It should be emphasized that all the comparison results in this paper are obtained under the same simulation environment. In the simulation experiment, each dwelling area deploys an AUV to collect packets. Then the AUV transports the collected packets to their target areas. Once the delivery is completed, the AUV goes to a new dwelling area and repeats the process. The parameters for the simulation experiments are set as in Table II.

TABLE II
Simulation Parameters.

parameter	value
Network sidelength	800m
Depth	600m-1000m
Number of nodes	500
Topology	Random uniform deployment
Packet size	1024bits
Control packet size	100bits
Node initial energy	10 J
Power consumption (Pr)	10^{-5}W
Carrier frequency(f)	20kHz
Data generation rate	100 packets per turn
AUV initial energy	∞
AUV velocity	8m/s
Unit consumption of AUV	5J/m
Node communication radius	200m
Adversary initial energy	∞
Adversary listening range	200m

A. Performance metrics

The following four metrics are used to evaluate the performance of the LDSLP-MA scheme and other comparison schemes: safety period, end-to-end delay, average energy consumption of nodes, and average energy consumption of AUV. The safety period is defined as the distance the adversary moves before locating the source, which is consistent with the definition in the literature [22]. The greater distance the adversary travels, the more challenges to detect the source's location, the higher level of SLP protection. End-to-end delay (EED) refers to the total delay experienced by a packet from the source node to the sink node. Given different end-to-end delays for different packets reaching the sink node from the source node, the subsequent EED refers to the average end-to-end delay of these packets which is given by Eq. (23).

$$EED = \frac{\sum_{j=1}^{N_{sink}} (T_{rj} - T_{sj})}{N_{sink}} \tag{23}$$

where T_{sj} denotes the time when the source node sends the packet, T_{rj} represents the time when the sink node successfully receives the packet, and N_{sink} denotes the number of packets successfully received by the sink node.

Most research on SLP for UASNs adopts the same energy consumption models for nodes and AUVs as in [22] due to their simplicity and effectiveness in typical UASN scenarios. To maintain consistency with prior work and enable comparability, we adopted the same model in our paper. Energy consumption consists of two parts: the energy consumed by the nodes and the energy consumed by the AUVs. The computational model for the energy consumption of underwater nodes is based on reference [38], and the energy consumption of nodes is calculated using Eq. (7). In this paper, the average energy consumption of nodes (AECNS) and the average energy consumption of AUV (AECA) are used to evaluate the energy efficiency of these schemes. AECNS represents the average energy consumed by a node to complete each turn of data transmission. AECA represents the average energy consumed by each AUV for each turn of data transmission.

B. The impact of coefficient η on performance

The magnitude of coefficients η and ξ in the MCMR algorithm has a significant impact on the performance of the LDSLP-MA scheme. Since $\eta+\xi=1$, this subsection focuses on the effect of coefficient η on the LDSLP-MA scheme, while the effect of coefficient ξ on the scheme is opposite to that of coefficient η. Fig. 4 illustrates the effect of coefficient η on the safety period. It can be observed from Fig. 4 that as the coefficient η increases, the safety period gradually increases and converges at $\eta = 0.8$. As the coefficient η increases, the candidate nodes with higher residual energy and lower selection frequency are more likely to be selected as the next-hop. This creates more diverse transmission paths which bring about great challenges for the adversary to locate the source node.

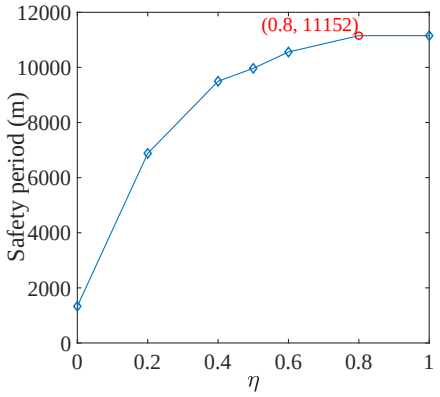


Fig. 4. Effect of coefficient $\boldsymbol{\eta}$ in the MCMR algorithm on the safety period of LDSLP-MA scheme.

The effect of the coefficient η on the EED is shown in Fig. 5. From Fig. 5 it can be seen that the EED gradually increases with the coefficient η. As the coefficient η increases, the network parameters such as forwarding angle, depth difference, overhead, and the number of preferred candidate nodes become less influential on the cost function. The selection of the best next-hop node increasingly focuses on the residual energy and the selection frequency of candidate nodes. Consequently, a packet may reach the sink node through a detour, which leads to a higher EED.

Considering the experimental results in Fig. 4 and Fig.5, to balance the safety period and end-to-end delay, the coefficients η and ξ are set to 0.5 in the following simulation experiments.

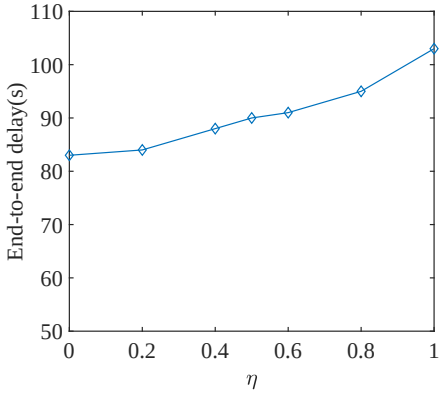


Fig. 5. Effect of coefficient $\boldsymbol{\eta}$ in the MCMR algorithm on the EED of LDSLP-MA scheme.

