sensors

MDPI

Article

An Underwater Source Location Privacy Protection Scheme Based on Game Theory in a Multi-Attacker Cooperation Scenario

Beibei Wang [1], Xiufang Yue [2], Kun Hao [2,*], Yonglei Liu [2], Zhisheng Li [2] and Xiaofang Zhao [2]

[1] School of Control and Mechanical Engineering, Tianjin Chengjian University, Tianjin 300384, China; wbbking@163.com
[2] School of Computer and Information Engineering, Tianjin Chengjian University, Tianjin 300384, China; xiufangyue@163.com (X.Y.); yongleiliu@vip.163.com (Y.L.); lzs@tcu.edu.cn (Z.L.); zhaoxftju@tju.edu.cn (X.Z.)
* Correspondence: kunhao@tcu.edu.cn

Abstract: Ensuring source location privacy is crucial for the security of underwater acoustic sensor networks amid the growing use of marine environmental monitoring. However, the traditional source location privacy scheme overlooks multi-attacker cooperation strategies and also has the problem of high communication overhead. This paper addresses the aforementioned limitations by proposing an underwater source location privacy protection scheme based on game theory under the scenario of multiple cooperating attackers (SLP-MACGT). First, a transformation method of a virtual coordinate system is proposed to conceal the real position of nodes to a certain extent. Second, through using the relay node selection strategy, the diversity of transmission paths is increased, passive attacks by adversaries are resisted, and the privacy of source nodes is protected. Additionally, a secure data transmission technique utilizing fountain codes is employed to resist active attacks by adversaries, ensuring data integrity and enhancing data transmission stability. Finally, Nash equilibrium could be achieved after the multi-round evolutionary game theory of source node and multiple attackers adopting their respective strategies. Simulation experiments and performance evaluation verify the effectiveness and reliability of SLP-MACGT regarding aspects of the packet forwarding success rate, security time, delay and energy consumption: the packet delivery rate average increases by 30%, security time is extended by at least 85%, and the delay is reduced by at least 90% compared with SSLP, PP-LSPP, and MRGSLP.

Keywords: underwater acoustic sensor networks; source location privacy; passive attacks; virtual coordinate system; network coding; evolutionary game theory

Citation: Wang, B.; Yue, X.; Hao, K.; Liu, Y.; Li, Z.; Zhao, X. An Underwater Source Location Privacy Protection Scheme Based on Game Theory in a Multi-Attacker Cooperation Scenario. *Sensors* **2024**, *24*, 2851. https://doi.org/10.3390/s24092851

Academic Editor: Jesús Ureña

Received: 18 March 2024
Revised: 24 April 2024
Accepted: 29 April 2024
Published: 30 April 2024

1. Introduction

The ocean, as a new frontier of overall national security, plays a more prominent role in safeguarding national sovereignty, security, and development interests. More and more countries pay attention to the monitoring of the marine environment by utilizing underwater acoustic sensor networks (UASNs) for scientific exploration, commercial development, military applications, etc. [1,2]. Source location privacy protection in UASNs is at the forefront of contemporary research due to its critical role in ensuring the security and integrity of underwater communication systems [3]. These networks consist of a large number of underwater sensor nodes that collect and transmit critical information. However, the precise location of these sensor nodes is sensitive information, and its exposure may lead to security threats such as adversarial tracking, resource targeting, and privacy breaches [4]. Therefore, ensuring reliable source location privacy protection in UASNs is critical [5].

When protecting source location privacy in UASNs, traditional encryption and authentication techniques usually ignore the strategic interaction and competition between network nodes, which may lead to failure to consider the strategic actions that attackers may take, thus reducing the effectiveness of privacy protection [6]. In addition, UASNs employ acoustic communication [7,8], and the underwater environment presents unique challenges such as limited bandwidth, high propagation latency, and dynamic network topologies, which require innovative and customized source location privacy protection schemes, rather than simply applying technologies from terrestrial networks to underwater environments. In this particular context, solutions must be developed for the needs and limitations of underwater acoustic sensor networks to ensure that privacy protection does not sacrifice network performance and availability. Hence, developing mechanisms based on methods such as game theory to account for competition and cooperation between nodes is essential for increasing the level of source location privacy [9,10].

In regard to source location privacy protection in UASNs, it is necessary to consider three main problems: source location privacy, latency and energy [11]. Among them, safeguarding the location privacy of source nodes is the paramount issue in UASNs. In underwater acoustic sensor networks, attackers can deduce a source node's location by analyzing acoustic signals [12]. Therefore, it is necessary to adopt privacy protection mechanisms, such as false source technology and multi-path routing, to reduce the possibility of attackers obtaining location information [13]. However, these mechanisms introduce problems of latency and energy consumption. Latency is another key factor to be balanced in UASNs. Excessive communication latency is unacceptable in real-time or interactive applications. Introducing source location privacy protection mechanisms may increase communication latency as additional processing steps take time. Therefore, the relationship between location privacy protection and communication latency needs to be balanced to meet the latency requirements of specific applications. Sensor nodes in UASNs usually rely on limited battery power [14]. Balancing between energy efficiency and location privacy protection is essential because location privacy protection mechanisms could introduce additional energy overhead in UASNs [15].

In this paper, a source location privacy protection scheme (SLP-MACGT) based on game theory is proposed to protect the location privacy of sensor nodes in multi-attacker cooperation scenarios by exploring the application of source location privacy challenges in depth. Through this study, a new perspective and solution for source location privacy protection in underwater acoustic networks are provided to meet the growing security needs. The main contributions of this paper are summarized as follows:

- Establish a multi-attacker model. Considering the cooperative behavior among attackers, attackers can launch active attacks in addition to common passive attacks. In this paper, we use game theory to analyze the cooperation and competition between multiple attackers so as to design a comprehensive defense strategy against multiple threats;
- A virtual coordinate system transformation method is proposed as a means to protect the location privacy of source nodes. The real location information of the source node is effectively hidden to reduce the success probability of potential attackers;
- A new relay node selection strategy is proposed. The number of hops between the source node and the target node is increased to confuse the attacker's inference about the source node location, thus reducing the possibility that the attacker can obtain the location of the source node by monitoring network traffic and strengthening the network's defense against passive attacks. Furthermore, a secure data transmission method based on fountain codes is proposed to resist the active attack of attackers. By introducing redundant information, the reliability of data transmission is improved, the feedback and control overhead is reduced, the transmission efficiency is improved, and it can be adapted to different network environments and application requirements;
- A source location privacy protection scheme based on game theory is proposed. The interaction process between the attacker and the source node is described by evolutionary game equilibrium analysis, the balance point under different strategies is evaluated in time, and the defense strategy of the source node is dynamically adjusted to deal with multiple threats in time to ensure the security of source location privacy.

The rest of this paper is organized as follows: in Section 2, the related work of source location privacy protection is analyzed. In Section 3, the network model, underwater acoustic communication model and attack model used in this research are described. In Section 4, the design of the SLP-MACGT model is introduced in detail. In Section 5, the experimental simulation and performance analysis of SLP-MACGT are carried out. In Section 6, conclusions are drawn, and future research directions are discussed.

2. Related Work

In the rapidly evolving field of underwater acoustic sensor networks, ensuring the security and privacy of data transmission is of paramount importance. Researchers have been exploring innovative techniques and strategies to protect sensitive information and maintain the integrity of communication in challenging underwater environments. This section provides an overview of the existing work in source location privacy protection and sets the stage for the novel contributions presented in this paper.

2.1. Source Location Privacy Protection in WSNs

In the early 2000s, a series of seminal works contributed to advancing the concept of source location privacy in wireless sensor networks. In 2004, Ozturk et al. proposed the concept of source location privacy for the first time [16], mainly discussing the problem of protecting the source sensor location privacy in energy-constrained sensor networks, and proposed a flexible routing strategy named "phantom routing". Building on this foundation, Koh et al. discussed the problem of optimal privacy protection probability routing in wireless networks. They proposed a novel privacy protection routing algorithm (OPERA) [17], aiming to optimize routing protocol privacy while considering utility constraints. Subsequently, they discussed the privacy utility trade-off issue and proposed a statistical decision-making framework to solve this problem. However, this method requires a lot of prior knowledge of location privacy routing, which is not easy to apply.

Continuing the exploration of privacy-preserving routing strategies, Chen et al. proposed a protection scheme based on Sector Phantom Routing (PSSPR) [18]. By utilizing the coordinates of the central node V to divide the sector area, phantom nodes execute the specific routing strategy to ensure that they can choose a variety of locations. Directed random routing ensures that data packets avoid visible areas when they move to the receiving node one by one and protects the source location privacy. Additionally, Sun et al. proposed a multi-path source location privacy protection scheme based on proxy nodes [19]. The sensor network is divided into four quadrants, and the source node initiates constrained flooding and directed routing algorithms to keep data packets away from the source location. By employing greedy quantitative routing, h-hop directional routing, and multi-path irregular spiral routing, the scheme makes it more difficult for attackers to backtrack paths, achieving a high level of privacy protection for the source location.

In a related development, Wu et al. proposed a game theory-based mobile location privacy protection [20], showing the necessity of game theory in solving the problem of mobile location privacy, proposed the classification of location privacy games among adversaries, data owners and collectors, and investigated and summarized the game models and equilibrium analysis in mobile location privacy. However, the authors treat service providers in mobile networks as untrustworthy, and each data owner needs to consider its own location privacy, which may lead to insufficient attention to the trust problem of service providers, and most of the privacy games are non-cooperative. Although significant progress has been made in wireless sensor networks, these source location privacy protection methods are not directly applicable to underwater network environments.

2.2. Source Location Privacy Protection in UASNs

In recent advancements in underwater sensor network research, several innovative source location privacy protection schemes have been proposed to address the unique challenges of securing data transmission in aquatic environments. Han et al. incorporated

SLP into UASNs as the basis for a novel stratification-based source location privacy (SSLP) scheme [21]. SSLP is protected through the cooperation of autonomous underwater vehicles (AUVs) at each network layer. Similar to WSN, SSLP adds a false source node to the underwater cluster structure to increase the randomness of the underwater network. Additionally, false data streams are included in the AUV data collection and transmission of each cluster. However, the introduction of false source nodes and data streams can easily interfere with the transmission of normal data. Building on this concept, Wang et al. proposed a push-based probabilistic approach for source location privacy protection (PP-SLPP) [22]. PP-SLPP uses the pseudo-packet technique and multi-path technique to counteract passive attacks and uses the Ekman drift current model to divide the underwater environment into dynamic and static layers. Data collection of autonomous underwater vehicle (AUV) swarms is realized by hierarchical clustering and position pushing. However, the addition of pseudo-data packets and the strategy of AUV data collection will greatly increase the data transmission delay.

