Journal of *Marine Science and Engineering*

MDPI

Article

A Secure Localization Scheme for UASNs Based on Anchor Node Self-Adaptive Adjustment

Ping Ding [1], Ziyu Zhou [1], Jinglan Ma [1], Guozhen Xing [1], Zhigang Jin [2,*] and Ye Chen [1,2,*]

[1] School of Applied Science and Technology, Hainan University, Haikou 570228, China
[2] School of Electrical and Information Engineering, Tianjin University, Tianjin 300072, China
* Correspondence: zgjin@tju.edu.cn (Z.J.); chenye@hainanu.edu.cn (Y.C.)

Abstract: The UASNs are widely used in underwater communications and monitoring, and many applications require accurate information regarding the position of nodes. However, intentional attacks against devices or information transmission may exist in the network, and the localization process is periodic, so it is necessary to quickly address attacks and optimize the network structure. This paper proposed an anchor node self-adaptive adjustment localization scheme (ASAL), in which the anchor node can adjust the state and depth of its participation. Two filters were used to adjust the states of referable nodes. The first filter was based on the distance difference of reverse information transmission after direct localization based on anchor nodes. The second was based on the error of the anchor node's reverse localization after network localization was completed. In addition, a depth-adjustment mechanism of anchor nodes was proposed to optimize the network structure, the virtual force vector was introduced to describe the cost of depth adjustment, and the whale optimization algorithm was used to converge to the depth with the minimum total cost. The simulation results showed that the scheme can ensure localization accuracy and coverage in attack scenarios and reduce localization energy consumption.

Keywords: secure localization; TDoA; referable nodes; self-detection; depth adjustment; underwater acoustic sensor networks

Citation: Ding, P.; Zhou, Z.; Ma, J.; Xing, G.; Jin, Z.; Chen, Y. A Secure Localization Scheme for UASNs Based on Anchor Node Self-Adaptive Adjustment. *J. Mar. Sci. Eng.* **2023**, *11*, 1354. https://doi.org/10.3390/jmse11071354

Academic Editor: Rouseff Daniel

Received: 2 June 2023
Revised: 26 June 2023
Accepted: 1 July 2023
Published: 3 July 2023

1. Introduction

The underwater acoustic sensor networks (UASNs) are widely used to acquire underwater information [1–3]. Due to the complex and changeable underwater environment [4–6], the data transmission rate is slow, the transmission distance is limited, and it is also interfered with by many factors. In a large-scale underwater environment, deployed nodes are usually sparse [7,8], and due to the influence of underwater ocean currents and other factors, the location of nodes is usually uncertain and variable [9,10]. Therefore, in practical situations, the localization scheme must be considered from many aspects, such as information utilization rate, network energy consumption, and localization cycle.

UASNs are mainly composed of ordinary and anchor nodes. The anchor node has accurate location information, which is used to help the ordinary node locate. After the ordinary node obtains the location information, it can also help to locate other unknown nodes. However, this process usually has a problem: the localization error gradually enlarges. Hence, it must be analyzed again and adjusted after localization is completed to achieve the most accurate node localization with the least energy consumption. In addition, the mobility of nodes in UASNs means that localization is impermanent and needs to be carried out periodically.

Because of the environment's complexity, UASNs are more vulnerable to attacks than terrestrial networks [11,12], so security is crucial. However, in UASNs [3,13], there is much research on precise low-energy localization, but the security problems engendered by attacks should be considered more. In the context of military applications, belligerents

can easily find and destroy a buoy floating on the ocean surface. Attacks on information transmission cause some nodes to be destroyed by belligerents and to be used to transmit misleading information to prevent the accurate localization of unknown nodes [14–17]. To determine the sensor nodes' location conveniently and safely, we modified the buoy into a base fixed on the seabed and connected it with an underwater data center with submarine cables [18,19], achieving precise control of the anchor nodes' movement in the vertical direction. Therefore, the cable on the vertical line where the anchor node is located plays the role of adjusting the anchor node's depth and transmitting the information. An underwater cable [20,21] is characterized by strong transmission capacity, high reliability, a high safety index, long service life, and low maintenance cost, and is buried in the seabed by different technologies according to different environments for signal transmission.

The main contributions of this paper are as follows:

1. A new UASN architecture was proposed in which the sensor nodes can move vertically, and the cable and data center realize the interaction and control of underwater information;
2. A referable node filtering mechanism was proposed. After direct localization based on anchor nodes, the trusted referable nodes were filtered out based on the distance sent by the reverse information and the distance difference calculated by the localization result, and these nodes were used in the subsequent iterative localization;
3. To make full use of the anchor node's computing resources, a self-detection mechanism of the anchor node was proposed, which estimated its position by using the nodes around it and judging whether it is being attacked or not based on the difference between the estimated location and the actual location;
4. To periodically optimize the network, an anchor node depth-adjustment strategy was proposed. A virtual force vector was introduced to describe the cost of depth adjustment, and the WOA was used to converge to the depth with a minimum total cost.

The rest of this paper is organized as follows. Section 2 introduces the previous work related to this paper. Section 3 introduces the network model of the proposed UASN. Section 4 introduces the localization mode, attack mode, and secure localization algorithm, then introduces the anchor nodes' self-detection mechanism and depth-adjustment mechanism. In Section 5, our proposed scheme is verified through simulation analysis. Finally, Section 6 summarizes our work and discusses future research directions.

2. Related Work

The most classic localization algorithms for WSNs include ToA [22], TDoA [23], AoA [24] and RSSI [25]. However, these algorithms cannot guarantee the accuracy and energy of localization when they are used in sparse and harsh underwater environments. Recently, people have proposed many improved localization schemes based on these algorithms. In [26], Liang et al. proposed a TDoA algorithm for the underwater environment. The improved UWB Saleh Valenzuela (S-V) model was applied to characterize the underwater acoustic fading channel. The introduction of underwater channel modeling enables the application of TDoA in underwater environments but cannot guarantee security in attack scenarios. A robust target-tracking algorithm based on TDoA can be used to estimate the target location when the sensor network obtains insufficient and inaccurate information [27].

Due to the limitation of moving range, ordinary nodes can only send location information to adjacent sensor nodes within their communication radius. When the nodes' number is insufficient, the localization rate greatly reduces. In this case, sensor nodes with autonomous mobility, such as AUVs and mobile beacons, can deal with this problem. In [28], Hao et al. proposed an AUV-assisted TDoA localization algorithm. The cost of moving beacons is lower compared with AUV, but in most cases, they can only move in one direction. In [29], Erol-Kantarci et al. used DNR beacons to locate. These beacons obtain coordinates from GPS when floating on the water and then dive into the water

to broadcast their locations during sinking and rising to locate the unknown nodes. The DNR beacon can provide relatively accurate location information, but it needs to float on the water surface and dive regularly, requiring high maintenance costs, and it may be maliciously salvaged. In [30], Su et al. proposed an iterative localization mechanism based on mobile beacons. Layering mobile beacons underwater can help locate unknown nodes. The introduction of mobile nodes can help improve localization coverage, but it requires accurate path planning and control, and, considering both cost and security issues, requires specialized hardware design.

However, these existing localization schemes often fail in the presence of attacks. Han et al. [31] proposed a collaborative secure localization algorithm based on a trust model (CSLT) aimed at malicious nodes in various attacks. The proposed algorithm conducts trust evaluation for node selection. However, this algorithm cannot find malicious nodes for each type of attack in mixed attack scenarios. Analogously, Misra et al. [32] proposed the SecRET algorithm based on the trustworthiness of nodes. This algorithm uses the Dempster–Shafer theory (DST) to combine evidence from different nodes autonomously and evaluates the nodes' trust level using multidimensional trust metrics. However, the localization accuracy of SecRET decreases with increasing node density. For different attacks, Shanthi et al. [33] estimates the parameters of the probability scheme by generating the required training set under various attacks and uses the proposed probability scheme and particle swarm optimization (PSO) to isolate malicious nodes. However, this algorithm cannot generate the optimal training set for the best performance due to the UASN's complex and dynamic environment. Regarding signal processing in transmission, Baranidharan et al. [34] proposed an improved secure localization algorithm based on the gradient descent algorithm (GDA) to remove misleading information. However, this algorithm does not consider the existence of malicious nodes among anchor nodes. Gao et al. [35] proposed a resilient target localization algorithm to counteract false clock data attacks (FCDA) in synchronization processes. It utilizes adaptive threshold secure testing to determine position accuracy and a deviation-tolerant secure target localization consensus algorithm (DLCA) to reduce the weight of attacked estimates. However, average clock synchronization approximation may cause computational errors in real environments, and the calculation of adaptive thresholds wastes transmission time and increases the workload on sensors.