C. The impact of communication radius on performance

In UASNs, the communication radius of nodes significantly impacts data transmission. Fig. 6 illustrates the effect of the communication radius on the safety period. From Fig. 6, it is seen that the safety period decreases with the increasing of communication radius. This is because when the communication radius is larger, the hop-count experienced by a packet from the source node to the sink node is smaller, which facilitates the adversary to trace the source node's location. Some packets even directly bypass the AUV's dwelling area (i.e., some packets reach the sink node without the collaboration of an AUV). This reduces the diversity of transmission paths, thereby decreasing the safety period.

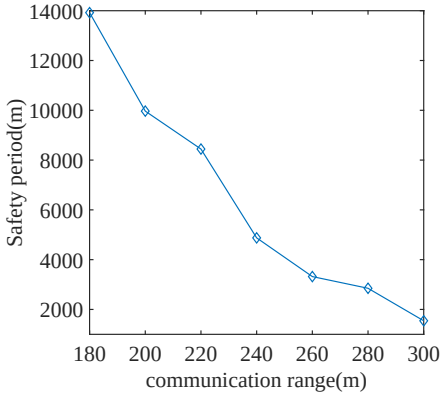


Fig. 6. Effect of communication radius on safety period of LDSLP-MA scheme.

Fig. 7 illustrates the effect of communication radius on EED. From Fig. 7, it is observed that as the communication radius increases, the EED decreases. This is because that an increased communication radius reduces the hop-count needed for the packet to travel from the source node to the sink node and reduces the use of AUVs in packet delivery, thereby decreasing the EED.

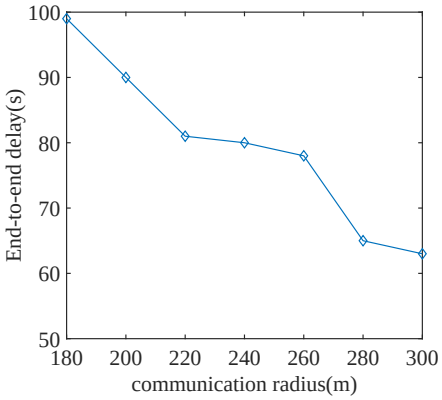


Fig. 7. Effect of communication radius on EED of LDSLP-MA scheme.

Fig. 8 shows the effect of communication radius on the AECNS. As the communication radius of nodes increases, the chance for AUVs to participate in data transmission gradually decreases, then the ordinary nodes bear most of the energy consumption required for data transmission. Additionally, with the increasing of communication radius, the hopping distance also increases, leading to higher energy consumption for nodes. Consequently, the AECNS gradually increases with the communication radius, which can be observed From Fig. 8.

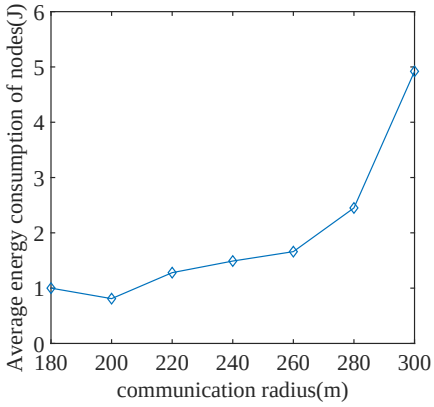


Fig. 8. Effect of communication radius on AECNS of LDSLP-MA scheme.

Fig. 9 illustrates the effect of communication radius on the AECA. When the communication radius of nodes increases, some packets may bypass the dwelling area of AUVs, reducing the AUVs' participation in data transmission. Consequently, the AECA gradually decreases as the communication radius increases. However, fluctuations are observed at 240 and 300 meters due to variations in the AUV's movement distance in each simulation.

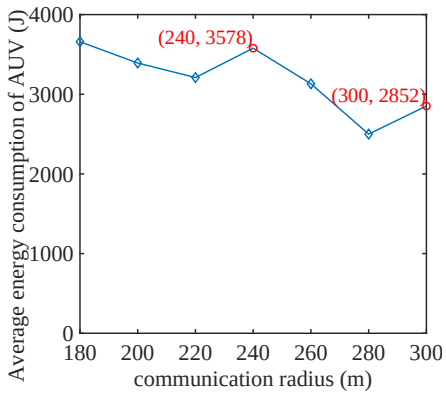


Fig. 9. Effect of communication radius on AECA of LDSLP-MA scheme.

D. Comparison experiment

To comprehensively evaluate the performance of the LDSLP-MA scheme, this subsection conducts comparative experiments of our LDSLP-MA, SSLP [21], PP-SLPP [22], LSLPR [29], 2hop-AHH-VBF [35], CS [36] and HAMA [37], which focuses on safety period, EED, AECNS, and AECA. It should be noted that the four schemes, LDSLP-MA, SSLP, PP-SLPP, and LSLPR, are designed for protecting SLP. Among which SSLP, PP-SLPP, and LDSLP-MA are designed for UASNs with AUVs while LSLPR is for UASNs without AUVs. In contrast, 2hop-AHH-VBF, CS, and HAMA schemes do not have the feature of SLP protection.