In parallel efforts, Liu et al. proposed a source location privacy protection scheme based on false packet time slot allocation (FPTSA-SLP) [23]. The time slot allocation mode is adopted to avoid interference with source data packets. Additionally, a handshake-based relay node selection method is also proposed to increase the diversity of routing paths to confuse adversaries. Based on reference [23], a conflict-free transmission-based source location privacy protection scheme (CFTSLP-TSA) was proposed in reference [24], selecting appropriate false source nodes to generate false data packets to conceal the traffic of source data packets. Subsequently, pseudo-sources and false data packets were arranged in different transmission time slots to prevent interference between each other. The handshake-based relay node selection strategy was used to diversify the paths, thereby imposing higher requirements on attackers for tracing the flow of source packets. However, the introduction of false sources and false data packets will increase the network's load.

In a more sophisticated approach, Wang et al. proposed a layered source location privacy protection scheme based on network coding (SSLP-NC) [25]. To address two scenarios where the source is located in shallow sea and deep sea, distinct pseudo-source selection algorithms were proposed. Each node utilizes a pseudorandom number generator to periodically generate sequences to achieve the time-division transmission of real and false data. Considering the ability of malicious nodes to decode data packets, nodes employ existing pseudorandom number sequences as encoding vectors to encrypt both the source and false data to prevent adversaries' decryption attempts. However, the capacity of linear network coding is limited, and currently, effective schemes for the integration of network coding with underwater source location privacy protection are still lacking.

Some achievements have been made in the research of underwater source location privacy protection schemes, but due to the complexity and uncertainty of underwater sensor networks, these schemes still need further research and improvement to enhance their practical application value. Currently, schemes designed for underwater source location privacy protection use the obfuscation technology of false sources and packets that increase communication and computation overheads, leading to network performance degradation. In addition, existing research focuses on resisting passive attacks, and there are a lack of strategies for resisting active attacks, which necessitate continuous updates and improvements. This paper comprehensively considers privacy protection, delay, and energy issues and presents a game theory-based underwater source location privacy protection scheme to address the aforementioned problems.

3. System Architecture and Assumptions

In this section, the network model, underwater acoustic communication model, and attack model used by the system are presented.

3.1. Network Model

In this paper, a spatial model of a 1000 m × 1000 m × 1000 m underwater acoustic network is constructed based on the classical panda hunter model [26], as illustrated in Figure 1. Sensor nodes are randomly placed in the underwater environment for sensing and transmitting data packets. Each sensor node is equipped with a depth sensor. Assuming that the network time is synchronized, all nodes work in half-duplex mode, transmitting and receiving packets at different time periods [27]. In addition, each node possesses a unique ID number and the same transmission capacity, buffer space, and computational power. The sink node is a strong and stable node deployed in the middle of the water, which is the ultimate destination of all source packets. An attacker lurks near the sink node but is unable to attack objects within a one-hop range from the sink node due to the region's robust surveillance capability [28]. Once the target object is detected, the sensor node closest to the object is promptly activated to serve as the source node and reports the information about the monitored object to the sink node. It is assumed that the monitored objects are randomly displayed within the network and only one node acts as the source node at any given time. Any two sensor nodes in the network communicate in either one-hop or multi-hop mode. It is assumed that each node has N transmission frequencies, and each node can switch its frequency to send or receive packets.

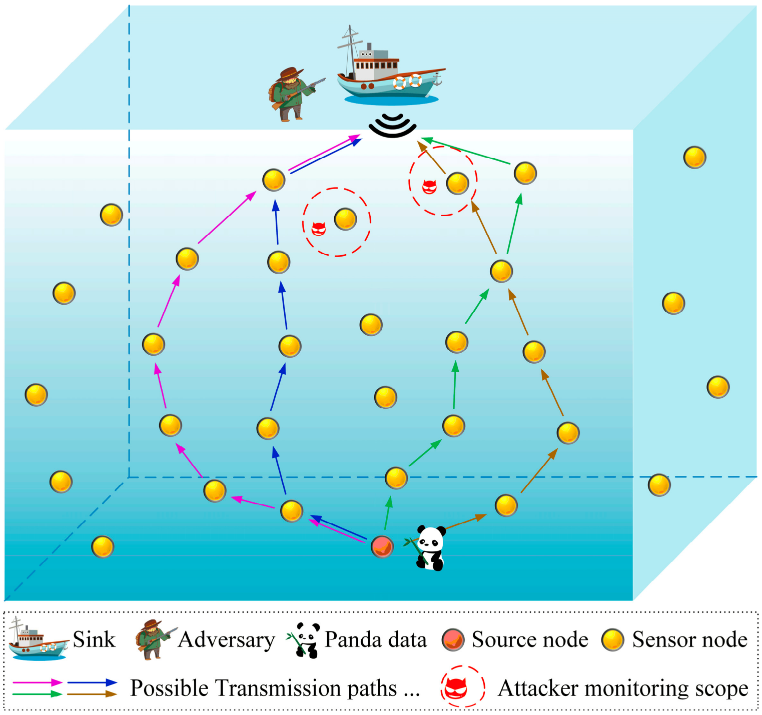


Figure 1. Network model.

3.2. Underwater Acoustic Communication Model

The communication methods commonly used on land, such as electromagnetic waves, infrared rays, and wireless signals, are not suitable for underwater environments due to propagation loss, multi-path interference, and spectrum limitations. Underwater acoustic propagation is suitable for underwater environments because it has characteristics such as long propagation distance and low loss, which allows underwater acoustic sensor networks to play an important role in underwater applications. The velocity of underwater acoustic propagation is affected by the properties of the medium such as temperature, pressure, salinity, and considering these factors comprehensively, the propagation velocity of an acoustic wave in an underwater environment can be expressed by the following equation [29]:

$$\begin{aligned} V = 1449 + 4.591T - 5.304 \times 10^{-2}T^2 + 2.374 \times 10^{-4}T^3 \\ +1.34(S-35) + 1.63 \times 10^{-2}D + 1.675 \times 10^{-7}D^2 \\ +1.025 \times 10^{-2}T(S-35) - 7.139 \times 10^{-3}TD^3 \end{aligned} \quad (1)$$

where T represents the temperature in degrees Celsius (°C), S represents the salinity in practical salinity units (PSU), and D represents the depth in meters (m).

3.3. Multiple-Attacker Model

It is assumed that the attacker lurks near the sink node. Once a new message is captured by the attacker, it will execute eavesdropping and traceback attacks [30]. Furthermore, this paper considers that the attacker carries out targeted active attacks in the case of passive attacks. The attacker has the capability of traffic analysis and packet deconstruction, including the ability to infer sensor node locations, and it can analyze and process eavesdropped data, deducing source locations by analyzing location information and communication data from multiple sensor nodes.

In previous research on the source location privacy protection of UASNs, scholars often consider that there is only a single attacker within the network. However, in actual situations, there may be multiple attackers who may collaborate with other attackers to jointly implement attack actions to achieve a common attack purpose. Forms of attacker cooperation include the division of labor cooperation, where each attacker is responsible for specific aspects or links of an attack; information sharing, where attackers enhance their attack abilities by sharing techniques, strategies, and information; and coordinated attacks, where multiple attackers act together with coordinated strategies and actions to carry out an attack. The differences between single-attacker and multiple-attacker scenarios are shown in Table 1.

Table 1. Comparison of single-attacker and multi-attacker capabilities.

Feature	Single Attacker	Multiple Attackers
Number of attackers	One attacker	Multiple attackers
Attack complexity	Usually independent operations, relatively simple attacks	More sophisticated coordinated attack strategies
Difficulty of detection	Easier to detect because it is a single entity	Complex to detect due to distributed actions
Network influence	Some privacy impact	Significant privacy threat, especially when acting in concert
Countermeasures to the attack	Easier to develop coping strategies	More sophisticated coping strategies may be required
Attack surface	Limited to the capabilities of a single attacker	Broader attack surface with diverse strategies and resources
Crypticity	Relatively easy to remain hidden and hard to detect	Difficult to remain completely hidden

It is worth noting that the attacker's actions do not cause any functional interference to the network, such as adding routing paths, changing packets, damaging sensor nodes, and so on. Additionally, the attacker can only monitor the area within the receiving range of its device. This paper assumes that the attacker's monitoring range is equal to the communication radius of the sensor node. Attackers use this eavesdropping radius to listen to the traffic in the network and try to detect the activity of the source node from it.

4. SLP-MACGT Model Design

The SLP-MACGT model's mechanism involves the following steps: (1) network initialization, where each node obtains information about its hop count with the sink node and the neighbor table, including neighbors within two hops; (2) based on the virtual coordinate system, a node obtains the virtual position coordinates of itself and its neighbor nodes; (3) the relay nodes are selected based on the relay node selection strategy; (4) data packets are transmitted based on adaptive coding; and (5) the source node and the attacker complete the multi-round game until the source is changed or is found by the attacker.

4.1. Network Initialization

Nodes in underwater acoustic sensor networks need to be initialized, which mainly includes establishing a neighbor table and obtaining the hop count between themselves and the sink node. The sink node establishes a horizontal Cartesian coordinate system centered on itself and sends broadcast packets $\{ID, HopCount\}$ to all sensor nodes in Flooding mode, where ID indicates the sending node, and $HopCount$ indicates the minimum hop count from the sink to this node. If the node receives a message from the sink for the first time, it records the hop count, updates the value of $HopCount$ to $HopCount + 1$, and sends the beacon message to its neighboring nodes. For each node that receives sink information, the ID and $HopCount$ of the forwarding node should be stored in its neighbor table. When the Flooding is completed, each node records the sink and its own coordinate information, and neighboring nodes record and store the minimum value of $HopCount$ from the sink.