In common network architecture, the underwater information is transmitted to the surface beacon node through multi-hop nodes, and then the information is shared through satellite. Unique network architecture was presented in [36], in which the information obtained by sensors was directly transmitted to the land base station through cables erected on the seabed, which can solve the malicious capture of buoys on the surface. In [37], a secure localization algorithm for information transmission attacks was proposed, which combines iterative gradient descent with selective pruning of inconsistent measurement to achieve accurate localization in attack scenarios. These two articles provide solutions to attacks on devices and information transmission in underwater sensor networks, respectively.

Therefore, this article proposed a localization scheme of secure UASNs based on anchor node self-adaptive adjustment to ensure localization accuracy and coverage and to minimize energy consumption in sparse underwater environments with attacks.

3. System Model

This paper proposed new UASN architecture consisting of sensor nodes, submarine cables, anchoring equipment, and an underwater data center. Sensor nodes were divided into anchor nodes and ordinary nodes. As shown in Figure 1, anchor nodes with accurate location information were anchored on the seabed by anchoring equipment, can directly communicate with the underwater data center, and have vertical mobility. The ordinary nodes need to locate themselves. Each sensor node has a CTD (conductivity, temperature, depth) sensor [38], which can estimate the sound-propagation speed underwater. Submarine cables are divided into the main cable and sub-cables. The main cable connects the

underwater data center and the seashore control center to realize the information exchange between land and underwater. The sub-cable connects the underwater data center and the anchor nodes through anchoring equipment to realize underwater information collection and global control of the distribution of the anchor nodes.

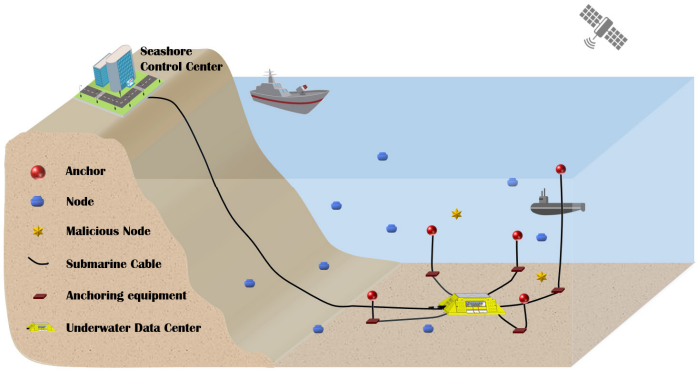

Figure 1. Network scenario of the proposed mechanism.

In the three-dimensional underwater space, each node in the network is equipped with a corresponding ID, and there are m anchor nodes, which can be expressed as $A = \{Anchor_1, Anchor_2, \cdots, Anchor_n, \cdots, Anchor_m\}, (1 \leq n \leq m)$. The location of $Anchor_n$ is expressed as $L_n = [X_n, Y_n, Z_n]^T$. There are j ordinary nodes, which can be expressed as $N = \{Node_1, Node_2, \cdots, Node_i, \cdots, Node_j\}, (1 \leq i \leq j)$. The estimated location of $Node_i$ using the localization algorithm is expressed as $\hat{P}_i = [\hat{x}_i, \hat{y}_i, \hat{z}_i]^T$, and its precise location is expressed as $P_i = [x_i^{true}, y_i^{true}, z_i^{true}]^T$. $Node_i$ is an upgraded node, $U - node_i$, after it is located, and subsequently participates in the localization of other unknown nodes after filtering.

Intentional attacks on UASNs may destroy some nodes and prevent the accurate localization of the remaining sensors by the transmission of misleading information. Since a belligerent's attack on ordinary nodes is not cost effective, we only considered attacks on anchor nodes that can affect a whole network's information transmission. Specifically, an anchor node destroyed by belligerents may report incorrect measurement information, causing the estimated location of the ordinary node to be inaccurate. In the simulation, we can model the attack as the influence on a parameter in the algorithm that can affect the accuracy of the result. This is because modifying any other parameter can be converted into an equivalent value modification. The specific modeling of intentional attacks is proposed in Section 4.1.2.

4. Description of Localization Scheme

Since localization is carried out periodically, our proposed scheme has the following objectives: exclude the nodes affected by the attack to ensure localization accuracy in attack scenarios, improve localization coverage, and reduce average energy consumption. To achieve these goals, the proposed localization scheme comprises the following three phases. Firstly, only anchor nodes were used to locate unknown nodes in the network, and then a list of trusted referable nodes was filtered out for subsequent iterative localization. Secondly, the filtered anchor nodes that may be attacked conducted self-detection with a threshold. Finally, the location of anchor nodes was adjusted periodically to achieve higher localization coverage and less energy consumption in the following cycles with the underwater data center's assistance. The overall flow chart of the ASAL scheme is shown in Figure 2.

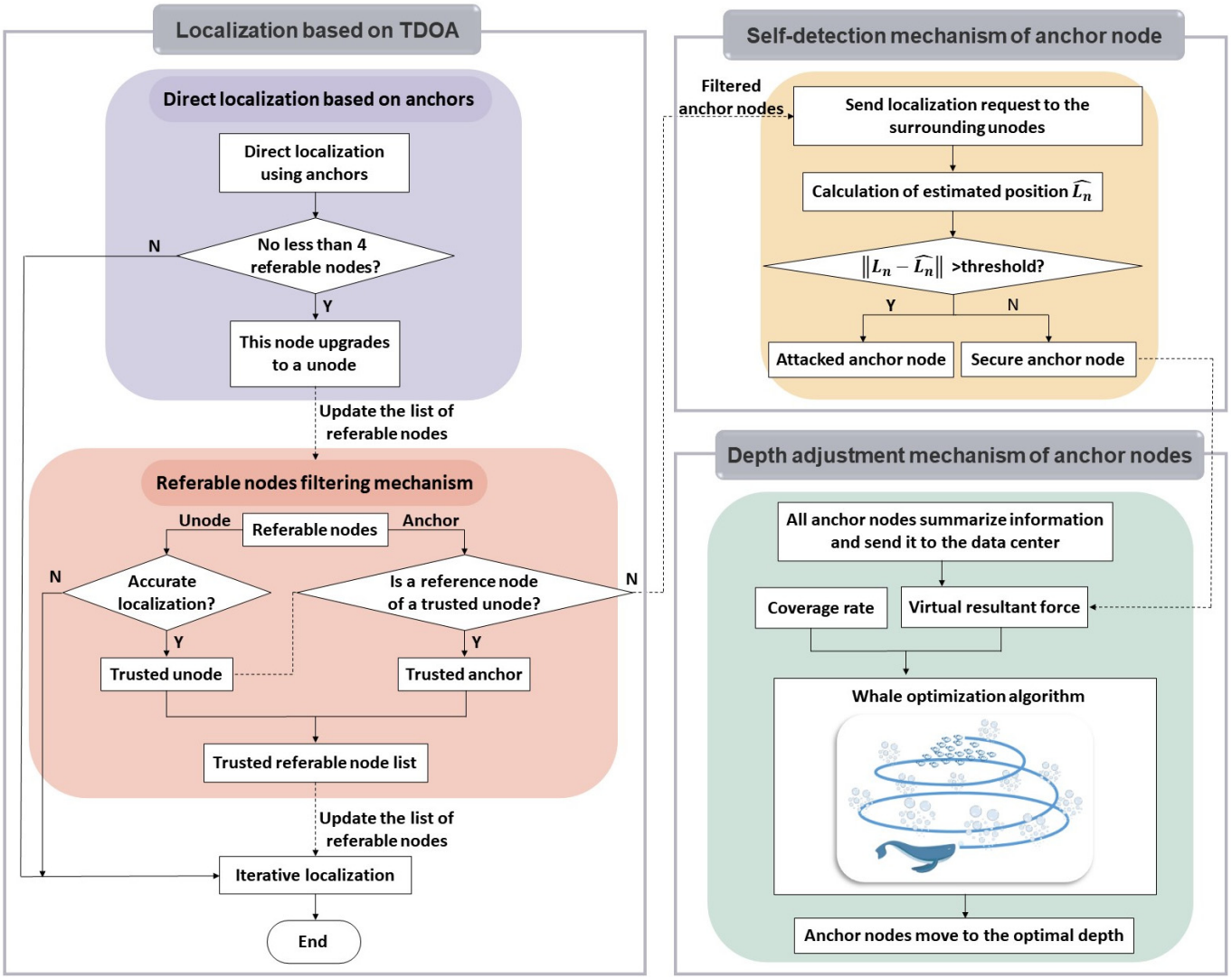

Figure 2. Overall flowchart of the ASAL scheme.