Fig. 10 shows the comparison results of the seven schemes in terms of safety period under various parameters. The LDSLP-MA scheme demonstrates a clear advantage over the other six schemes. This is because the proposed MCMR algorithm and AUV scheduling method in our LDSLP-MA scheme provide more diverse and dispersed transmission paths. Path diversity is a critical factor in enhancing SLP protection [29]. Compared to the diverse paths in the LDSLP-MA scheme, the LSLPR scheme adopts a proxy node to transmit data packets, resulting in a shorter safety period. From Fig. 10 it can be seen that the safety periods of both SSLP and PP-SLPP are shorter than those of the LDSLP-MA and LSLPR. In either the SSLP or PP-SLPP scheme, AUVs collect and transmit packets within specific areas. In contrast, the AUVs in the LDSLP-MA scheme move across multiple areas. Additionally, LSLPR employs proxy nodes to distribute packets across various areas. As a result, both LDSLP-MA and LSLPR expand the adversary's search scope, and enhance SLP protection. The multipath technique used in PP-SLPP results in a longer safety period than that of SSLP. The 2hop-AHH-VBF, CS, and HAMA schemes do not utilize any SLP protection techniques, resulting in a relatively low safety period compared to the other six schemes. The safety periods of the CS and HAMA schemes are longer than those of the 2hop-AHH-VBF scheme. This improvement in SLP security through AUV movements has been demonstrated in several studies [21]–[24]. In summary, diverse and dispersed transmission paths as well as AUV movement enhance SLP protection by increasing the unpredictability of transmission paths.

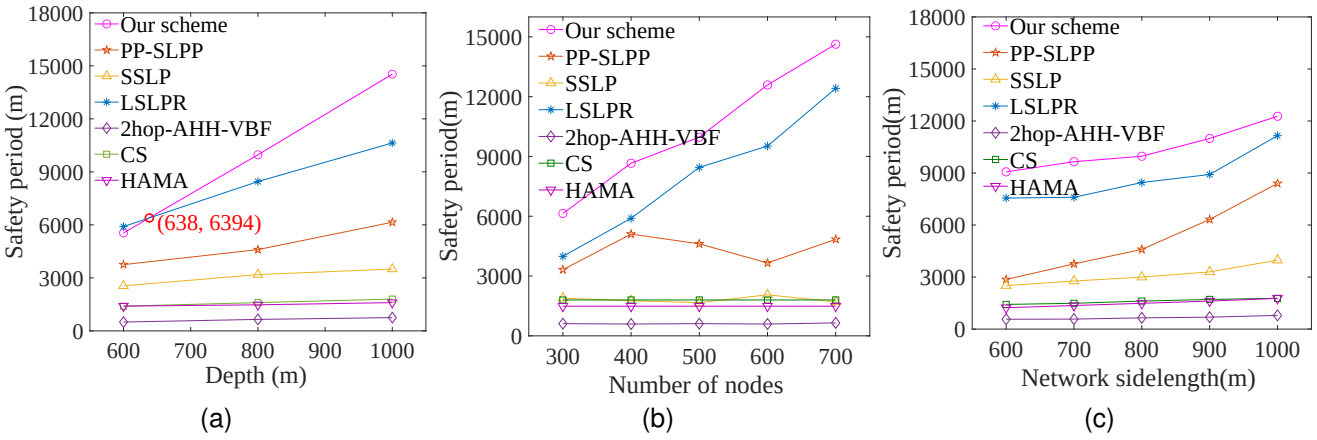


Fig. 10. Safety period comparison of LDSLP-MA, PP-SLPP, SSLP, LSLPR, 2hop-AHH-VBF, CS and HAMA under various parameters. (a) Safety period under different depths with 500 nodes and network sidelength of 800 m. (b) Safety period under different numbers of nodes with depth of 800 m and network sidlength of 800 m. (c) Safety period under different network sidelengths with 500 nodes and depth of 800 m.

From Fig. 10(a), it is observed that the safety period increases with the depth of water for all seven schemes. As the depth of water increases, the adversary has to traverse a farther distance to locate the source, resulting in a longer safety period. It is worth noting that when the depth of water is less than 638 meters, our LDSLP-MA scheme does not show any advantage over the LSLPR scheme. This is because that the reduced depth of water decreases the distance traveled by the AUVs as well as the diversity of the transmission paths. However, in the LSLPR scheme, the selection of proxy nodes is not affected by depth, thus the path diversity is maintained. From Fig. 10(b), it is observed that the safety periods of both 2hop-AHH-VBF, SSLP and HAMA schemes remain almost constant since they have fixed transmission trajectories. In the CS scheme, multiple AUVs cooperate to collect data from the oil pipeline. So, the safety period extends slowly with the number of nodes. In each experiment of the PP-SLPP scheme, the amount of location information pushed to the leader AUV is variable, thus the distance traveled by the follower AUVs is changeable. As a result, the safety period fluctuates with the number of nodes. The safety periods of both LSLPR and LDSLP-MA increase with the number of nodes. This is because that the increased number of nodes provides a more diverse selection of next-hop nodes, thereby enhancing SLP security. Fig. 10(c) depicts a gradual increase in the safety period of these schemes as the network sidelength increases. SSLP, 2hop-AHH-VBF, CS, and HAMA exhibit a slow increase in safety period as the network sidelength grows, while the other three schemes show a more significant increase.