4.2. Transformation Method Based on a Virtual Coordinate System

The virtual coordinate system is a technique used to locate nodes in a network. It does not rely on global location information, but it uses relative coordinates to represent the positional relationships between nodes. In this paper, the virtual coordinate system is combined with underwater acoustic sensor networks to protect the source location privacy, assuming that the location information of sensor nodes can be obtained by existing localization algorithms [31]. In underwater acoustic sensor networks, each node can generate virtual coordinates using its own physical location and the relative location information of neighboring nodes. Graph theory is used to model the communication relationships between nodes in underwater acoustic sensor networks in which sensor nodes can be represented as nodes in the graph and the relationships between sensors can be represented as edges in the graph, namely, $G = (V, E)$. As shown in Figure 2, the graph is traversed according to a breadth-first search to determine virtual coordinates for each node. First, node A is selected as the initial node and given the coordinate (0). All the neighbors of node A are found, and the neighbor nodes are numbered according to the binary representation. For example, node A has three neighboring nodes B, C, and D with numbers 00, 01, and 10, respectively, and the coordinates are (−1, 1), (−1, 1), and (1, 1), respectively. Node B has two neighbors, E and F, whose numbers are 00 and 01 and whose coordinates are (−2, −2, −1, −1) and (−2, −2, −1, 1), respectively. Node C has three neighbors D, G, and H. Since node D has virtual coordinates, the coordinates of node D are unchanged, and the coordinates of neighboring nodes G and H are (−2, 2, −1, −1), and (−2, 2, −1, 1), respectively. The remaining nodes are traversed by the same graph traversal method to determine their virtual coordinates.

The nodes maintain a mapping table that corresponds virtual coordinates to actual locations. These virtual coordinates are only used for internal calculations and do not reveal actual geographic location. When data need to be transmitted, a node can use the virtual coordinate system to select the next-hop transmission node. During data transmission, nodes can map virtual coordinates back to actual geographic coordinates to determine the actual transmission path of the data. This mapping process should take place inside the node and does not need to be propagated outside. Before the source node sends data, the virtual coordinates of the source node can be obfuscated or encrypted to protect the source location's privacy. Only the nodes inside the network know how to decrypt or restore these coordinates.

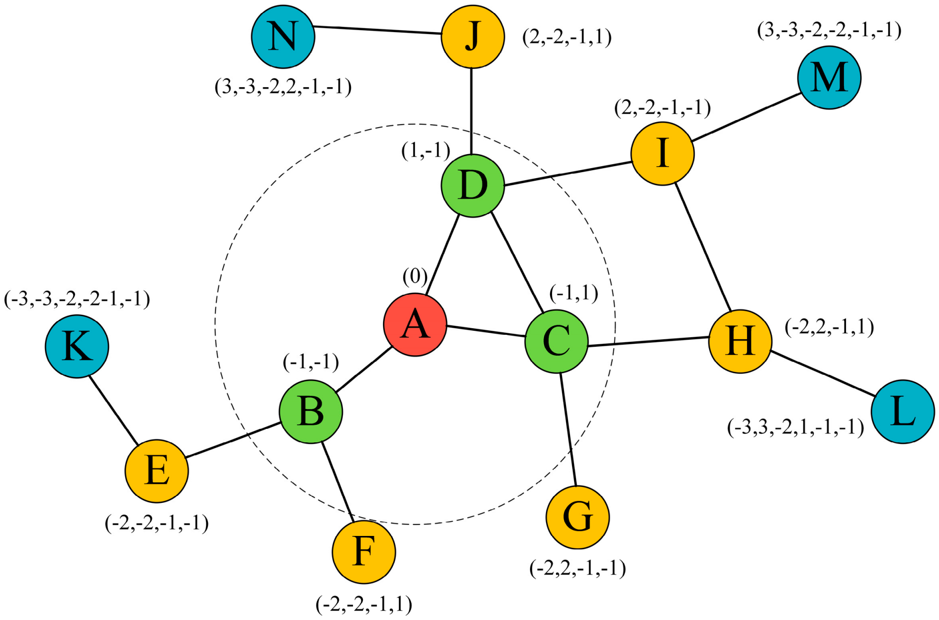


Figure 2. Setting virtual coordinates.

Combined with the virtual coordinate system, the underwater acoustic sensor network can achieve source location privacy protection to a certain degree. The virtual coordinate system allows nodes in the network to perform routing and data transmission according to their relative positions without revealing actual geographic coordinate information, ensuring that the geographic locations of the source nodes are not easily determined by external malicious parties or potential attackers. Moreover, each node only knows the location of itself and its neighboring nodes and does not need to obtain the location information of all nodes in the network, which saves storage space and improves security.

4.3. Relay Node Selection Strategy

In order to further protect the location privacy of the source node and make the actual location of the source node more difficult to observe or trace externally, the selection of relay nodes is very important. Once panda data are monitored, the source node periodically generates packets and transmits them to the sink node via multiple hops. The strategy proposed in this paper is divided into four distinct stages and is shown in Algorithm 1.

1. Limited Flooding: The source node uses limited Flooding to transmit messages within the monitoring range, and the number of hops is limited to H to achieve directional routing. Once the target enters the monitoring range, the source node sets a timer and broadcasts the message $Smessage = \{ID, Stime\}$ to the nodes within the range of H hops, and the ID of the sensor node is used as a unique identifier. $Stime$ is set to the maximum transmission time H, which decreases with the transmission time until it reaches zero, when the receiving node stops forwarding messages. A node ID_v receiving message $Smessage$ is marked as visible if its Hop_{count} is less than R (communication radius < eavesdropping distance). During the Flooding process, each node receiving message $Smessage$ can obtain the minimum hop count from the source node to the node itself;
2. H-hop-directed routing: According to the minimum number of hops from neighboring nodes to the source node, the next-hop node is selected for H-hop-directed routing to participate in packet forwarding. The forwarding time starts at zero and is increased by one for each execution until H is reached. The farthest H-hop neighbor node acts as participant M and is responsible for forwarding the packet from the source node;

3. Greedy quantitative routing: The length of greedy quantitative routing is defined as L, and the relay node N forwards the data packet to the sink node with a transmission time of L. In this process, care should be taken to randomly select a relay node N from the unseen region;
4. Multi-path forwarding routing based on relay nodes: Node N generates angle τ, where $\tau \in [0, \pi]$, and randomly completes a variable length equal-hop path H_m in the counterclockwise or clockwise direction to reach the next relay node O. Node O randomly selects an I-step equal-hop route to reach the sink node.

Algorithm 1: Relay Node Selection Strategy

```
Input: Source Node, Communication Radius, Monitoring Range
Output: Selected Relay Nodes
Limited Flooding:
Set the maximum transmission time $Stime$ to a predefined value;
Initialize the hop count $H$ to limit the number of hops for directional routing;
Broadcast a message within the monitoring range;
Nodes receiving the message mark themselves as visible if their distance is less than the communication radius $R$;
Calculate the minimum hop count from the source node to each visible node;
Relay Node Selection:
Identify relay nodes based on the minimum hop count and visibility;
The farthest neighbor node of the $H$ hop acts as participant M and forwards the data packet away from the source node;
The node that forwards the packet to the Sink node by forwarding time $L$ is selected as the next relay node N;
The relay node N generates angle $\tau$ and randomly completes a variable length equal-hop path to reach the next relay node O;
Node O randomly selects an $I$-step equal-hop route to reach the sink node;
Ensure the relay node is positioned to obscure the actual location of the source node;
Path Establishment:
Establish secure transmission paths through selected relay nodes;
Ensure data packets are forwarded through relay nodes to reach the sink node;
Maintain the integrity and confidentiality of data transmission;
End of Transmission:
Stop the transmission process once data packets reach the sink node.
```

The selection of relay nodes has an important impact on the safety time. In network communication, safety time is the time required for data to travel from the source node to the destination node, including the data transmission and forwarding time of the relay node. Selecting appropriate relay nodes can optimize the data transmission path, prolong the safety time, and improve the efficiency and reliability of data transmission.

Utilizing H-hop-directed routing forwards packets away from the source. Greedy quantitative routing is used to expand the optional range relay node N. It can be seen that there are $4\pi H^2$ forwarding paths generated in these phases. During the relay node-based multi-path forwarding routing phase, the relay node O may be positioned in any direction relative to the sink node. It can be seen that there are $4\pi l^2$, where $l \in [Hop_{source-\sin k} - H - L, Hop_{source-\sin k} + H - L]$, forwarding paths generated in these phases. Therefore, the number of paths generated by the relay node selection strategy is $4\pi H^2 \times 4\pi l^2 = 16\pi^2 H^2 l^2$ and the probability of path duplication is $\frac{1}{16\pi^2 H^2 l^2}$.

4.4. Secure Data Transmission Based on Fountain Codes

In the previous section, we realized the multi-path transmission of data packets through the selection of relay nodes mainly to resist eavesdropping attacks and backtracking attacks. The primary objective of this section is to resist an active attack during a passive attack. For a powerful attacker who can record eavesdropping packets and mine them for analysis, encrypted packets are insufficient to protect source location and monitor target location privacy. Therefore, the algorithm of this paper combines network coding technology and proposes a secure data transmission method based on fountain codes to resist active attacks. Luby transform codes (LT codes) are used to encode the data packets sent by the source, which is an error-correcting coding method designed to achieve high error tolerance [32]. Unlike traditional error-correcting codes, fountain codes are characterized by the ability to generate an unlimited number of coded symbols, which makes them superior in unreliable underwater acoustic communication.

4.4.1. Data Encoding

In the data transmission phase, the message to be transmitted by the source node is first divided into $K(s_1, s_2, \ldots, s_K)$ packets, and the length of each packet is n. The degree d_n of each code element is randomly selected by a random number generator according to a specific degree probability distribution function $\rho(d)$, and $1 \leq d_n \leq K$ represents the number of packets that a set of messages must contain. The d_n code elements involved in encoding are also random, and the output of the encoder t_n is obtained from an XOR operation of any $d_n s_k$.

The degree distribution function of LT codes is determined by the ideal solitary wave distribution first proposed by Luby [32]:

$$\rho(d) = \begin{cases} \frac{1}{K}, & d = 1 \\ \frac{1}{d(d-1)}, & d = 2, 3, \ldots, K \end{cases} \tag{2}$$

After determining the degree of an encoding, it is also necessary to determine which s_k values participate in the XOR coding operations. s_k can be selected in the same way as the determination of degree. The encoding process of LT codes is shown in Figure 3.