4.1. Localization Based on TDoA

4.1.1. Overview of TDoA Localization

TDoA is a hyperbolic localization method based on time difference. In our algorithm, two-way message exchange estimated the propagation delay sent by the unknown nodes to two reference nodes. At time $t = T_0$, the unknown node sends a ranging request data packet. Then, the two reference nodes send an acknowledgment packet back to the unknown node after receiving this data packet, which contains the location information of the two reference nodes. Meanwhile, it is assumed that the unknown node receives the acknowledgment packets from the two reference nodes at times $t_1^{arrival} = T_1$ and $t_2^{arrival} = T_2$, respectively. T_0, T_1, and T_2 are all measured by the unknown node's local clock. Therefore, the time difference between sending and receiving information by unknown nodes is expressed as follows:

$$\begin{cases} T_1 - T_0 = t_1^{forward} + t_1^{back} + \delta \\ T_2 - T_0 = t_2^{forward} + t_2^{back} + \delta \end{cases} \quad (1)$$

where $t_1^{forward}$ is the time sending information from the nodes unknown to the reference, t_1^{back} is the time sending back, and δ is the clock drift. Then, the unknown node can estimate

the propagation delay as $\Delta t_{1,2} = \left|\frac{T_1 - T_2}{2}\right|$ and multiply the arrival time difference with the sound speed to obtain the propagation distance difference $R_{ref,1} = v * \Delta t_{ref,1}$.

Let the location of the unknown node $Node_i$ be (x_i, y_i, z_i) and the coordinates of the reference node $Rnode_{ref}$ be $\left(X_{ref}, Y_{ref}, Z_{ref}\right)$, ref= 1,2,3,4, where $Rnode_1$ is the confidence node and z_i and Z_{ref} are known. Then, the distance from each reference node to the unknown node is recorded as follows:

$$R_{ref,i} = \sqrt{\left(X_{ref} - x_i\right)^2 + \left(Y_{ref} - y_i\right)^2 + \left(Z_{ref} - z_i\right)^2} \tag{2}$$

when the signals' propagation difference arriving at two anchor nodes is constant, a hyperbola with the reference node as the focus and the distance difference as the long axis can be made. The intersection of multiple hyperbolas is the node's location. Then, the hyperbolic equations are as follows:

$$\begin{cases} \sqrt{(X_2 - x_i)^2 + (Y_2 - y_i)^2 + (Z_2 - z_i)^2} - \sqrt{(X_1 - x_i)^2 + (Y_1 - y_i)^2 + (Z_1 - z_i)^2} = R_{2,1} \\ \sqrt{(X_3 - x_i)^2 + (Y_3 - y_i)^2 + (Z_3 - z_i)^2} - \sqrt{(X_1 - x_i)^2 + (Y_1 - y_i)^2 + (Z_1 - z_i)^2} = R_{3,1} \\ \sqrt{(X_4 - x_i)^2 + (Y_4 - y_i)^2 + (Z_4 - z_i)^2} - \sqrt{(X_1 - x_i)^2 + (Y_1 - y_i)^2 + (Z_1 - z_i)^2} = R_{4,1} \end{cases} \tag{3}$$

Chan's method is used to solve the problem, and the specific steps are as follows:

$$\begin{aligned} R_{ref,1}^2 = &\left(X_{ref} - x_i\right)^2 + \left(Y_{ref} - y_i\right)^2 + \left(Z_{ref} - z_i\right)^2 \\ &- \left[(X_1 - x_i)^2 + (Y_1 - y_i)^2 + (Z_1 - z_i)^2\right] \end{aligned} \tag{4}$$

Let $X_{i,ref} = x_i - X_{ref}, Y_{i,ref} = y_i - Y_{ref}, Z_{i,ref} = z_i - Z_{ref}$, then we can obtain:

$$R_{ref,1}^2 = 2\left[X_{i,ref} \| Y_{i,ref} \| Y_{i,ref}\right] \begin{bmatrix} x_i \\ y_i \\ z_i \end{bmatrix} + K_{ref} - K_1 \tag{5}$$

where $K_{ref} = X_{ref}^2 + Y_{ref}^2 + Z_{ref}^2$, $K_1 = X_1^2 + Y_1^2 + Z_1^2$. The location of the node to be located is as follows:

$$\begin{bmatrix} x_i \\ y_i \\ z_i \end{bmatrix} = -\begin{bmatrix} X_{i,2} \| Y_{i,2} \| Z_{i,2} \\ X_{i,3} \| Y_{i,3} \| Z_{i,3} \\ X_{i,4} \| Y_{i,4} \| Z_{i,4} \end{bmatrix} * \left\{ \begin{bmatrix} R_{2,1} \\ R_{3,1} \\ R_{4,1} \end{bmatrix} R_1 + \frac{1}{2} \begin{bmatrix} R_{3,1}^2 - K_2 - K_1 \\ R_{3,1}^2 - K_3 - K_1 \\ R_{3,1}^2 - K_4 - K_1 \end{bmatrix} \right\} \tag{6}$$

4.1.2. Intentional Attack Model

A method similar to the uncoordinated attacks in [38] was used for intentional underwater attacks. In the three-dimensional environment, supposing that there is a set of measurement values $\left\{\left(P_1, P_{ref}, R_{ref,1}\right) ref = 2,3,4\right\}$, where P_1 and P_{ref} are the coordinates of $Rnode_1$ and $Rnode_{ref}$, respectively, and $R_{ref,1}$ is the distance difference between them. The unknown node's estimated location $\hat{P}_i = [\hat{x}_i, \hat{y}_i, \hat{z}_i]^T$ can be obtained by solving the following equation:

$$\| P_1 - \hat{P}_i \| - \| P_{ref} - \hat{P}_i \| - R_{ref,1} = 0, ref = 2,3,4 \tag{7}$$

In the TDoA scenario, an opponent is interfering with the distance difference reported to the unknown node to prevent accurate localization. Specifically, the attack is modeled by adding an independent and evenly distributed disturbance to the distance difference provided by each attacked anchor node. Without losing generality, assuming that every anchor node attacked by malicious nodes modifies the distance difference. This is because modifying any other parameter can be converted into an equivalent value modification.

Therefore, the localization process with the anchor node will have an unreal distance difference, leading to localization failure.

Let the distance difference between the unknown node and two reference nodes be $R_{ref,1} = \| P_1 - \hat{P}_i \| - \| P_{ref} - \hat{P}_i \|$. Then, $R_{ref,1}^{attack}$ affected by the attack is defined as follows:

$$R_{ref,1}^{attack} = \begin{cases} \Delta d_{ref,1} + u_{ref,1} + n_{ref,1}, \| \| & \text{if } Rnode_1 \text{ or } Rnode_{ref} \text{ is malicious} \\ \Delta d_{ref,1} + n_{ref,1}, \| \| & \text{otherwise} \end{cases} \tag{8}$$

where $u_{ref,1}$ is an independent zero-mean uniform random variable, its variance σ^2_{attack} models the disturbance introduced by the attack, and $n_{ref,1}$ is an independent Gaussian $\mathcal{N}(0, \sigma^2)$ variable, representing the measurement noise. Furthermore, the unknown nodes receive the measured values of the reference nodes $\left\{ \left(P_1, P_{ref}, R_{ref,1}^{attack} \right) ref = 2, 3, 4 \right\}$, and use this information to determine their location.

4.1.3. Secure Localization Algorithm

The proposed localization algorithm was divided into three stages. In the first stage, only anchor nodes were used to locate ordinary nodes in unknown locations. Due to the limited referable nodes, many unknown nodes remained after localization was completed. In the second stage, the list of trusted referable nodes was filtered out. In the third stage, the iterative localization method was used to locate the remaining unknown nodes.

A. Direct localization based on anchor

In the initial localization stage, only the location information of anchor nodes in the network is known. Unknown nodes can only use the anchor nodes that should communicate with them as reference nodes to estimate their location. After obtaining the location information, ordinary nodes are upgraded to u-nodes, which are qualified to reply to the following messages to the unknown nodes that send localization requests to them. The content of the information is shown in Figure 3.

ID	Position coordinates	ID of the four reference nodes	Upgrade flag

Figure 3. Message format replied to by u-nodes.