Fig. 11 demonstrates a comparison of the seven schemes in term of EED. As shown in Fig. 11, among the five multi-AUV-based schemes, our LDSLP-MA scheme achieves the lowest EED. However, the EED of our scheme remains slightly higher than that of 2hop-AHH-VBF and LSLPR, which do not use AUVs. It is a common issue for these schemes that rely on AUVs for data collection and transmission, as highlighted in previous works [29]. The reason is that the speed of AUVs is significantly lower than that of acoustic wave in water. Additionally, AUVs cruising is also desired for collecting

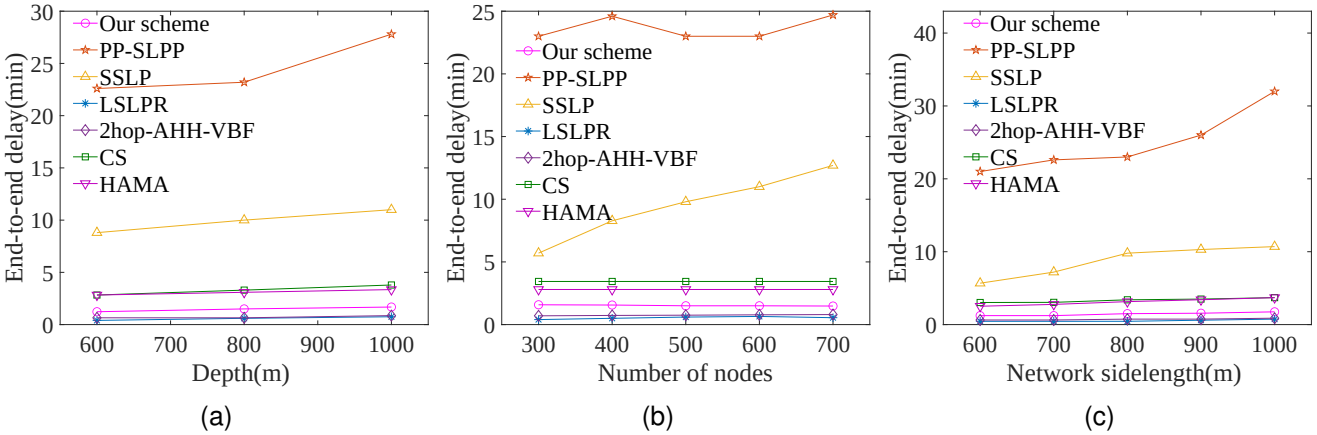


Fig. 11. EEDs comparison of LDSLP-MA, PP-SLPP, SSLP, LSLPR, 2hop-AHH-VBF, CS and HAMA under various parameters. (a) EED under different depths with 500 nodes and network sidelength of 800 m. (b) EED under different numbers of nodes with depth of 800 m and network sidlength of 800 m. (c) EED under different network sidelengths with 500 nodes and depth of 800 m.

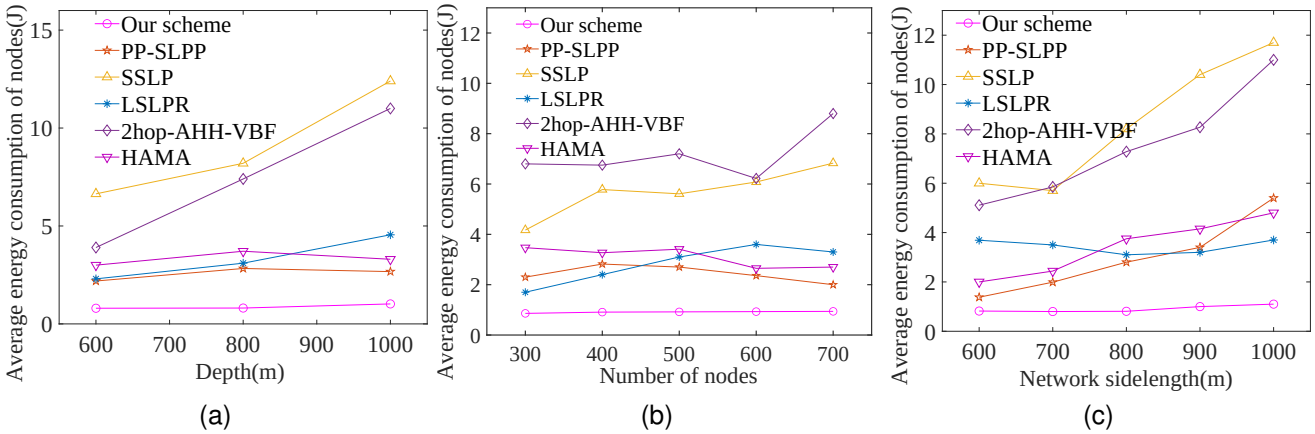


Fig. 12. AECNS comparison of LDSLP-MA, PP-SLPP, SSLP, LSLPR, 2hop-AHH-VBF and HAMA under various parameters. (a) AECNS under different depths with 500 nodes and network sidelength of 800 m. (b) AECNS under different numbers of nodes with depth of 800 m and network sidlength of 800 m. (c) AECNS under different network sidelengths with 500 nodes and depth of 800 m.

and transmitting data, which adds extra delay. Nevertheless, AUVs are crucial in dealing with complex underwater issues and play an essential role in certain scenarios. Therefore, one major objective of our research is to reduce the delay caused by AUVs cruising. Overall, among the five multi-AUV-based schemes, our scheme achieves the lowest EED and significantly outperforms the other SLP protection schemes that rely on AUVs for packet transmission, such as PP-SLPP and SSLP.

Specifically, PP-SLPP has the highest EED, followed by SSLP. This is because the EED of PP-SLPP includes the time taken by all the follower AUVs for collecting data, whereas the AUVs of SSLP transmit packets along the fixed trajectories. The CS and HAMA schemes do not involve waiting times for collecting follower AUV data, and the area where the AUVs collect data is restricted. As a result, their delays are shorter than those in the PP-SLPP and SSLP schemes. Despite LDSLP-MA also utilizes AUVs to transmit packets, it does not require AUVs to cruise for packet collection; instead, the AUVs directly transmit packets to the target area via the shortest path. Furthermore, LDSLP-MA allows the packets that are not collected by AUVs to reach the sink node through multi-hop routing, thereby avoiding the delay caused by the AUVs for collecting packets. Consequently, the EED of LDSLP-MA is significantly lower compared to other schemes based on multi-AUV collaboration. 2hop-AHH-VBF and LSLPR do not utilize AUVs, resulting in their EEDs being relatively small.