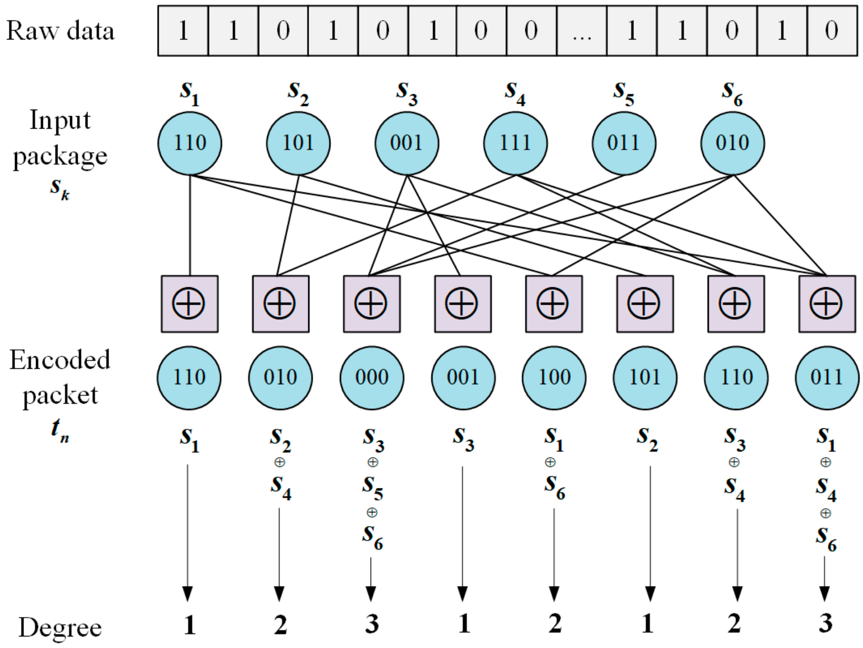


Figure 3. Data encoding process.

4.4.2. Data Decoding

After receiving an encoded packet, the receiver finds a check code t_n with a degree of 1. If there is no such check code, decoding terminates, and the source files cannot be recovered. Next, let $s_k = t_n$, carry out XOR operations between s_k and all t_n that are connected to s_k, and delete all connections with s_k. The above procedure is repeated until all s_k are determined. The decoding process of LT code is shown in Figure 4. First, an encoded packet with a degree of 1 is found, which is used as a check code; s_1, s_2, s_3 with degrees of 1 are found as shown in the figure; and s_1, s_2, s_3 are determined to be 110, 101, and 001, respectively. Since s_1, s_2, s_3 are also related to s_4, s_6, XOR is performed between s_1, s_2 and s_4, s_6, respectively; hence, s_4, s_6 are 111 and 010, and all links with s_1, s_2, s_3 are disconnected at the same time. Then, the search for a check code of degree 1 is continued, s_6 is found, and the above decoding process is repeated until all s_k values are determined.

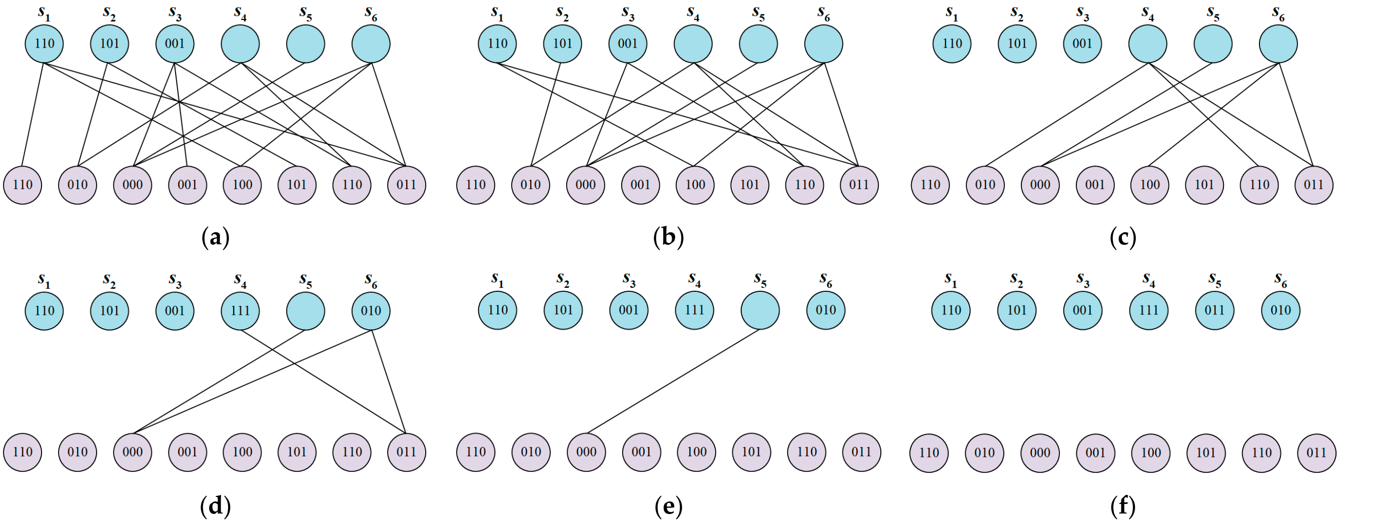


Figure 4. Data decoding process: (**a**) the received coded packets; (**b**) recovering S_1, S_2, S_3; (**c**) removing the edges connected to S_1, S_2, S_3; (**d**) recovering S_4, S_6; (**e**) removing the edges connected to S_4, S_6; (**f**) recovering S_4, S_6.

The reliability of data transmission can be improved by the introduction of redundant data, the security of data transmission can be increased through using the random coding method, and the risk of information leakage and tampering during data transmission is reduced by the forward error correction feature of the LT code. The secure data transmission method based on fountain codes adapts to a complex transmission environment, provides effective support for the secure transmission of underwater acoustic sensor networks and effectively resists active attacks during passive attacks.

4.5. Game Process between Sensor Nodes and Attackers

Source location privacy protection is an important issue in underwater acoustic communication and location-based services. The source node aims to protect its location information, while the attacker tries to obtain this information, and this competitive relationship can be modeled and analyzed by game theory. Game theory can play an important role in quantifying source location privacy and safety time and can be used to model and analyze the interactions between source nodes and potential attackers to determine the best privacy protection strategy. Through the analysis of game theory, the balance point of the strategy can be found to achieve the best trade-off between privacy protection and time efficiency, which helps to ensure that source location privacy is fully protected within a given safe time.

4.5.1. Basic Assumptions of the Game Model

The relationship between the source node and the attacker can be regarded as a zero-sum game. In general, the source node knows its own position, while the attacker can only estimate or infer the position information through certain methods [33]. In this paper, we consider a scenario where there are multiple attackers in the network, involving interactions and decisions among multiple participants. Source location privacy in underwater acoustic sensor networks usually involves multiple rounds of the game, which includes repeated strategy selection, confrontation, and adjustment between the source node and attackers. The strategies of source nodes and attackers are often dynamic and can evolve over time, and evolutionary game theory can capture these changes [34] and allow analysis strategies to adapt to changing environments over time. Unlike traditional static games, evolutionary games focus on how players choose strategies in multiple rounds of the game, and these strategies can spread and mutate through a series of evolutionary mechanisms. At the same time, evolutionary game theory no longer treats both players of the game as superrational players but believes that players usually reach game equilibrium through trial and error.

The main components of game theory include several elements: players, game strategies, and game benefits.

The participant set is $PLAYER = (player_X, player_Y, player_Z, \ldots)$. The source node $(player_X)$ is a player that actively protects its location privacy in the network, and its goal is to select a strategy that maximizes location privacy while maintaining communication performance. This paper takes the existence of two attackers as an example: A $(player_Y)$ and B $(player_Z)$ are two players who actively try to obtain the location information of the source node, and the goal is to choose a strategy to infer the location of the source node to the greatest extent.

The game strategy set is $STR = (S_X, S_Y, S_Z)$. S_X is the strategy space of the source node, and the source node can choose different protection strategies, such as a virtual coordinate system, relay node selection, and network coding, to form the source node strategy space $S_X = \{X_1, X_2\}$ (weak defense, strong defense). S_Y is the strategy space of attacker A, who can adopt methods, such as eavesdropping attack, traceback attack, traffic analysis, or cooperation with other attackers, to form the attacker's strategy space $S_Y = \{Y_1, Y_2\}$ (single attack, cooperative attack). The strategy space of attacker B, $S_Z = \{Z_1, Z_2\}$ (single attack, cooperative attack), is the same as that of attacker A. Only when both attackers choose a cooperative strategy can cooperation between the attackers be achieved.

The probability $P = (P_X, P_Y, P_Z)$ of game strategy selection is the probability set of the source node and attacker strategies, where $P_X = \{x, 1-x\}$ represents the probability of weak defense and strong defense of the source node, $P_Y = \{y, 1-y\}$ represents the probability of attacker A's single attack and cooperative attack, and $P_Z = \{z, 1-z\}$ represents the probability of attacker B's single attack and cooperative attack.

The game return can be set as $RETURN = (R_X, R_Y, R_Z)$. R_X represents the return set of the source node, R_Y represents the return set of attacker A, and R_Z represents the return set of attacker B. The return of the source node is measured by the information entropy, and the return of the attacker is measured by the information gain, indicating that the attacker's uncertainty about the location of the source node is reduced after obtaining a certain amount of information.

The game cost can be set as $COST = (C_X, C_Y, C_Z)$. C_X represents the payoff set of the source node, C_Y represents the payoff set of attacker A, and C_Z represents the payoff set of attacker B. The energy consumption of a node represents the game cost for the source node and the attacker.

4.5.2. Establishment of an Evolutionary Game Model

According to the behavioral strategies of the source node and the attacker, it can be concluded that there are eight kinds of game combinations. In game theory, the payoff usually refers to the utility or benefit that the parties involved in the game can obtain under different strategies. The game gain matrix for UASNs is derived based on the aforementioned definition in combination with the underwater acoustic sensor network model, as illustrated in Table 2.

Table 2. Game gain matrix.

Strategy combination	$\left(X_i, Y_j, Z_k\right)$
Payoff of source node gain	$R_{Xi} - R_{Yj} - R_{Zk} - C_{Xi}$
Payoff of attacker A gain	$R_{Yj} - R_{Xi} - C_{Yj}$
Payoff of attacker B gain	$R_{Zk} - R_{Xi} - C_{Zk}$

Where $i, j, k = 1$ *or* 2.