At this stage, only the anchor node can be used as a reference node and the localization coverage is low. Furthermore, the localization accuracy of all upgraded nodes is only related to the anchor node. U-nodes and anchor nodes participate in the next iterative localization. If u-nodes and attacked anchor nodes with large location errors are not eliminated in time, the localization error will be enlarged, generation by generation, in the iterative process, leading to network localization failure. To avoid this situation, we introduced a referable node filtering mechanism.

B. Referable nodes filtering mechanism

According to Section 4.1.2, the anchor node may be attacked, which may cause the unknown node to obtain the wrong distance difference between the two reference nodes and become a u-node with inaccurate localization. However, since the upgrade node will not be attacked, there will be no error in the arrival time of the information sent out to the anchor node after its localization. Hence, the error of distance difference between $Node_i$ and $Anchor_n$ is defined as follows:

$$L_{i,n}^{err} = v * t_{i,n}^{real} - \left\| \hat{P}_i - L_n \right\| \tag{9}$$

when $L_{i,n}^{err}$ is greater than the threshold, the node is considered to have failed in localization and is downgraded to a node, which needs to be relocated. On the contrary, it becomes a confidence u-node.

In addition to filtering u-nodes in reference nodes, the attacked anchor also needs to be filtered out. Ordinary nodes that still maintain the identity of the u-node have high

localization accuracy and are considered to be successful in localization. Because only the anchor node participates in localization at this stage, the localization accuracy of the node is only related to the anchor node. Therefore, when an anchor node appears in the reference node list used in a certain trusted u-node localization, it becomes a trusted anchor node and participates in the next localization. Otherwise, it no longer participates in localization.

The trusted u-node and the trusted anchor filtered by these two parts form a list of trusted referable nodes. Furthermore, the nearest referable nodes are selected as the reference nodes first to complete the localization of unknown nodes that need to be located.

C. Iterative localization based on trusted referable nodes

At this stage, the iterative localization method was used to locate the remaining unknown nodes. It is the same as the first stage localization process. However, as shown in Figure 4, they were directly upgraded to u-nodes to participate in the localization of the remaining nodes after the localization is completed, without detection and filtering. This is because the reference nodes used in the next unknown node localization are all credible.

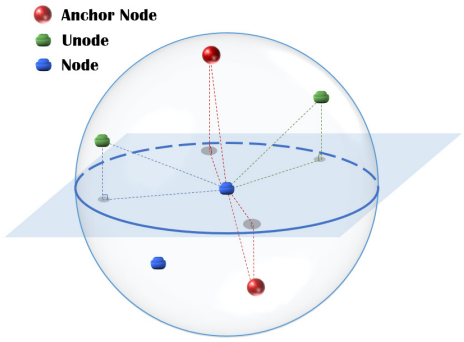

Figure 4. Localization based on trusted referable nodes.

After the three stages, all unknown nodes know their location information and are upgraded to u-nodes.

4.2. Self-Detection Mechanism of the Anchor Nodes

In part B of Section 4.1.2, the basis of filtering the trusted anchor is determining whether or not it is a reference node of a trusted u-node, which may cause the anchor node that has not been attacked to be missed and unable to participate in the next localization, wasting limited high-quality computing resources.

In the localization stage, the attacked anchor node's influence is excluded, and the u-node can obtain a more accurate location. Hence, the excluded anchor nodes utilize the surrounding u-nodes' self-detection to judge whether it is attacked. They send a localization request to the four nearest u-nodes, and if the anchor is really attacked, $R_{ref,1}$ will deviate, leading to a difference between the estimated and real locations, as shown in Figure 5:

$$\| P_1 - \hat{L_n} \| - \| P_{ref} - \hat{L_n} \| = R_{ref,1} \tag{10}$$

If the location error $Err_n = \| L_n - \hat{L_n} \|$ is greater than the threshold, the anchor node will confirm that it has been attacked and will not participate in network localization in the next cycle. However, it will still carry out self-detection, and the anchor node whose localization error is less than the threshold will regain its qualification to participate in localization after the whole network localization is completed in the next cycle.

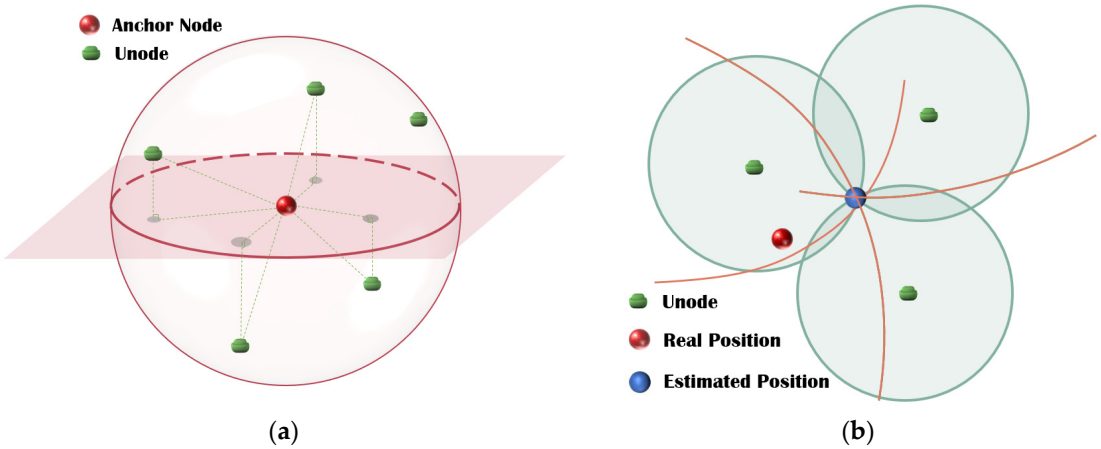

Figure 5. Self-detection of the anchor node. (**a**) Localization of the anchor node using surrounding u-nodes; (**b**) the difference between the estimated location and the real location.

4.3. Depth-Adjustment Mechanism of Anchor Nodes

With time, unbalanced residual energy will appear in the network. For ordinary nodes with low residual energy, we hope to make them closer to the anchor nodes. In addition, we also hope to cover more ordinary nodes within the communication radius of anchor nodes. Therefore, the trusted anchor nodes' depth was adjusted with the assistance of underwater cables and the data center.

4.3.1. Depth-Adjustment Mechanism

The set of ordinary nodes within the communication radius of each anchor node was recorded as $N_n = \{node_1, node_i, \cdots\}$, and the anchor nodes transmitted the location information and residual energy of these nodes to the submarine data center through underwater cables. After collecting the data of all anchor nodes, the data center calculated the number of times that different anchor nodes covered each ordinary node. Furthermore, the more times a node was covered by anchor nodes, the better. The number of times a node should be covered is as follows:

$$\hat{count} = \frac{\sum_{i=1}^{j} count_i}{j} \tag{11}$$

To synthesize the influence of all ordinary nodes within the communication radius of the anchor node and find the optimal depth, the "virtual force vector" was introduced to describe the cost of depth adjustment.

The vector size between $Node_i$ and $Anchor_n$ is as follows:

$$F_i = \alpha * \frac{E_{in}}{E_{res}} + \beta * \frac{1}{Z_n - z_i} \tag{12}$$

where E_{in} and E_{res}, respectively, represent the initial energy and residual energy of the ordinary node pointed by this force vector, and α and β are adjustment factors, where $\alpha + \beta = 1$. All the vectors within the communication range of the anchor node were synthesized, and the component of the synthesized force in the vertical direction was taken as the resultant force, as shown by the orange vector in Figure 6.

The orientation is positive, and the vertical component of each "virtual force vector" is calculated as follows:

$$F_{niv} = sym * F_i * \frac{|Z_n - z_i|}{\left\| P_n - \hat{L}_i \right\|} \tag{13}$$

when $Z_n > z_i$, sym takes -1; when $Z_n < z_i$, sym takes 1. P_n is the location of the anchor node. Therefore, the resultant force $Anchor_n$ receives $F_n^{node} = \sum F_{iv}$. When the depth of the

anchor node changes, the ordinary node within its communication radius will change, or the location of the ordinary node relative to the anchor node will change, which may lead to a change in the magnitude and direction of the resultant force. Therefore, every point on the vertical line where the anchor node is located corresponds to a resultant force, as shown in Figure 7.

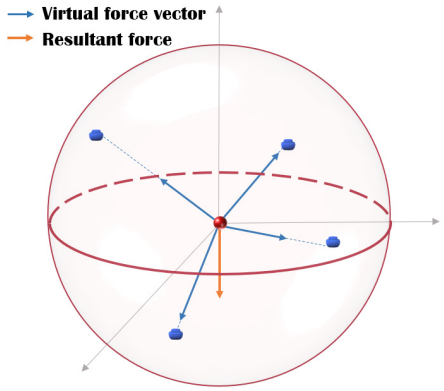

Figure 6. Virtual force vector.