From Fig. 11(a) and Fig. 11(c), it can be observed the EEDs show an increasing trend with the increasing of the depth of water or network sidelength. Fig. 11(b) illustrates the fluctuation in the EED of PP-SLPP under different numbers of nodes, which is attributed to the different initial or pushed locations of AUVs in PP-SLPP. In SSLP, as the number of nodes increases, the packets from more nodes are collected along a fixed trajectory, leading to increased EED. 2hop-AHH-VBF and HAMA employ a fixed path for packet transmission, while CS does not use nodes, resulting in a nearly constant EEDs even as the number of nodes increases. In Fig. 11(b), both LSLPR and LDSLP-MA exhibit a slight decrease in EED

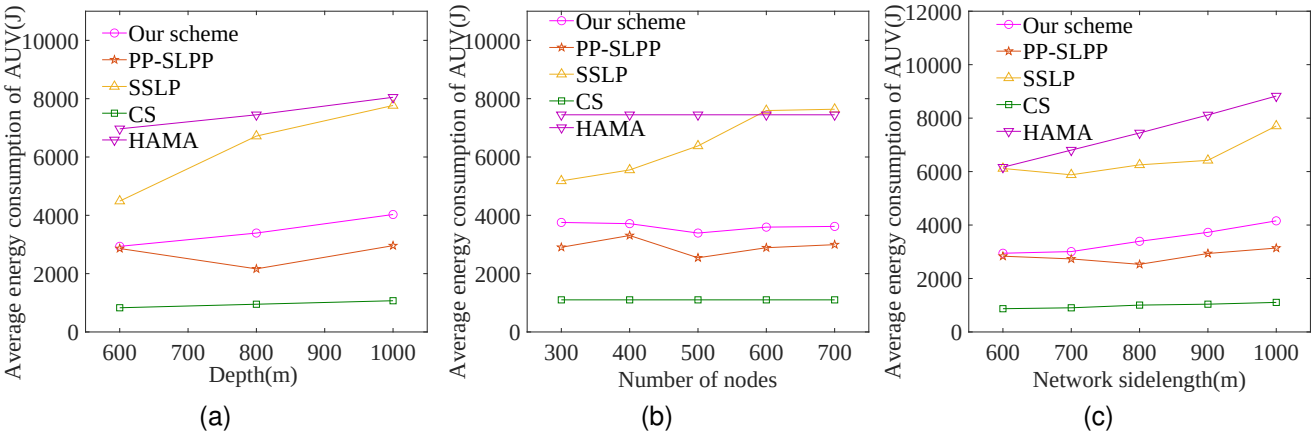


Fig. 13. AECA comparison of LDSLP-MA, PP-SLPP, SSLP, CS and HAMA under various parameters. (a) AECA under different depths with 500 nodes and network sidelength of 800 m. (b) AECA under different numbers of nodes with depth of 800 m and network sidlength of 800 m. (c) AECA under different network sidelengths with 500 nodes and depth of 800 m.

with the increase in the number of nodes. This is because that the best next hop selected among more nodes is more optimal.

Considering the CS scheme does not utilize any nodes, Fig. 12 shows the AECNS comparison of the other six schemes. As shown in Fig. 12,our proposed LDSLP-MA scheme achieves the lowest AECNS among the six schemes. This result highlights the effectiveness of our scheme in minimizing energy consumption, which is desirable in resource-constrained UASNs. In contrast, the AECNSs of both the 2hop-AHH-VBF and SSLP schemes are higher compared to the other four schemes. The 2hop-AHH-VBF is essentially a broadcast routing protocol with a high AECNS. In SSLP, both nodes and AUVs are involved in data transmission, and a pseudo packet technique is used to protect SLP, which leads to higher AECNS. PP-SLPP also employs the pseudo packet technique. However, the nodes in PP-SLPP just push the location information to the leader AUV and are not involved in forwarding data, thus PP-SLPP has a lower AECNS compared to SSLP. Notably, PP-SLPP employs the k-means algorithm for clustering, which introduces instability and additional energy consumption for re-clustering. Even though the common nodes in the PP-SLPP scheme do not participate in data transmission, the pseudo packets and cluster maintenance consume some energy. Consequently, the AECNS of the PP-SLPP scheme is not significantly different from that of the HAMA and LSLPR schemes. The AECNS of the LDSLP-MA scheme is lower than that of the LSLPR scheme due to the AUVs in the LDSLP-MA scheme bear a portion of energy consumption. Overall, packets broadcast, pseudo packet transmitting, and cluster maintenance significantly increase the energy consumption of common nodes while enhancing data transmission efficiency and SLP security. Consequently, we need to trade off the balance between performance optimization and energy consumption in UASNs.

From Fig. 12(a) and Fig. 12(c), it can be seen that the AECNS increases with the increasing of depth of water or network sidelength. The increase in depth of water or network sidelength results in a long routing path and large AECNS. In Fig. 12(b), the AECNS of both LDSLP-MA and HAMA remains almost constant as the number of nodes increases, this is because the number of nodes involved in data transmission does not change significantly. In PP-SLPP, the AECNS fluctuates in the cases where some packets within clusters are not collected. The AECNS of 2hop-AHH-VBF increases with the number of nodes as more nodes become eligible to forward the same packet in the pipeline. The AECNS of SSLP increases gradually with the number of nodes due to the increased energy for cluster splitting, cluster maintenance, and real and pseudo packets transmission. As the number of nodes increases, LSLPR needs more energy to maintain the layer information for each node, leading to an increase in the AECNS.