4.5.3. Replication Dynamic Equation of Tripartite Evolutionary Game

A key concept in game theory is equilibrium analysis. By studying the Nash equilibrium point of the game, insight can be gained into the interactions between the source node and the attacker and possible results. At the equilibrium point, no party can achieve better results by changing its strategy, which helps balance the trade-off between privacy protection and information access. Therefore, the payoff of the source node choosing a different strategy is

$$\begin{cases} G(X_1) = yz(R_{X1} - R_{Y1} - R_{Z1} - C_{X1}) + (1-y)z(R_{X1} - R_{Y2} - R_{Z1} - C_{X1}) \\ +y(1-z)(R_{X1} - R_{Y1} - R_{Z2} - C_{X1}) + (1-y)(1-z)(R_{X1} - R_{Y2} - R_{Z2} - C_{X1}) \\ G(X_2) = yz(R_{X2} - R_{Y1} - R_{Z1} - C_{X2}) + (1-y)z(R_{X2} - R_{Y2} - R_{Z1} - C_{X2}) \\ +y(1-z)(R_{X2} - R_{Y1} - R_{Z2} - C_{X2}) + (1-y)(1-z)(R_{X2} - R_{Y2} - R_{Z2} - C_{X2}) \end{cases}, \quad (3)$$

The average revenue of the source node is as follows: $\overline{G(X)} = xG(X_1) + (1-x)G(X_2) = \sum_i P_x G(X_i)$. The replication dynamic equation of the source node is

$$F(x) = \frac{dx(t)}{dt} = x\left(G(X_i) - \overline{G(X)}\right). \quad (4)$$

The payoff for attacker A in choosing a different strategy is

$$\begin{cases} G(Y_1) = xz(R_{Y1} - R_{X1} - C_{Y1}) + x(1-z)(R_{Y1} - R_{X1} - C_{Y1}) \\ +(1-x)z(R_{Y1} - R_{X2} - C_{Y1}) + (1-x)(1-z)(R_{Y1} - R_{X2} - C_{Y1}) \\ G(Y_2) = xz(R_{Y2} - R_{X1} - C_{Y1}) + x(1-z)(R_{Y2} - R_{X1} - C_{Y1}) \\ +(1-x)z(R_{Y2} - R_{X2} - C_{Y1}) + (1-x)(1-z)(R_{Y2} - R_{X2} - C_{Y1}) \end{cases}, \quad (5)$$

The average revenue of attacker A is as follows: $\overline{G(Y)} = yG(Y_1) + (1-y)G(Y_2) = \sum_i P_y G(Y_i)$. The replication dynamic equation of attacker A is as follows:

$$F(y) = \frac{dy(t)}{dt} = y\left(G(Y_i) - \overline{G(Y)}\right). \quad (6)$$

The payoff for attacker B in choosing a different strategy is

$$\begin{cases} G(Z_1) = xy(R_{Z1} - R_{X1} - C_{Z1}) + x(1-y)(R_{Z1} - R_{X1} - C_{Z1}) \\ +(1-x)y(R_{Z1} - R_{X2} - C_{Z1}) + (1-x)(1-y)(R_{Z1} - R_{X2} - C_{Z1}) \\ G(Z_2) = xy(R_{Z2} - R_{X1} - C_{Z2}) + x(1-y)(R_{Z2} - R_{X1} - C_{Z2}) \\ +(1-x)y(R_{Z2} - R_{X2} - C_{Z2}) + (1-x)(1-y)(R_{Z2} - R_{X2} - C_{Z2}) \end{cases}, \quad (7)$$

The average revenue of attacker B is as follows: $\overline{G(Z)} = zG(Z_1) + (1-z)G(Z_2) = \sum_i P_z G(Z_i)$. The replication dynamic equation of attacker B is as follows:

$$F(z) = \frac{dz(t)}{dt} = z\left(G(Z_i) - \overline{G(Z)}\right). \quad (8)$$

Combining the above Equations (4), (6) and (8) into Equation (9), the replication dynamic equation system is established as follows:

$$Y = \begin{bmatrix} F(x) \\ F(y) \\ F(z) \end{bmatrix} = f(Y,t) = 0. \tag{9}$$

Solving the equation yields: $Y_1 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, $Y_2 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, $Y_3 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$, $Y_4 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$, $Y_5 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$, $Y_6 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$, $Y_7 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$, and $Y_8 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$.

4.5.4. Nash Equilibrium of the Tripartite Game

Each equilibrium point in the system corresponds to an evolutionary game equilibrium. Table 3 shows the eigenvalues corresponding to all equilibrium points.

Table 3. Eigenvalues at different equilibrium points.

The Equilibrium Point	Eigenvalue 1	Eigenvalue 2	Eigenvalue 3
$(0,0,0)$	$C_{X2} - C_{X1} + R_{X1} - R_{X2}$	$C_{Y2} - C_{Y1} + R_{Y1} - R_{Y2}$	$C_{Z2} - C_{Z1} + R_{Z1} - R_{Z2}$
$(1,0,0)$	$C_{X1} - C_{X2} - R_{X1} + R_{X2}$	$C_{Y2} - C_{Y1} + R_{Y1} - R_{Y2}$	$C_{Z2} - C_{Z1} + R_{Z1} - R_{Z2}$
$(0,1,0)$	$C_{X2} - C_{X1} + R_{X1} - R_{X2}$	$C_{Y1} - C_{Y2} - R_{Y1} + R_{Y2}$	$C_{Z2} - C_{Z1} + R_{Z1} - R_{Z2}$
$(0,0,1)$	$C_{X2} - C_{X1} + R_{X1} - R_{X2}$	$C_{Y2} - C_{Y1} + R_{Y1} - R_{Y2}$	$C_{Z1} - C_{Z2} - R_{Z1} + R_{Z2}$
$(1,1,0)$	$C_{X1} - C_{X2} - R_{X1} + R_{X2}$	$C_{Y1} - C_{Y2} - R_{Y1} + R_{Y2}$	$C_{Z2} - C_{Z1} + R_{Z1} - R_{Z2}$
$(1,0,1)$	$C_{X1} - C_{X2} - R_{X1} + R_{X2}$	$C_{Y2} - C_{Y1} + R_{Y1} - R_{Y2}$	$C_{Z1} - C_{Z2} - R_{Z1} + R_{Z2}$
$(0,1,1)$	$C_{X2} - C_{X1} + R_{X1} - R_{X2}$	$C_{Y1} - C_{Y2} - R_{Y1} + R_{Y2}$	$C_{Z1} - C_{Z2} - R_{Z1} + R_{Z2}$
$(1,1,1)$	$C_{X1} - C_{X2} - R_{X1} + R_{X2}$	$C_{Y1} - C_{Y2} - R_{Y1} + R_{Y2}$	$C_{Z1} - C_{Z2} - R_{Z1} + R_{Z2}$

Using the indirect Lyapunov method, if all the eigenvalues of the Jacobian matrix have a negative real part, the equilibrium point is an asymptotically stable point. When $C_{X2} - C_{X1} + R_{X1} - R_{X2} > 0$, $C_{Y2} - C_{Y1} + R_{Y1} - R_{Y2} > 0$, and $C_{Z2} - C_{Z1} + R_{Z1} - R_{Z2} > 0$ are satisfied, the above eight equilibrium points are all stable.

5. Experimental Simulation and Analysis

5.1. Simulation Setup

In this paper, the performance of the SLP-MACGT model is compared with that of the stratification-based source location privacy scheme (SSLP) [11], the push-based probabilistic method source location privacy scheme (PP-SLPP) [12], and the multi-round game-based source location privacy scheme (MRGSLP) [35]. Simulations were performed using MATLAB 2021 to evaluate the performance of these models. In the simulations, all sensor nodes are randomly distributed in a space of 1000 m × 1000 m × 1000 m with the default simulation parameters listed in Table 4.

The performance evaluation indexes used in this paper are

- Packet delivery ratio (PDR): PDR is the probability of successfully forwarding data packets from the source node to the sink node;
- Network safety time: Network safety time refers to the time between the activation of the source node and the successful detection of the source node by the attacker under the premise that the source node continues to send packets;
- End-to-end delay: End-to-end delay represents the time required to transmit a data packet from a source node to the sink node;

- Energy consumption: Energy consumption represents the energy consumption of transmitting and receiving data and controlling data packets during a simulation run.

Table 4. Simulation parameters.

Parameters	Default Values
Scale of the space	1000 m × 1000 m × 1000 m
Number of nodes	250
Node placement method	Random placement
Range of communication	200 m
Initial energy	100 J
Data packet size	1024 bits
Control package size	128 bits
Transmit power	2 W
Received power	0.2 W

According to Xing et al. [36], the energy consumed by a sensor node to send a data packet with l bits can be expressed as follows:

$$E_{sent}(l,d) = lP_0A(d,f) = lP_0d^k\alpha(f)^d, \tag{10}$$

where P_0 is the received power level of the node, $A(d,f)$ is the power attenuation coefficient relevant to the distance, k is the spreading factor of the propagation geometry, and $\alpha(f)$ is the acoustic signal absorption coefficient.

The energy consumed by the node to receive l bits data can be calculated by

$$E_{received}(l) = lE_1. \tag{11}$$

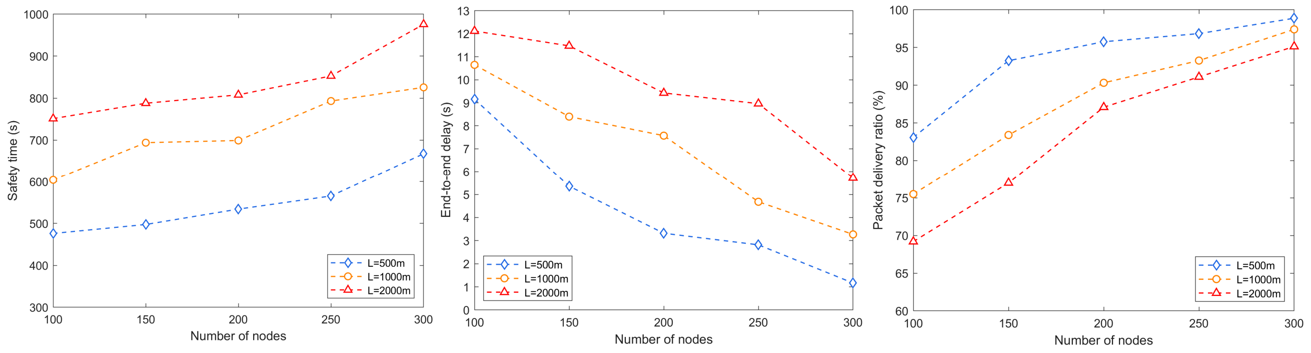
where E_1 represents the reception coefficient, which is the energy consumption for receiving 1 bit data.