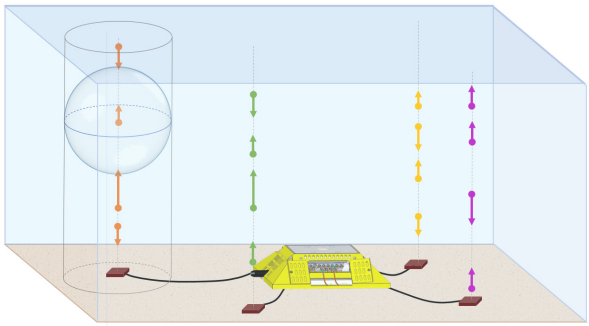

Figure 7. Resultant force in the vertical direction of anchor nodes.

The problem of finding the optimal depth can be described as an optimization problem. Therefore, the whale optimization algorithm (WOA) is used to solve it, and the objective function used in the algorithm is as follows:

$$F_n(h_n) = k * F_n^{node} + l * \hat{count} \tag{14}$$

Both F_n^{node} and $\hat{count}$ will change with the change in $Anchor_n$'s depth and both can be fitted as functions of depth, and k and l are adjustment factors, where $k + l = 1$.

4.3.2. Whale Optimization Algorithm

The WOA is a new swarm intelligence optimization algorithm that imitates the predatory behavior of whales in nature [39], which is mainly divided into the following three categories:

A. Encircling prey

The best whale location is $\vec{X}^*(t)$, and the individual whale location is $\vec{X}(t)$. Then, the formula for calculating the next location of whale individual X under the influence of the best whale X^* is $\vec{X}(t+1)$. The formula of $\vec{X}(t+1)$ is as follows:

$$\vec{D} = \left| \vec{C} \cdot \vec{X}^*(t) - \vec{X}(t) \right| \tag{15}$$

$$\vec{X}(t+1) = \vec{X^*}(t) - \vec{A} \cdot \vec{D} \tag{16}$$

$$\vec{A} = 2\vec{a} \cdot \vec{r} - \vec{a} \tag{17}$$

$$\vec{C} = 2 \cdot \vec{r} \tag{18}$$

where $\vec{a}$ is linearly decreased from 2 to 0 throughout iterations (in both exploration and exploitation phases), $\vec{r}$ is a random vector in [0,1], and $\vec{A}$ and $\vec{C}$ are coefficient vectors.

B. Bubble-net attacking method

Bubble-net attack is a unique bubble-spitting predation behavior of humpback whales. Two mathematical models are used to express this predation behavior as follows:

a. Shrinking encircling mechanism

This predation behavior is almost identical to the above mathematical encircling prey behavior model, but the range of $\vec{A}$ is adjusted from the original $[-a, a]$ to $[-1,1]$.

b. Spiral updating location

An individual whale approaches the current best individual whale in a spiral way:

$$\vec{X}(t+1) = \vec{D'} \cdot e^{bl} \cdot \cos(2\pi l) + \vec{X^*}(t) \tag{19}$$

$$\vec{D'} = \left| \vec{X^*}(t) - \vec{X}(t) \right| \tag{20}$$

where b is a logarithmic spiral shape constant, and l is a random number in $[-1,1]$. When hunting prey, each humpback whale decides to perform shrink encirclement or swim to the prey in a spiral form with a probability of 50%. The mathematical model is as follows:

$$\vec{X}(t+1) = \begin{cases} \vec{X^*}(t) - \vec{A} \cdot \vec{D} \| \| & \text{if} p < 0.5 \\ \vec{D'} \cdot e^{bl} \cdot cos(2\pi l) + \vec{X^*}(t) \| \| & \text{if} p \geq 0.5 \end{cases} \tag{21}$$

where p is a random number in [0,1]. In addition to the bubble-net method, humpback whales search for prey randomly. The mathematical model of the search is as follows.

C. Search for prey

In the mathematical model of predation behavior surrounded by contraction, the value range of the $\vec{A}$ vector is limited to $[-1,1]$. While the value of $\vec{A}$ is not $[-1,1]$, the current individual whale may not approach the current best individual whale, but randomly select an individual whale from the current whale population to approach, which is the idea of searching for prey. Although searching for prey may make the current individual whale deviate from the target prey, it will enhance the global search ability of the whale population. The mathematical model of searching for prey is as follows:

$$\vec{D} = \left| \vec{C} \cdot \vec{X_{\text{rand}}} - \vec{X} \right| \tag{22}$$

$$\vec{X}(t+1) = \vec{X_{\text{rand}}} - \vec{A} \cdot \vec{D} \tag{23}$$

where $\vec{X_{\text{rand}}}$ is a random location vector (a random whale) chosen from the current population.

The depth-adjustment mechanism's pseudo-code is detailed in Algorithm 1.

Algorithm 1 Depth-Adjustment Algorithm

Input: Residual energy E_{res} and location coordinate $\hat{L}_i$ of the ordinary node. Location coordinates P_n of trusted anchor node.

Output: Optimal depth h_n^* of the anchor node

```
Initialize the whales population
Calculate the resultant force F_n^node and anchor node coverage côunt
Calculate the fitness of each search agent by the Equation (14)
h_n^* = the best search agent
while (t < maximum number of iterations) do
    for each search agent do
        Update a, A, C, l, and p
        Select search behavior
        Update the location of the current search
    end for
    Calculate the fitness of each search agent
    Update h_n^* if there is a better solution
    t = t + 1
end while
return h_n^*
```

5. Simulation Results

5.1. Simulation Settings

In the network scenario of the proposed scheme, 50 sensor nodes were arranged in an area of 500 m × 500 m × 500 m. We compared ASAL to 3DUL [40], which uses three beacons on the water surface and performs iterative localization, and TDoA [41], which is the basic localization algorithm of ASAL. In addition, by comparing different simulation results, we assumed that $\alpha = 0.7$, $\beta = 0.3$, $k = 0.4$, and $l = 0.6$. In Table 1, some related parameter settings are shown.

Table 1. System symbols.

Parameter	Value
Number of sensor nodes	50
Ratio of anchor nodes	20%
Simulation area	500 m × 500 m × 500 m
Transmission range	100 m ≤ R ≤ 300 m
Unit energy consumption	5
Initial energy	30,000

5.2. Results Analysis

5.2.1. Localization Coverage Changes with Communication Radius

In Figure 8a, the coverage rate is shown to have increased with the increase in the communication radius, and ASAL had higher coverage than 3DUL. The average localization coverage of 3DUL was 48.38%, and that of ASAL with 10% anchors, ASAL with 20% anchors, and ASAL with 30% anchors was 61.6%, 69.85%, and 73.22%, respectively. In ASAL, higher proportions of anchor nodes correspond to higher location coverage, which is because the direct localization rate of anchor nodes increases. In Figure 8b, we can see that when the communication radius was the same, smaller thresholds corresponded to smaller corresponding coverage. This is because smaller thresholds cause harsher conditions for filtering the trusted reference nodes. The three curves with thresholds of 0.5, 1, and 10 and the two curves with thresholds of 0.05 and 0.1 were relatively close because the points filtered by them were not very different. Therefore, ASAL can obtain a higher node location rate by increasing the anchor node ratio, threshold, and communication radius.

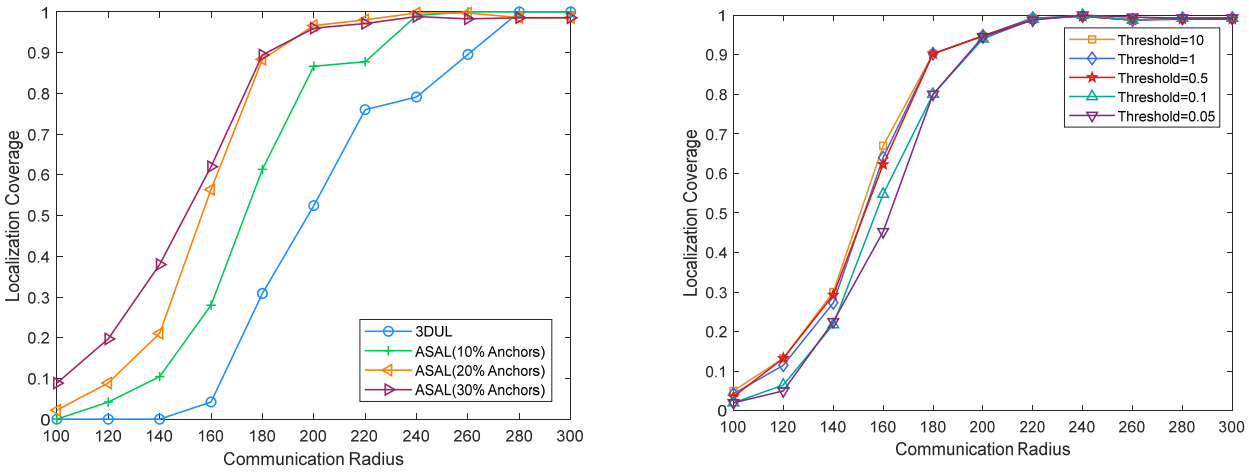

Figure 8. Localization coverage changes with communication radius. (**a**) ASAL comparison between 3DUL and different anchor node ratios; (**b**) comparison between different thresholds of ASAL.