Since LSLPR and 2hop-AHH-VBF do not use AUVs, only the AECA comparison of the five schemes is shown in Fig. 13. The AUVs in SSLP and HAMA schemes have the highest average energy consumption. This is because the AUVs collect packets along fixed trajectories, and the AUVs travel longer distances compared to the other three schemes. In the PP-SLPP scheme, the AECA fluctuates due to the randomness of the pushed position and the varying VoI of cluster head. In LDSLP-MA, each AUV continuously travels through different areas to transport packets, resulting in longer travel distances compared to PP-SLPP. Consequently, the AECA of LDSLP-MA is higher than that of PP-SLPP. In the CS scheme, the AUVs follow a predetermined circular route to collect data, resulting in the lowest energy consumption. Although the LDSLP-MA scheme has a higher AECA than some other schemes, the AUVs are easy to charge due to their flexible mobility.

In Fig. 13(a) and Fig. 13(c), as the depth of water or network sidelength increases, the AUVs need to travel longer distances, leading to a gradual increase in the AECA. In Fig. 13(b), the AECA of LDSLP-MA remains relatively constant with the increase in number of nodes since the distance traveled by each AUV in LDSLP-MA is unaffected by the number of nodes. In SSLP, as the number of nodes increases, the AUVs need to collect data from more nodes on a fixed trajectory, resulting in the increased AECA.

From Figs. 10(b), 11(b), 12(b), and 13(b) we can see the variation in the four performance metrics of the LDSLP-MA scheme as the number of nodes increases. It can be observed that as the number of nodes increases, the safety period increases rapidly, the end-to-end delay decreases slightly, the average energy consumption of nodes rises slightly, and the average energy consumption of AUV fluctuates slightly. As the number of nodes increases, the LDSLP-MA scheme enhances SLP security and reduces delay due to the better diversity of transmission paths and improved next-hop selection. However, as the number of nodes increases, more energy is required to maintain connectivity between neighboring nodes, leading to a rise in the average energy consumption of nodes, which is unavoidable in any scheme and is also a vital factor affecting the scalability of the LDSLP-MA scheme.

原来是 to affect

After conducting a series of comparison experiments, it is evident that our proposed LDSLP-MA scheme achieves lower delay, higher SLP security, and smaller energy consumption compared to other multi-AUV cooperation-based schemes. It is worth noting that, unlike SSLP and PP-SLPP, which sacrifice delay to achieve SLP protection, our LDSLP-MA scheme safeguards SLP without compromising on delay, making it a more efficient low-delay SLP protection scheme.

E. Experiment discussion

The above simulation results confirm the superior performance of the LDSLP-MA scheme in SLP security, delay, and energy consumption. Unlike the simulation experiments, real underwater experiments are affected by environmental factors such as temperature, salinity, conductivity, pressure, and hydrological conditions. These factors have an effect on signal propagation by causing attenuation, speed variations, refraction, and multipath effects. As a result, they lower the signal-to-noise ratio, increase bit error rates and delay, and weaken network stability, ultimately degrading communication quality. Consequently, metrics such as delay and delivery rate are typically lower in real underwater experiments than

原来是 take

that in simulation experiments. This degradation of communication quality not only makes it more challenging for adversaries to locate the source but also hinders their ability to share information and coordinate attacks, resulting in stronger SLP protection in real underwater environments compared to simulations. In summary, while the LDSLP-MA scheme applied in real underwater environments may reduce network performance, it enhances SLP security.

VI. Conclusion and Future Work

In this paper, we propose a novel SLP protection scheme with multi-AUV collaboration, called LDSLP-MA, to tackle the long delay commonly seen in multi-AUV-based SLP protection schemes for UASNs. This scheme has two key innovations: the MCMR algorithm and a novel AUV scheduling method. In LDSLP-MA, the MCMR algorithm as well as a novel AUV scheduling method to facilitate data transmission are proposed. In the MCMR algorithm, the residual energy and selection frequency of candidate nodes are considered for establishing multipath routing, which enhances SLP protection. Additionally, the network performance is optimized by incorporating constraints on forwarding angle, depth difference, overhead, and the number of preferred candidate nodes. To mitigate the high end-to-end delay caused by AUV cruising, we strategically plan the dwelling and target areas of AUVs. This scheduling method not only reduces delay but also diversifies packet transmission paths and enhances SLP security. Simulation results show that, compared with other schemes, our proposed scheme exhibits superior performance in terms of safety period, end-to-end delay, and energy consumption. The results demonstrate the effectiveness of our scheme in SLP protection and delay reducing in UASNs.

In UASNs, protecting SLP is crucial for fields such as national defense, disaster monitoring, and marine exploration. In national defense, ensuring the security of SLP effectively prevents adversaries from targeting strategic locations, thereby safeguarding the confidentiality of military deployments and operations. For disaster monitoring, ensuring the security of SLP strengthens the reliability of early warning systems. In marine exploration, ensuring the security of SLP prevents the exposure of valuable resource data, mitigating economic and security risks. In summary, the LDSLP-MA scheme enhances SLP security, providing significant protection for critical applications.

In future work, it is crucial to explore coding protocols for SLP, focusing on achieving low energy consumption, high packet delivery rates, and effective defense against decodable and traffic-analyzing adversaries. Additionally, incorporating differential privacy techniques into UASNs for SLP protection represents a promising direction.