5.2. Performance of the SLP-MACGT Model

5.2.1. Effect of the Network Side Length on Performance

The network scale plays an important role in network performance. When the network scale increases, such as increasing the number of nodes or the side length of the network, it will directly affect the capacity, coverage, transmission efficiency and data security of the network. L represents the network side length, which is the length, width and height of the network space. In the following, we explore the impact of different network sizes (L = 500 m, 1000 m, and 2000 m) on source location privacy protection. As shown in Figure 5a, increasing the number of nodes can enhance the capacity and coverage of the network while improving the privacy protection of the source location when the length of the network side is fixed. As the scale of the network increases, the communication paths between nodes become longer, resulting in prolonged information transmission times. This may increase the time needed for attackers to obtain the source location information. Therefore, increasing the number of nodes and the side length of the network will result in a longer safety time.

As shown in Figure 5b,c, more nodes can provide more path choices, reduce congestion and network delay, and improve the transmission efficiency of data packets in the network, thus increasing the packet forwarding rate. However, the increase in network side length leads to longer transmission paths between nodes, which increases the delay of data transmission, negatively affecting real-time applications and delay-sensitive tasks. At the same time, a longer network side length increases the risk of instability and packet loss during data transmission. The packets need to pass through more nodes during forwarding and may face problems such as signal attenuation, interference, or node failure, which leads to a decrease in the packet delivery ratio.

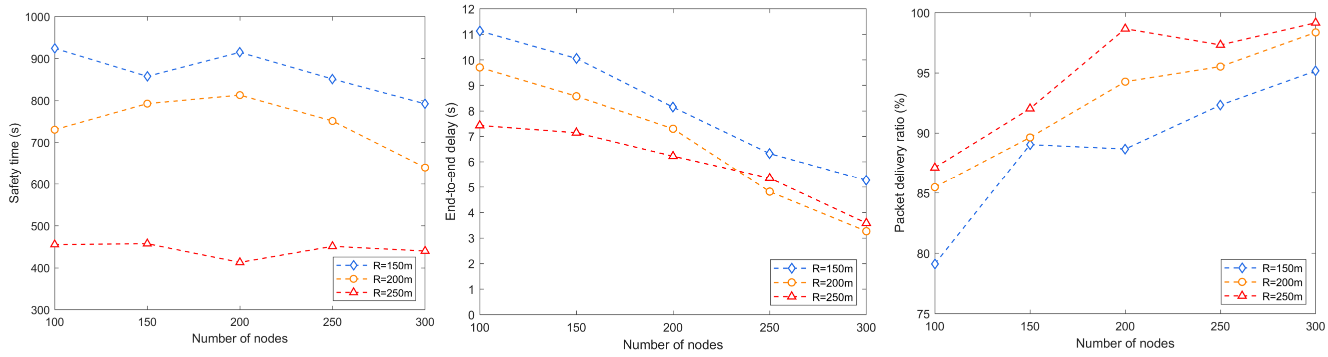


(**a**) (**b**) (**c**)

Figure 5. Effect of network side length on performance: (**a**) safety time; (**b**) end-to-end delay; (**c**) packet delivery ratio.

5.2.2. Effect of the Communication Radius on Performance

The following experiment investigates the effect of the communication radius on performance. As shown in Figure 6a, when the communication radius increases, the communication range between nodes expands, and the probability of an attacker contacting the network also increases. Therefore, a larger transmission radius may lead to a shorter safety time, and it will be easier for the attacker to obtain the source location information.



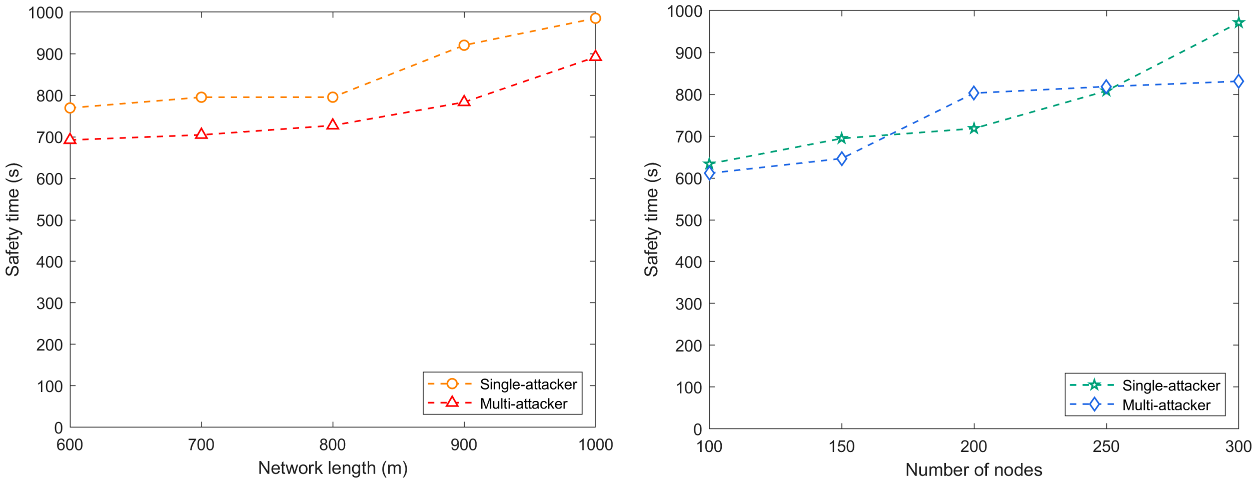
(**a**) (**b**) (**c**)

Figure 6. Effect of the communication radius on performance: (**a**) safety time; (**b**) end-to-end delay; (**c**) packet delivery ratio.

As shown in Figure 6b, a larger communication radius means that data may be delivered through fewer intermediate nodes, thus reducing latency. As shown in Figure 6c, the change in the communication range may affect the direct communication ability between nodes. If the communication range is reduced, the direct connections between nodes may decrease, resulting in a lower success rate of data forwarding. In contrast, an increase in the communication range may increase the direct connection between nodes and may help improve the data forwarding success rate.

5.2.3. Effect of the Number of Attackers on the Safety Time

As shown in Figure 7, it typically takes more time for a single attacker to successfully breach or compromise network security. They may need to conduct eavesdropping, analysis, and attack attempts for longer periods of time to identify weaknesses and obtain valuable data. In contrast, multiple attackers can attack different targets at the same time, taking advantage of cooperation to speed up the attack and shorten the time window for a successful attack. A larger network scale complicates the transmission path, and the attacker needs more time to obtain the source location information. In addition, a longer network side length may result in a longer signal transmission path, which increases the time required for the attacker to determine the source location.



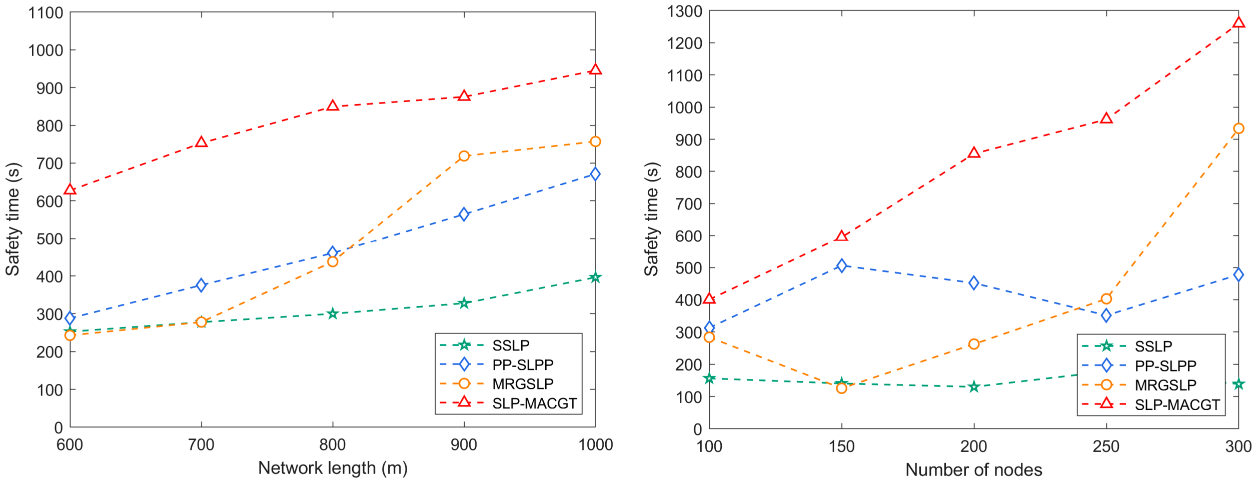
(**a**) (**b**)

Figure 7. Safety time for a single attacker and multiple attackers: (**a**) network side length vs. safety time; (**b**) number of nodes vs. safety time.

5.3. SLP-MACGT Comparison with Other SLP Schemes

5.3.1. Network Safety Time

In the evaluation of network safety time depicted in Figure 8a, the influence of network side length on algorithm performance is striking. With the integration of multiple source location privacy protection strategies and the attainment of Nash equilibrium via evolutionary games, SLP-MACGT emerges as the frontrunner among the algorithms considered. Conversely, the safety times of SSLP and PP-SLPP exhibit dependence on AUV movement. When the network scale increases, the safety times of these three algorithms will suddenly increase.