5.2.2. Localization Coverage Changes with the Ratio of Malicious Nodes under Different Thresholds

Figure 9 shows that with the increase in the malicious node ratio, the coverage of node localization decreased. The ratio of malicious nodes increased, that is, the number of attacked anchor nodes increased, which led to an increased effect on the u-node after direct localization was completed. More referable nodes were filtered out. When the ratio of malicious nodes was the same, the threshold decreased, and the localization coverage decreased. This is because smaller thresholds correspond to harsher conditions for filtering the trusted reference nodes.

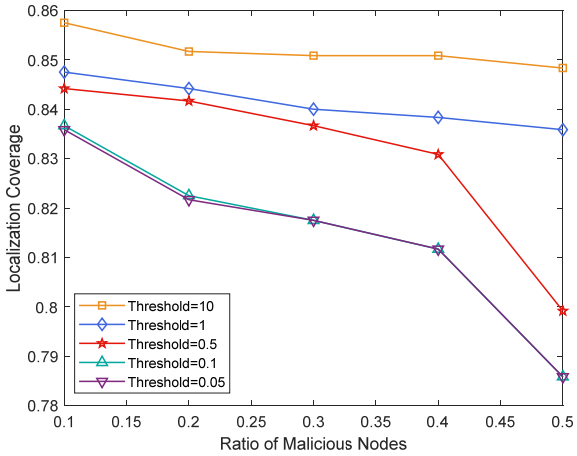

Figure 9. Localization coverage changes with the ratio of malicious nodes under different thresholds.

5.2.3. Localization Error Changes with Attack Intensity

In Figure 10, the localization error is shown to have increased with the increase in attack intensity. The error sources of ASAL were mainly affected by attacks and the increase in iteration times. When the threshold was 0.1, all the nodes affected by the attack were filtered out, and the error was close to zero. When the threshold was 10, the error did not always rise. When the attack intensity was low, many nodes affected by the attack were not filtered out, and there were more referable nodes than ASAL with a threshold of 0.1 and less than TDoA, which led to greater errors caused by the attack than ASAL with a threshold of 0.1 and greater errors caused according to iteration times than TDoA. When

the attack intensity was further increased from 5 to 7, the direct error caused by the attack increased, which made it easier to filter out than before, thus gradually eliminating the influence of the attack and rapidly decreasing the error. Additionally, the error caused by the increase in iteration times assumed the main location and slowly rose when the attack intensity was greater than 7. When comparing ASAL with 3DUL and TDoA, the average localization error decreased by about 99.82% and 98.25%, respectively.

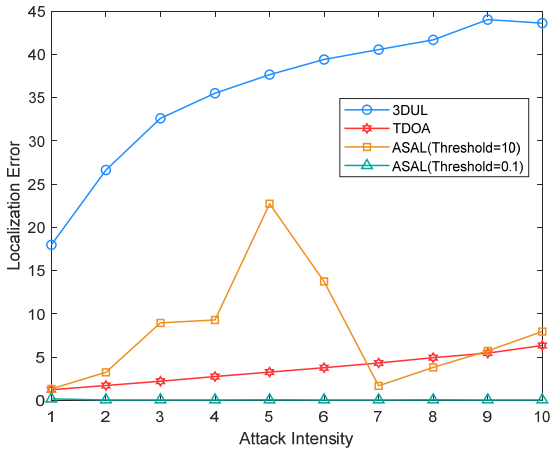

Figure 10. Localization error changes with attack intensity.

5.2.4. Localization Error Changes with the Ratio of Malicious Nodes

In Figure 11, there may be one, two, or three anchor nodes attacked in 3DUL, and the error was obviously higher than in other cases due to the large number of iterations. TDoA did not filter out malicious nodes, and the error increased slowly with the increase in the attack node ratio. For ASAL, almost all malicious nodes were filtered out when the threshold was 0.1, and the error curve rose rapidly as many nodes affected by the attack were not filtered out when the threshold was 10. Similar to the analysis in Figure 10, its error was larger than ASAL with a threshold of 0.1 and TDoA. The average localization error decreased by about 99.82% and 98.59% when compared ASAL with 3DUL and TDoA, respectively.

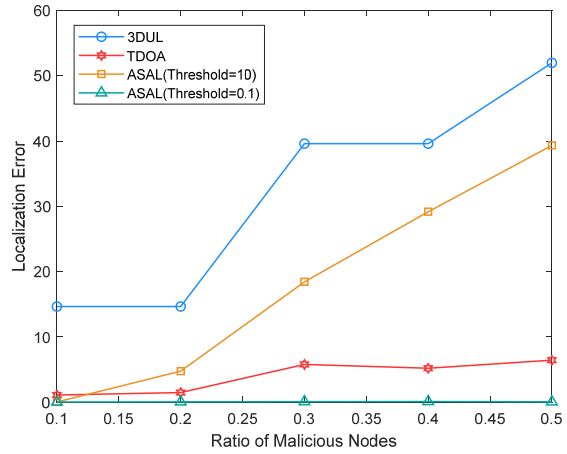

Figure 11. Localization error changes with the ratio of malicious nodes.

5.2.5. Localization Error Changes with Communication Radius under Different Thresholds

In Figure 12, errors with thresholds of 0.5, 0.1, and 0.05 are shown to have all been close to zero, and most malicious nodes were filtered out. However, the ASAL error with thresholds of 10 and 1 was relatively large. These two curves can be divided into three

stages. Firstly, the communication radius of nodes was small, and the localization coverage was low. Then, with the increase in communication radius, the coverage rate increased. However, due to the large threshold, the error caused by the attack could not be filtered out. After that, as the communication radius continued to increase, the anchor node directly located more nodes, the number of iterations decreased, and the error gradually decreased.

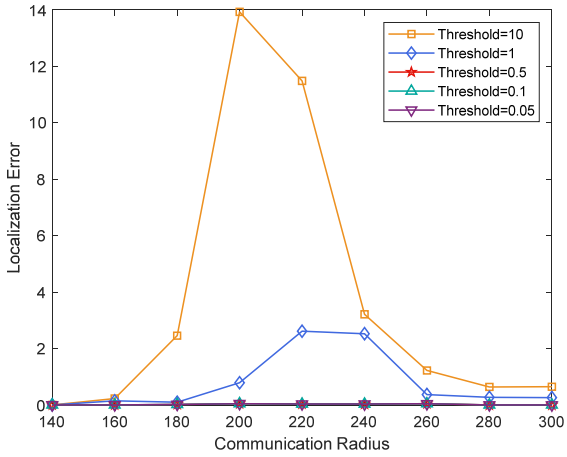

Figure 12. Localization error changes with communication radius under different thresholds.

5.2.6. Evaluation of Performance Metrics between Cycles with Radar Graph (Localization Error, Localization Coverage, Energy Consumption)

In each cycle of ASAL, localization was performed first, and then depth adjustment was performed. As shown in Figure 13, TDoA had the highest localization coverage, but the localization error and energy consumption were also the largest. Because TDoA did not filter out the nodes affected by the attack and there were many referable nodes, the error was large, but the localization coverage rate was also higher than that of ASAL. Since the nodes affected by the attack were filtered out, there was little difference in the localization error between the two cycles of ASAL. However, the average energy consumption in the second cycle of ASAL was smaller than that in the first cycle because the adjustment of anchor node depth led to the optimization of the network structure, which in turn led to the reduction in energy consumption. The depth-adjustment mechanism is therefore feasible. From the results, regarding TDoA as a baseline, the localization error of ASAL decreased by about 92.67%. After the adjustment of anchor node depth, the localization coverage of ASAL attained a 4.37% increase and a 12.28% decrease in energy consumption.