References

[1] C. Li, X. Du, and X. Tian, "A Layering Routing Protocol Based on Node Mobility Prediction for Underwater Sensor Networks," *IEEE Sensors J.*, vol. 23, no. 24, pp. 31368–31379, Dec. 2023.

[2] W. Jiang, X. Yang, F. Tong, Y. Yang, and T. Zhou, "A Low-Complexity Underwater Acoustic Coherent Communication System for Small AUV," *Remote Sens.*, vol. 14, no. 14, p. 3405, Mar. 2022.

[3] X. Liu, X. Du, J. Zhang, D. Han, and L. Jin, "ROFC-LF: Recursive online fountain code with limited feedback for underwater acoustic networks," *IEEE Trans. on Commun.*, vol. 70, no. 7, pp. 4327–4342, Jul. 2022.

[4] K. F. Haque, K. H. Kabir, and A. Abdelgawad, "Advancement of routing protocols and applications of underwater wireless sensor network (UWSN)-A survey," *J. of Sensor and Actuator Netw.*, vol. 9, no. 2, p. 19, Apr. 2020.

[5] C. Li, X. Du, and L. Wang, "IATLR: Improved ACO and TOPSIS based layering routing protocol for underwater acoustic networks," *IEEE Sensors J.*, vol. 23, no. 3, pp. 3262–3269, Feb. 2023.

[6] M. Y. I. Zia, J. Poncela, and P. Otero, "State-of-the-art underwater acoustic communication modems: Classifications, analyses and design challenges," *Wireless Pers. Commun.*, vol. 116, no. 2, pp. 1325–1360, Jan. 2021.

[7] H. Khan, S. A. Hassan, and H. Jung, "On underwater wireless sensor networks routing protocols: A review," *IEEE Sensors J.*, vol. 20, no. 18, pp. 10371–10386, Sep. 2020.

[8] K. Hao, J. Zhao, Z. Li, Y. Liu, and L. Zhao, "Dynamic path planning of a three-dimensional underwater AUV based on an adaptive genetic algorithm," *Ocean Eng.*, vol. 263, p. 112421, Mar. 2020.

[9] Y. Wang, Z. Tian, Y. Sun, X. Du, and N. Guizani, "Preserving location privacy in UASN through collaboration and semantic encapsulation," *IEEE Netw.*, vol. 34, no. 4, pp. 284–290, Jul. 2020.

[10] G. Han, Y. Liu, H. Wang, and Y. Zhang, "A Collision-Free Transmission-based Source Location Privacy Protection Scheme in UASNs under Time Slot Allocation," *IEEE Internet of Things J.*, vol. 10, no. 2, pp. 1546–1557, Sep. 2022.

[11] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energyconstrained sensor network routing," in *Proc. 2nd ACM Workshop Secur. Ad Hoc Sensor Netw.*, Washington, DC, USA, Oct. 2004, pp. 88–93, doi: 10.1145/1029102.1029117.

[12] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing sourcelocation privacy in sensor network routing," in *Proc. 25th IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Columbus, OH, USA, Jun. 2005, pp. 599–608, doi: 10.1109/ICDCS.2005.31.

[13] Y. He, G. Han, M. Xu, and M. Martínez-García, "A Pseudopacket Scheduling Algorithm for Protecting Source Location Privacy in the Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9999–10009, Jun. 2022.

[14] H. Wang, G. Han, L. Zhou, J. A. Ansere, and W. Zhang, "A source location privacy protection scheme based on ring-loop routing for the IoT," *Comput. Netw.*, vol. 148, pp. 142–150, Jan. 2019.

[15] J. Long, A. Liu, M. Dong, and Z. Li, "An energy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing," *J. Parallel Distrib. Comput.*, vol. 81, pp. 47–65, Jul. 2015.

[16] Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, and H. Zhou, "PSSPR: A source location privacy protection scheme based on sector phantom routing in WSNs," *Int. J. Intell. Syst.*, vol. 37, no. 2, pp. 1204–1221, Sep. 2021.

[17] D. Tang, T. Li, J. Ren, and T. Wu, "Cost-aware secure routing (CASER) protocol design for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 960–973, Apr. 2014.

[18] C. Gu, M. Bradbury, and A. Jhumka, "Phantom walkabouts: A customisable source location privacy aware routing protocol for wireless sensor networks," *Concurrency Comput. Pract. Exp.*, vol. 31, no. 20, p. e5304, Apr. 2019.

[19] H. Wang, B. Sheng, and Q. Li, "Privacy-aware routing in sensor networks," *Comput. Netw.*, vol. 53, no. 9, pp. 1512–1529, Jun. 2009.

[20] L. Mutalemwa and S. Shin, "Achieving source location privacy protection in monitoring wireless sensor networks through proxy node routing," *Sensors*, vol. 19, no. 5, p. 1037, Feb. 2019.

[21] G. Han, H. Wang, J. A. Ansere, J. Jiang, and Y. Peng, "SSLP: A stratification-based source location privacy scheme in underwater acoustic sensor networks," *IEEE Netw.*, vol. 34, no. 4, pp. 188–195, Jul. 2020.

[22] H. Wang, G. Han, Y. Zhang, L. Xie, "A push-based probabilistic method for source location privacy protection in underwater acoustic sensor networks," *IEEE Internet of Things J.*, vol. 9, no. 1, pp. 770–782, Jan. 2022.