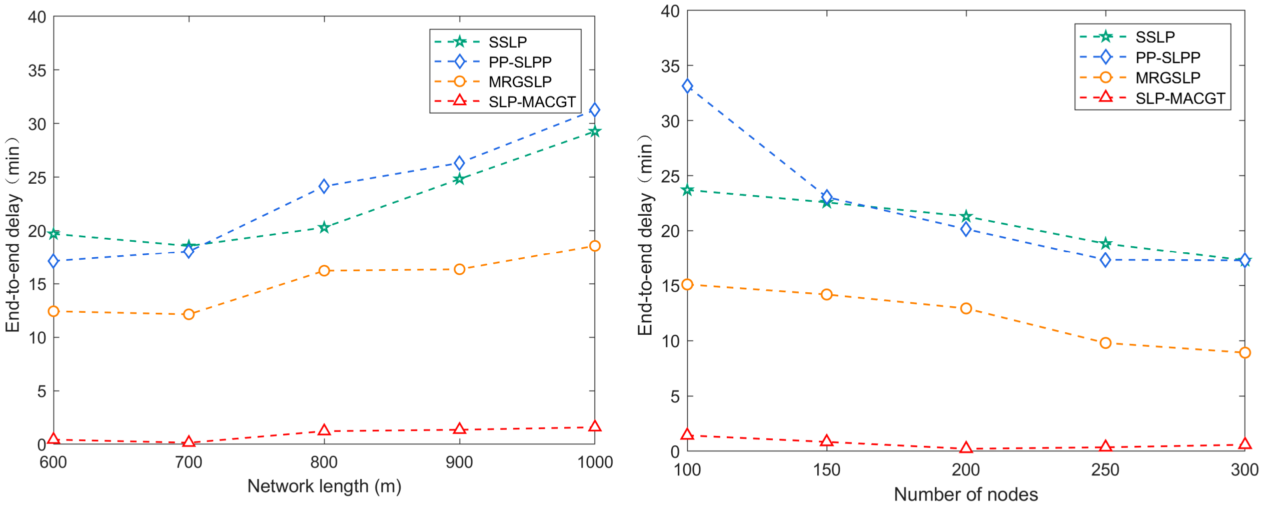
(**a**) (**b**)

Figure 8. Safety time: (**a**) network side length vs. safety time; (**b**) number of nodes vs. safety time.

Moreover, Figure 8b offers results into safety time dynamics concerning varying node counts. Despite fluctuations in the curves, a consistent trend emerges: both the SLP-MACGT algorithm and its counterparts exhibit an incremental rise in safety times with increasing sensor nodes. This trend stems from the heightened node density, which augments the number of available transmission paths, thereby enhancing path diversity and bolstering the overall network safety time. Notably, the performance of MRGSLP initially falters, but it gradually improves, which could be chiefly attributed to communication range adjustments.

5.3.2. End-to-End Delay

Figure 9a shows that in terms of latency, SLP-MACGT exhibits significantly lower end-to-end latency compared to SSLP, PP-SLPP, and MRGSLP. While PP-SLPP, SSLP, and MRGSLP experience a notable increase in latency due to the utilization of AUVs, with latency on the order of minutes, the latency magnitude of SLP-MACGT is on the scale of seconds. Specifically, the higher latency in PP-SLPP compared to SSLP is attributed to the time taken for the leading AUV to collect data from all following AUVs, whereas in SSLP, AUVs collect data based on trajectories without significant delays. MRGSLP divides the network into static and dynamic layers, with nodes in the static layer requiring AUV assistance for data transmission.



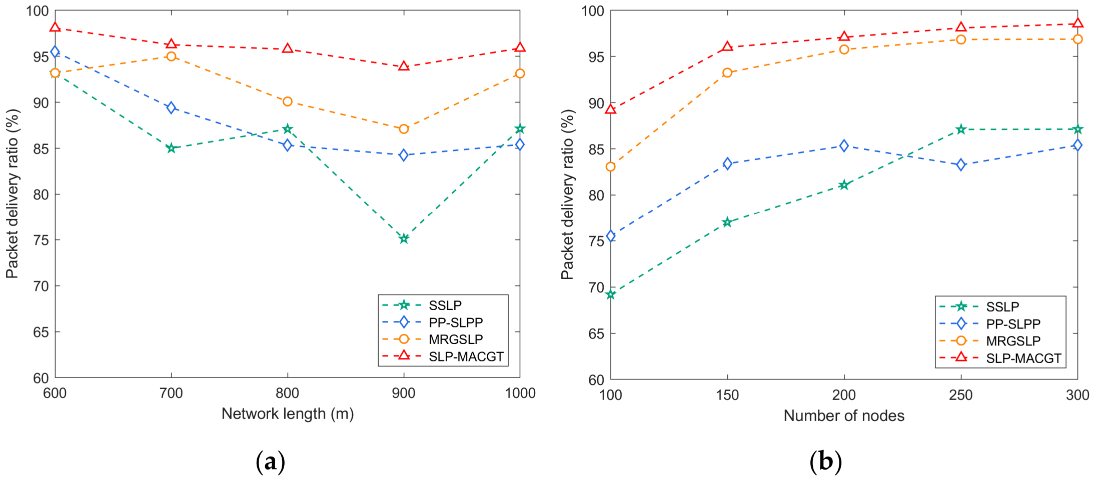
(**a**) (**b**)

Figure 9. End-to-end delay: (**a**) network side length vs. end-to-end delay; (**b**) number of nodes vs. end-to-end delay.

Moreover, Figure 9a indicates that latency increases with the growth of the network edge length. In Figure 9b, the fluctuations in PP-SLPP latency stem from variances in pushing positions and random initial positions of AUV groups. The latency of SSLP increases with the rising number of nodes as AUVs collect data from more nodes along fixed trajectories. In SLP-MACGT, as the number of nodes increases, senders can choose the next hop nodes closer to the convergence node, resulting in a gradual decrease in latency as node count rises.

5.3.3. Packet Delivery Ratio

Figure 10 shows that SLP-MACGT demonstrates the highest data packet transmission rate among the compared protocols. SLP-MACGT implements a secure data transmission strategy based on fountain codes, which enhances the success rate of data transmission while reducing the need for data retransmission. In PP-SLPP, AUVs primarily handle most of the network functionalities, and the data packet transmission rate in PP-SLPP is influenced by the collaboration between leading AUVs and their followers, as the leading AUVs gather data from all the following AUVs.



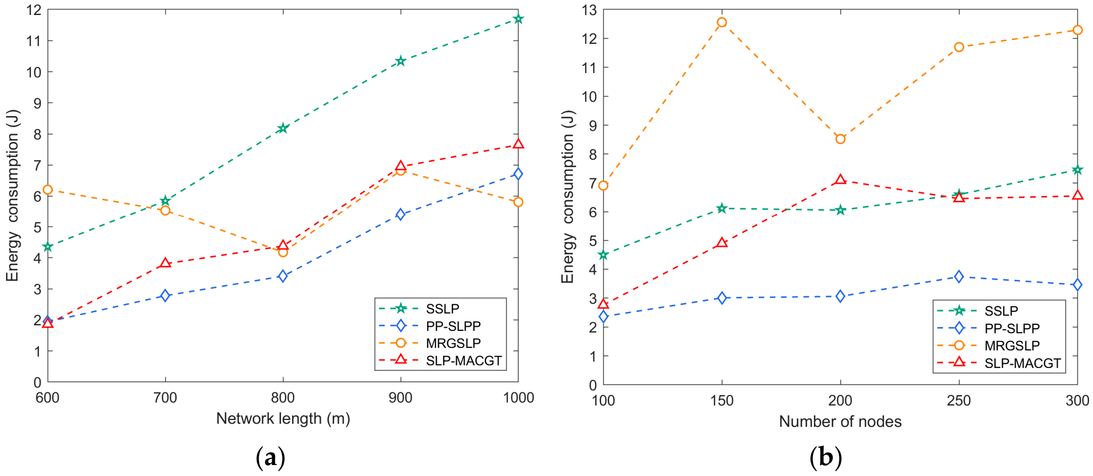
(**a**) (**b**)

Figure 10. Packet delivery ratio: (**a**) network side length vs. packet delivery ratio; (**b**) number of nodes vs. packet delivery ratio.

SSLP utilizes AUVs to collect data and necessitates periodic data relaying, potentially leading to higher node energy consumption, thereby influencing data packet transmission rates. As the number of nodes increases, AUVs collect data from more nodes along fixed trajectories, impacting data packet transmission rates. MRGSLP partitions the network into static and dynamic layers, with nodes in the static layer requiring assistance from AUVs for data transmission. This layering scheme may influence data packet transmission rates.

5.3.4. Energy Consumption

Figure 11a illustrates the comparison of node energy consumption among different methods, showcasing that the energy consumption of SLP-MACGT remains at an intermediate level even when facing multiple attackers. The incorporation of network coding and multi-round games in SLP-MACGT does impose a slight burden on the nodes; however, the variance in energy consumption between SLP-MACGT and MRGSLP is not notably significant. In contrast, the utilization of SSLP results in the highest energy consumption by nodes due to the traversal of multiple AUVs across all clusters and the energy requirements for periodic data relays. Conversely, PP-SLPP demonstrates relatively low energy consumption as several AUVs manage the majority of network functions, thereby consuming the bulk of the energy resources.



(**a**) (**b**)

Figure 11. Energy consumption: (**a**) network side length vs. energy consumption; (**b**) number of nodes vs. energy consumption.

Furthermore, Figure 11b provides additional insights into the comparison of energy consumption across varying numbers of nodes. In SSLP and PP-SLPP, changes in the node count have minimal effects on energy consumption, as AUVs predominantly handle data transmission tasks. Conversely, in SLP-MACGT and MRGSLP, nodes are responsible for a significant portion of the network functionality, leading to heightened energy consumption during simulation scenarios. Notably, the adaptive coding strategy employed in SLP-MACGT enhances data transmission success rates, reduces the need for data retransmissions, and ultimately lowers overall energy consumption compared to MRGSLP.

6. Conclusions

Source location privacy protection is a challenging task in underwater acoustic sensor networks. This paper discusses the key challenges of source location privacy protection, designs for the scenario of multiple cooperative attackers, and proposes an underwater source location privacy protection scheme based on game theory. The scheme comprehensively considers privacy protection, delay and energy issues, and it effectively protects the source location privacy by means of virtual coordinate system transformation, relay node selection strategy and fountain code secure data transmission technology. The introduction of game theory as a framework allows strategic interaction between source nodes and malicious nodes, provides a new perspective for source location privacy protection in underwater acoustic sensor networks, and improves network security. The simulation results show that the proposed scheme achieves significant improvements in terms of packet delivery ratio, security time, delay and energy consumption. The packet delivery rate average increases by 30%, security time is extended by at least 85%, and the delay is reduced by at least 90% compared with SSLP, PP-LSPP, and MRGSLP, which provides strong support for the security and performance of underwater acoustic sensor networks.