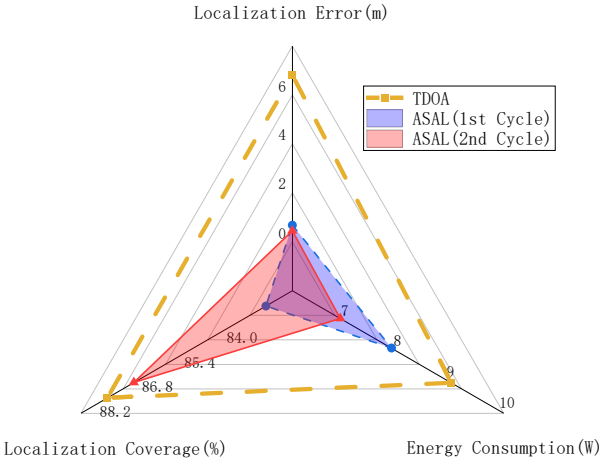

Figure 13. Evaluation of performance metrics between cycles with radar graph (localization error, localization coverage, energy consumption).

5.2.7. Motion Trajectory Tracking

Figure 14 shows the underwater trajectory tracking based on ASAL. The blue line represents the actual three-dimensional motion trajectory, and the red marker points are the estimated locations of trajectory tracking, so most locations can be accurately located.

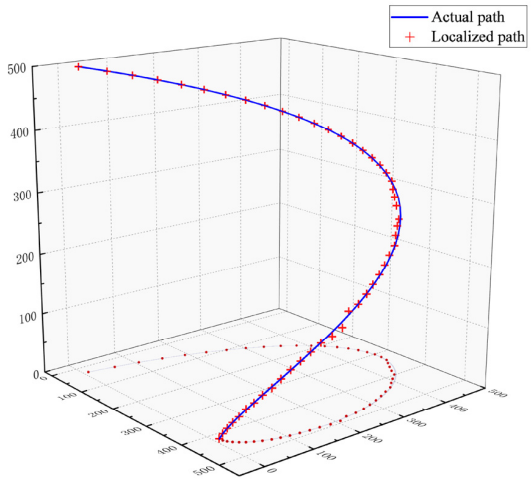

Figure 14. Motion trajectory tracking.

5.2.8. Finding the Optimal Depth with the WOA

In this stage, an optimization method combined with the WOA was proposed for the depth-adjustment strategy. Each depth had corresponding $\frac{E_{in}}{E_{res}}$, $\hat{count}$ and $Z_n - Z_i$. Then, the virtual force vector corresponding to each depth could be calculated for adjustable anchor nodes. Therefore, these variables were discretely distributed in three-dimensional space. The WOA was used to find the optimal value in these discrete points. We express it in the form of slices in three-dimensional space, and the intersection of slices is one of the feasible solutions. The size of the virtual force vector changed with color, as shown on the right of Figure 15a. We hope that the anchor node can move to a depth where the resultant force vector is minimal. Figure 15b shows the iterative process of the WOA, and the optimal force vector value is demonstrated. The number of iterations was from 1 to 6, and the value of the force vector decreased continuously. When the iteration value was 6, the value of the force vector decreased to about 0.33 and then remained stable.

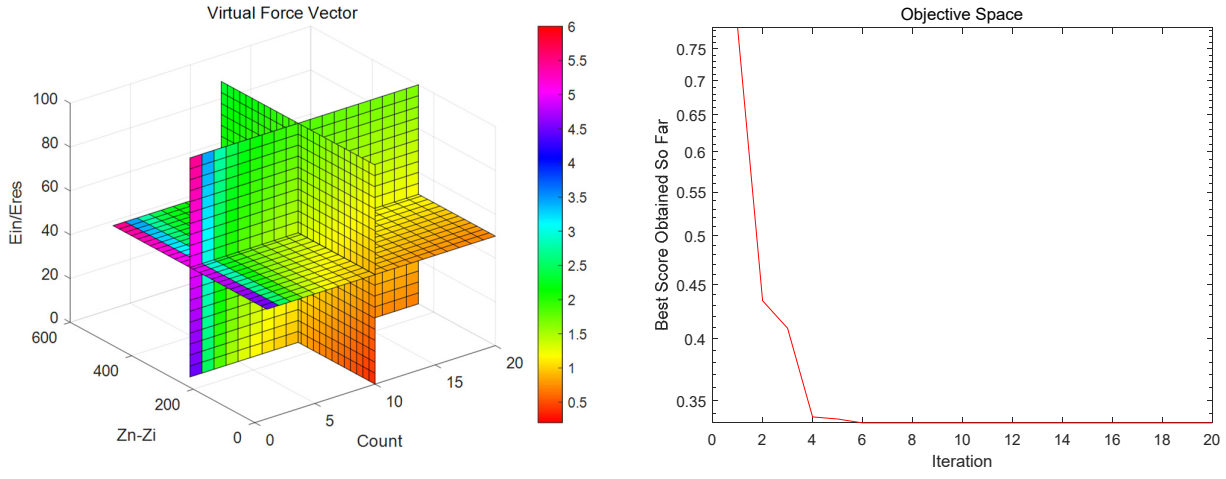

Figure 15. Finding the optimal depth with the WOA. (**a**) Slice of force vector function in three-dimensional space; (**b**) iterative curve of the algorithm.

6. Conclusions

This article proposed a localization scheme, ASAL, to deal with attacks in UASNs. In UASNs, accurate node localization is crucial. In attack scenarios such as equipment destruction, signal interference, and node deception, the node location information may be inaccurate, which affects the reliability and efficiency of the network.

To resist the attack, a referable node was selected for iterative localization after direct localization based on anchor nodes. After the localization was completed, the filtered anchor node utilized the ordinary nodes around it to locate reversely and judged whether it was attacked to adjust the state of participating in the localization in the next cycle. In addition, we optimized the network structure through a depth-adjustment strategy of anchor nodes, introduced a virtual force vector to describe the cost of depth adjustment, and used the WOA to converge to the depth with the minimum total cost. Compared to 3DUL and TDoA, the simulation results of ASAL showed that it achieved better localization accuracy and coverage and less energy consumption in attack scenarios. In addition, we also proved that ASAL can be used to track mobile nodes with small localization errors in attack scenarios.

ASAL still has some limitations, such as not verifying more attack types. In future work, we will optimize the referable node selection scheme based on its contribution to adapt to more complex underwater attack scenarios. In addition, we will carry out verification of ASAL in real underwater scenarios.

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

Funding: This work has been funded by the National Natural Science Foundation of China, grant number (52171337), and the Natural Science Foundation of Hainan Province, grant number (RZ2100000416, SQ2024MSXM0152), and supported in part by the key project of Hainan Province under the grant (ZDYF2020199).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The code of this article is available at https://github.com/XiaoMapleLeaf/Code_on_ASAL.git (accessed on 1 May 2023).

Acknowledgments: The authors would like to thank the anonymous reviewers for their careful reading and valuable comments.

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

References

1. Badawy, M.; Khater, E.; Tolba, M.; Ibrahim, D.M.; El-Fishawy, N.A. A New Technique for Underwater Acoustic Wireless Sensor Network. In Proceedings of the 2020 15th International Conference on Computer Engineering and Systems, Cairo, Egypt, 15–16 December 2020; pp. 1–5.
2. Agajo, J.; Adewale, A.L.; Idama, E.O.; Prudence, E.E.; Felix, E. A Conceptualized Model for Data Transmission in Underwater Acoustic Wireless Sensor Network. *Appl. Model. Simul.* **2020**, *4*, 40–46.
3. Gomathi, R.M.; Manickam, J.M.L. Energy Efficient Static Node Selection in Underwater Acoustic Wireless Sensor Network. *Wirel. Pers. Commun.* **2019**, *107*, 709–727. [CrossRef]
4. Llor, J.; Malumbres, M.P. Statistical Modeling of Large-Scale Signal Path Loss in Underwater Acoustic Networks. *Sensors* **2013**, *13*, 2279–2294. [CrossRef] [PubMed]
5. Barber, C.; Becker, K.M. Issues for improved characterization of the acoustic field due to radiated noise of ships in shallow water environments. *J. Acoust. Soc. Am.* **2004**, *116*, 2649. [CrossRef]
6. Tu, X.; Xu, X.; Song, A. Statistical analysis and hybrid modeling of high-frequency underwater acoustic channels affected by wind-driven surface waves. *J. Acoust. Soc. Am.* **2022**, *151*, 3266. [CrossRef]