[23] H. Wang, G. Han, A. Gong, A. Li and Y. Hou, "A Backbone-Network-Construction-Based Multi-AUV Collaboration Source Location Privacy Protection Algorithm in UASNs," *IEEE Internet of Things J.*, vol. 10, no. 20, pp. 18198–18210, Oct. 2023.

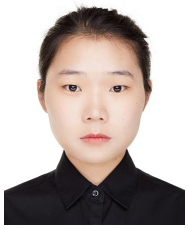
[24] H. Wang, G. Han, Y. Liu, A. Li and J. Jiang, "AUV-Assisted Stratified Source Location Privacy Protection Scheme Based on Network Coding in UASNs," *IEEE Internet of Things J.*, vol. 10, no. 12, pp. 10636–10648, Jun. 2023.

[25] D. Han, X. Du, and X. Liu, "CELR: Connectivity and energy aware layering routing protocol for UANs," *IEEE Sensors J.*, vol. 21, no. 5, pp. 7046–7057, Mar. 2020.
[26] G. Han, X. Miao, H. Wang, M. Guizani, and W. Zhang, "CPSLP: A cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2739–2750, Jan. 2019.
[27] D. Han, X. Du, X. Liu, X. Tian, "FCLR: Fuzzy Control-Based Layering Routing Protocol for Underwater Acoustic Networks," *IEEE Sensors J.*, vol. 22, no. 23, pp. 23590–23602, Nov. 2022.
[28] H. Zhang, Y. Xu, Q. Liu, X. Wang and Y. Li, "Solving Fokker–Planck equations using deep KD-tree with a small amount of data," *Nonlinear Dyn.*, vol. 108, no. 4, pp. 4029-4043, Dec. 2022.
[29] X. Tian, X. Du, L. Wang, L. Zhao and D. Han, "LSLPR: A Layering and Source-Location-Privacy-Based Routing Protocol for Underwater Acoustic Sensor Networks," *IEEE Sensors J.*, vol. 23, no. 19, pp. 23676–23691, Oct. 2023.
[30] Y. Wang, H. Pan, Y. Shi, R. Wang and P. Wang, "A new active-learning estimation method for the failure probability of structural reliability based on Kriging model and simple penalty function," *Comput. Methods Appl. Mech. Eng.*, vol. 410, p. 116035, May. 2023.
[31] A. H. Bademlioglu, A. S. Canbolat, and O. Kaynakli, "Multi-objective optimization of parameters affecting Organic Rankine Cycle performance characteristics with Taguchi-Grey Relational Analysis," *Renew. Sustainable Energy Rev.*, vol. 117, p. 109483, Jan. 2020.
[32] J. Jia, B. Wang, R. Ma, Z. Deng and M. Fu, "State Monitoring of Gas Regulator Station Based on Feature Selection of Improved Grey Relational Analysis," *IEEE Internet of Things J.*, vol. 9, no. 22, pp. 22765–22773, Nov. 2022.
[33] Gündoğdu FK, Duleba S, Moslem S, and Aydın S, "Evaluating public transport service quality using picture fuzzy analytic hierarchy process and linear assignment model," *Appl. Soft Comput.*, vol. 100, p. 106920, Mar. 2021.
[34] S. M. Ghoreyshi, A. Shahrabi, and T. Boutaleb, "Void-handling techniques for routing protocols in underwater sensor networks: Survey and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 800–827, Jan. 2017.
[35] Z. Li, N. Yao, and Q. Gao, "Relative distance-based forwarding protocol for underwater wireless sensor networks," *Appl. Mech. Mater.*, vol. 437, pp. 655–658, Oct. 2013.
[36] H. Zheng, N. Wang, and J. Wu, "Minimizing deep sea data collection delay with autonomous underwater vehicles," *J. Parallel Distrib. Comput.*, vol. 104, pp. 99–113, Jun. 2017.
[37] G. Han, X. Long, C. Zhu, M. Guizani, and W. Zhang, "A HighAvailability Data Collection Scheme based on Multi-AUVs for Underwater Sensor Networks," *IEEE Trans. Mob. Comput.*, vol. 19, no. 5, pp. 1010–1022, May. 2020.
[38] G. Han, S. Shen, H. Wang, J. Jiang, and M. Guizani, "Prediction-Based Delay Optimization Data Collection Algorithm for Underwater Acoustic Sensor Networks," *IEEE Trans. Vehicular Technol.*, vol. 68, no. 7, pp. 6926–6936, Jul. 2019.

Xiaojing Tian received the master's degree from Qinghai Normal University, Xining, Qinghai, China, in 2021, where she is pursuing the Ph.D. degree. Her current research interests include location privacy protection of underwater acoustic sensor networks.

Xiujuan Du received the Ph.D. degree from Tianjin University, Tianjin, China, in 2010. She is currently a Professor with Qinghai Normal University, Xining, Qinghai, China. Her research interests include underwater acoustic networks, wireless networks and security, and the Internet of Things. Dr. Du received the New Century Excellent Talent from the Ministry of Education, China, in 2011.

Xiuxiu Liu received the Ph.D. degree from Qinghai Normal University, Xining, China, in 2024. She is currently a associate professor with Qinghai Normal University. Her research interests include information security and underwater acoustic networks.



Lijuan Wang received the Ph.D. degree from Qinghai Normal University, Xining, Qinghai, China, in 2023. She is a Lecturer with Qinghai Normal University. Her research interests include underwater acoustic networks.

Lei Zhao received her master's degree from University of Rennes 1, Rennes, France, in 2015. She is now a doctoral student in Qinghai Normal University, Qinghai, China. Her research interest includes underwater sensor networks.