However, there are some limitations to the proposed scheme. Due to the lack of real marine data, mathematical methods are currently the only means to quantify the benefits and costs of the game between source nodes and attackers. In the future, research needs to delve deeper into the cooperative patterns among multiple attackers to devise more effective response strategies. Considering simulation experiments and actual observational data for validating and optimizing the accuracy and practicality of the model, and further understanding the advantages and limitations of various methods, will be crucial in exploring more effective and reliable source location privacy protection mechanisms to ensure location privacy and data security in underwater acoustic sensor networks.

Author Contributions: Conceptualization, B.W. and X.Y.; methodology, B.W. and Y.L.; software, B.W., X.Y. and Y.L.; validation, K.H., Y.L. and X.Y.; formal analysis, K.H.; investigation, X.Y.; resources, X.Z.; data curation, X.Z.; writing—original draft preparation, X.Y.; writing—review and editing, K.H. and B.W.; visualization, Z.L.; supervision, Z.L.; project administration, K.H.; funding acquisition, K.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Chunhui Cooperation Program of the Ministry of Education, HZKY20220590-202200265; National Natural Science Foundation of China under Grant 61902273.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Lyu, C.; Hu, X.; Niu, Z.; Yang, B.; Jin, J.; Ge, C. A light-weight neural network for marine acoustic signal recognition suitable for fiber-optic hydrophones. *Expert Syst. Appl.* **2024**, *235*, 121235. [CrossRef]
2. Uyan, O.G.; Akbas, A.; Gungor, V.C. Machine learning approaches for underwater sensor network parameter prediction. *Ad. Hoc Netw.* **2023**, *144*, 103139. [CrossRef]
3. Han, G.; Chen, Y.; Wang, H.; He, Y.; Peng, J. AUV-Aided Data Importance Based Scheme for Protecting Location Privacy in Smart Ocean. *IEEE Trans. Veh. Technol.* **2022**, *71*, 9925–9936. [CrossRef]
4. Wang, Z.; Du, J.; Jiang, C.; Zhang, Z.; Ren, Y.; Han, Z. Dynamic Packet Routing Based on Acoustic Signal Curve Propagation in the AUV-Assisted IoUT. *IEEE Internet Things J.* **2023**, *11*, 9854–9869. [CrossRef]
5. Han, G.; Shen, S.; Song, H.; Yang, T.; Zhang, W. A Stratification-Based Data Collection Scheme in Underwater Acoustic Sensor Networks. *IEEE Trans. Veh. Technol.* **2018**, *67*, 10671–10682. [CrossRef]
6. Wang, Y.; Tian, Z.; Sun, Y.; Du, X.; Guizani, N. Preserving location privacy in UASN through collaboration and semantic encapsulation. *IEEE Netw.* **2020**, *34*, 284–290. [CrossRef]
7. Sendra, S.; Lloret, J.; Jimenez, J.M.; Parra, L. Underwater acoustic modems. *IEEE Sens. J.* **2015**, *16*, 4063–4071. [CrossRef]
8. Zia, M.Y.I.; Poncela, J.; Otero, P. State-of-the-art underwater acoustic communication modems: Classifications, analyses and design challenges. *Wirel. Pers. Commun.* **2021**, *116*, 1325–1360. [CrossRef]
9. Abdalzaher, M.S.; Muta, O. A game-theoretic approach for enhancing security and data trustworthiness in IoT applications. *IEEE Internet Things J.* **2020**, *7*, 11250–11261. [CrossRef]
10. Shokri, R.; Theodorakopoulos, G.; Troncoso, C. Privacy games along location traces: A game-theoretic framework for optimizing location privacy. *ACM Trans. Priv. Secur. TOPS* **2016**, *19*, 1–31. [CrossRef]
11. Tian, X.; Du, X.; Wang, L.; Zhao, L.; Han, D. LSLPR: A Layering and Source-Location-Privacy-Based Routing Protocol for Underwater Acoustic Sensor Networks. *IEEE Sens. J.* **2023**, *23*, 23676–23691. [CrossRef]
12. Wang, H.; Han, G.; Hou, Y.; Guizani, M.; Peng, Y. A Multi-Channel Interference Based Source Location Privacy Protection Scheme in Underwater Acoustic Sensor Networks. *IEEE Trans. Veh. Technol.* **2022**, *71*, 2058–2069. [CrossRef]
13. Yanti, Y.; Away, Y.; Arif, T.Y.; Nasaruddin, N. Routing technique in location source privacy for wireless sensor network: A review. *AIP Conf. Proc.* **2024**, *3082*, 050002.
14. Yang, G.; Dai, L.; Wei, Z. Challenges, threats, security issues and new trends of underwater wireless sensor networks. *Sensors* **2018**, *18*, 3907. [CrossRef] [PubMed]
15. Luo, J.; Chen, Y.; Wu, M.; Yang, Y. A survey of routing protocols for underwater wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 137–160. [CrossRef]
16. Ozturk, C.; Zhang, Y.; Trappe, W.; Ott, M. Source-location privacy for networks of energy-constrained sensors. In Proceedings of the Second IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems, Vienna, Austria, 12 May 2004; pp. 68–72.
17. Koh, J.Y.; Leong, D.; Peters, G.W.; Nevat, I.; Wong, W.-C. Optimal Privacy-Preserving Probabilistic Routing for Wireless Networks. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2105–2114. [CrossRef]
18. Chen, Y.; Sun, J.; Yang, Y.; Li, T.; Niu, X.; Zhou, H. PSSPR: A source location privacy protection scheme based on sector phantom routing in WSNs. *Int. J. Intell. Syst.* **2021**, *37*, 1204–1221. [CrossRef]
19. Sun, J.; Chen, Y.; Lv, X.; Qian, X. A Multipath Source Location Privacy Protection Scheme in Wireless Sensor Networks via Proxy Node. In Proceedings of the 2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Espoo, Finland, 22–25 August 2022; pp. 280–286.
20. Wu, X.; Ji, G.; Dou, W.; Yu, S.; Qi, L. Game Theory for Mobile Location Privacy. In Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, Taipei, Taiwan, 6 October 2020; pp. 106–116.
21. Han, G.; Wang, H.; Ansere, J.A.; Jiang, J.; Peng, Y. SSLP: A Stratification-Based Source Location Privacy Scheme in Underwater Acoustic Sensor Networks. *IEEE Netw.* **2020**, *34*, 188–195. [CrossRef]
22. Wang, H.; Han, G.; Zhang, Y.; Xie, L. A Push-Based Probabilistic Method for Source Location Privacy Protection in Underwater Acoustic Sensor Networks. *IEEE Internet Things J.* **2022**, *9*, 770–782. [CrossRef]
23. Liu, Y.; Han, G.; Wang, H.; Jiang, J. FPTSA-SLP: A Fake Packet Time Slot Assignment-based Source Location Privacy Protection Scheme in Underwater Acoustic Sensor Networks. In Proceedings of the 2021 Computing, Communications and IoT Applications (ComComAp), Shenzhen, China, 26–28 November 2021; pp. 307–311.
24. Han, G.; Liu, Y.; Wang, H.; Zhang, Y. A Collision-Free-Transmission-Based Source Location Privacy Protection Scheme in UASNs Under Time Slot Allocation. *IEEE Internet Things J.* **2023**, *10*, 1546–1557. [CrossRef]
25. Wang, H.; Han, G.; Liu, Y.; Li, A.; Jiang, J. AUV-Assisted Stratified Source Location Privacy Protection Scheme based on Network Coding in UASNs. *IEEE Internet Things J.* **2023**, *10*, 10636–10648. [CrossRef]
26. Jian, Y.; Chen, S.; Zhang, Z.; Zhang, L. A novel scheme for protecting receiver's location privacy in wireless sensor networks. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 3769–3779. [CrossRef]
27. Wang, Q.; Dai, H.N.; Li, X.; Wang, H.; Xiao, H. On Modeling Eavesdropping Attacks in Underwater Acoustic Sensor Networks. *Sensors* **2016**, *16*, 721. [CrossRef]

28. Li, F.; Ren, P.; Yang, G.; Sun, Y.; Wang, Y.; Wang, Y.; Li, S.; Zhou, H.; Li, W. An Efficient Anonymous Communication Scheme to Protect the Privacy of the Source Node Location in the Internet of Things. *Secur. Commun. Netw.* **2021**, *2021*, 6670847. [CrossRef]
29. Ghoshal, R.; Mitra, N. Underwater explosion induced shock loading of structures: Influence of water depth, salinity and temperature. *Ocean Eng.* **2016**, *126*, 22–28. [CrossRef]
30. Ozmen, A.; Yildiz, H.U.; Tavli, B. Impact of minimizing the eavesdropping risks on lifetime of underwater acoustic sensor networks. In Proceedings of the 2020 28th Telecommunications Forum (TELFOR), Belgrade, Serbia, 24–25 November 2020; pp. 1–4.
31. Zhao, H.; Gong, Z.; Yan, J.; Li, C.; Guan, X. Unsynchronized Underwater Localization with Isogradient Sound Speed Profile and Anchor Location Uncertainties. *IEEE Trans. Veh. Technol.* **2024**, 1–14. [CrossRef]
32. Puducheri, S.; Kliewer, J.; Fuja, T.E. The design and performance of distributed LT codes. *IEEE Trans. Inf. Theory* **2007**, *53*, 3740–3754. [CrossRef]
33. Bian, Y.; Lin, H.; Song, Y. Game model of attack and defense for underwater wireless sensor networks. In Proceedings of the 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 17–19 June 2022; pp. 559–563.
34. Adami, C.; Schossau, J.; Hintze, A. Evolutionary game theory using agent-based methods. *Phys. Life Rev.* **2016**, *19*, 1–26. [CrossRef] [PubMed]
35. Wang, H.; Han, G.; Lai, W.; Hou, Y.; Lin, C. A Multi-Round Game-based Source Location Privacy Protection Scheme with AUV enabled in Underwater Acoustic Sensor Networks. *IEEE Trans. Veh. Technol.* **2023**, *72*, 7728–7742. [CrossRef]
36. Xing, G.; Chen, Y.; Hou, R.; Dong, M.; Zeng, D.; Luo, J.; Ma, M. Game-theory-based clustering scheme for energy balancing in underwater acoustic sensor networks. *IEEE Internet Things J.* **2021**, *8*, 9005–9013. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.