7. Misra, S.; Ojha, T.; Mondal, A. Game-Theoretic Topology Controlfor Opportunistic Localization in Sparse Underwater Sensor Networks. *IEEE Trans. Mob. Comput.* **2015**, *14*, 990–1003. [CrossRef]
8. Prateek; Arya, R. An underwater localization scheme for sparse sensing acoustic positioning in stratified and perturbed UASNs. *Wirel. Netw.* **2021**, *28*, 241–256.
9. Nain, M.; Goyal, N. Energy Efficient Localization Through Node Mobility and Propagation Delay Prediction in Underwater Wireless Sensor Network. *Wirel. Pers. Commun.* **2021**, *122*, 2667–2685. [CrossRef]
10. Dong, M.; Li, H.; Yin, R.-R.; Qin, Y.; Hu, Y. Scalable asynchronous localization algorithm with mobility prediction for underwater wireless sensor networks. *Chaos Solitons Fractals* **2021**, *143*, 110588. [CrossRef]
11. Aman, W.; Al-Kuwari, S.M.; Kumar, A.; Rahman, M.M.U. Security of Underwater and Air-Water Wireless Communication. *Ad Hoc Networks* **2023**, *142*, 103114. [CrossRef]
12. Aman, W.; Al-Kuwari, S.M.; Kumar, A.; Rahman, M.M.U.; Muzzammil, M. Underwater and Air-Water Wireless Communication: State-of-the-art, Channel Characteristics, Security, and Open Problems. *arXiv* **2022**, arXiv:2203.02667.
13. Verma, P.R.; Kumar, A.; Ranjan, R. An Energy Efficient Localization of the Sensory Nodes based on Secure Routing Protocol for Underwater Network. In Proceedings of the 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON), Kuala Lumpur, Malaysia, 24–26 September 2021; pp. 1–9.
14. Mengchen, X.; Jie, Z.; Dong, Y.; Xin, J. A Layout Strategy for Distributed Barrage Jamming against Underwater Acoustic Sensor Networks. *J. Mar. Sci. Eng.* **2020**, *8*, 252.
15. Vadori, V.; Scalabrin, M.; Guglielmi, A.V.; Badia, L. Jamming in Underwater Sensor Networks as a Bayesian Zero-Sum Game with Position Uncertainty. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6.
16. Li, X.; Zhou, Y.; Yan, L.; Zhao, H.; Yan, X.; Luo, X. Optimal Node Selection for Hybrid Attack in Underwater Acoustic Sensor Networks: A Virtual Expert-Guided Bandit Algorithm. *IEEE Sens. J.* **2020**, *20*, 1679–1687. [CrossRef]
17. Xiao, L.; Jiang, D.; Wan, X.; Su, W.; Tang, Y. Anti-Jamming Underwater Transmission With Mobility and Learning. *IEEE Commun. Lett.* **2018**, *22*, 542–545. [CrossRef]
18. Periola, A.A.; Osanaiye, O.A.; Olusesi, A.T. Future cloud: Spherical processors for realizing low-cost upgrade in underwater data centers. *J. Supercomput.* **2021**, *77*, 7046–7072. [CrossRef]
19. Periola, A.A.; Alonge, A.A.; Ogudo, K.A. Heat Wave Resilient Systems Architecture for Underwater Data Centers. *Sci. Rep.* **2022**, *12*, 17161. [CrossRef]
20. Finn, B. Underwater Cables. *Proc. IEEE* **2013**, *101*, 1253–1259. [CrossRef]
21. Eleftherakis, D.; Vicen-Bueno, R. Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors. *Sensors* **2020**, *20*, 737. [CrossRef]
22. Ma, Z.; Ho, K.C. TOA localization in the presence of random sensor position errors. In Proceedings of the 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Prague, Czech Republic, 22–27 May 2011; pp. 2468–2471.
23. Huang, B.; Xie, L.; Yang, Z. TDOA-Based Source Localization With Distance-Dependent Noises. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 468–480. [CrossRef]
24. Niculescu, D.; Badrinath, B.R. Ad hoc positioning system (APS) using AOA. In Proceedings of the IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), San Francisco, CA, USA, 30 March–3 April 2003; Volume 1733, pp. 1734–1743.
25. Molla, J.P.; Dhabliya, D.; Jondhale, S.R.; Arumugam, S.S.; Rajawat, A.S.; Goyal, S.B.; Răboacă, M.S.; Mihaltan, T.C.; Verma, C.; Suciu, G. Energy Efficient Received Signal Strength-Based Target Localization and Tracking Using Support Vector Regression. *Energies* **2023**, *16*, 555. [CrossRef]
26. Liang, Q.; Zhang, B.; Zhao, C.; Pi, Y. TDoA for Passive Localization: Underwater versus Terrestrial Environment. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 2100–2108. [CrossRef]
27. Shin, H.; Ku, B.; Nelson, J.K.; Ko, H. Robust Target Tracking with Multi-Static Sensors under Insufficient TDOA Information. *Sensors* **2018**, *18*, 1481. [CrossRef] [PubMed]
28. Hao, K.; Yu, K.; Gong, Z.; Du, X.; Liu, Y.; Zhao, L. An Enhanced AUV- Aided TDoA Localization Algorithm for Underwater Acoustic Sensor Networks. *Mob. Netw. Appl.* **2020**, *25*, 1673–1682. [CrossRef]
29. Erol-Kantarci, M.; Vieira, L.F.M.; Gerla, M. Localization with Dive'N'Rise (DNR) beacons for underwater acoustic sensor networks. In Proceedings of the 2nd Workshop on Underwater Networks, Montreal Quebec Canada, 14 September 2007.
30. Su, Y.; Guo, L.; Jin, Z.; Fu, X. A Mobile-Beacon-Based Iterative Localization Mechanism in Large-Scale Underwater Acoustic Sensor Networks. *IEEE Internet Things J.* **2021**, *8*, 3653–3664. [CrossRef]
31. Han, G.; Liu, L.; Jiang, J.; Shu, L.; Rodrigues, J.J.P.C. A Collaborative Secure Localization Algorithm Based on Trust Model in Underwater Wireless Sensor Networks. *Sensors* **2016**, *16*, 229. [CrossRef]
32. Misra, S.; Ojha, T.; Madhusoodhanan, P. SecRET: Secure Range-based Localization with Evidence Theory for Underwater Sensor Networks. *ACM Trans. Auton. Adapt. Syst.* **2021**, *15*, 1–26. [CrossRef]
33. Shanthi, M.; Anvekar, D.K. Secure Localization for Underwater Wireless Sensor Networks Based on Probabilistic Approach. In Proceedings of the 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC), Bangalore, India, 9–10 February 2018; pp. 1–6.

34. Baranidharan; Varadharajan, K. Secure localization using coordinated gradient descent technique for underwater wireless sensor networks. *ICTACT J. Commun. Technol.* **2018**, *9*, 1716–1720. [CrossRef]
35. Gao, C.; Yan, J.; Luo, X.; Wu, X. Target Localization in Underwater Acoustic Sensor Networks with False Data Attacks. In Proceedings of the 2021 China Automation Congress (CAC), Beijing, China, 22–24 October 2021; pp. 3719–3724.
36. Chen, Y.; Jin, Z.; Zeng, Q.; Yang, Q. A Collision-Avoided MAC Protocol With Time Synchronization and Power Control for Underwater Sensor Networks. *IEEE Sens. J.* **2022**, *22*, 19073–19087. [CrossRef]
37. Garg, R.; Varna, A.L.; Wu, M. An Efficient Gradient Descent Approach to Secure Localization in Resource Constrained Wireless Sensor Networks. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 717–730. [CrossRef]
38. Lv, B.; Liu, H.; Hu, Y.-F.; Wu, C.X.; Liu, J.; He, H.; Chen, J.; Yuan, J.; Zhang, Z.-W.; Cao, L.; et al. Experimental study on integrated and autonomous conductivity-temperature-depth (CTD) sensor applied for underwater glider. *Mar. Georesources Geotechnol.* **2020**, *39*, 1044–1054. [CrossRef]
39. Mirjalili, S.M.; Lewis, A. The Whale Optimization Algorithm. *Adv. Eng. Softw.* **2016**, *95*, 51–67. [CrossRef]
40. Isik, M.T.; Akan, Ö.B. A three dimensional localization algorithm for underwater acoustic sensor networks. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 4457–4463. [CrossRef]
41. Liu, F.; Chen, H.; Zhang, L.; Xie, L. Time-difference-of-arrival-based localization methods of underwater mobile nodes using multiple surface beacons. *IEEE Access* **2021**, *9*, 31712–31725. [CrossRef]