sensors

MDPI

Article

A Collaborative Secure Localization Algorithm Based on Trust Model in Underwater Wireless Sensor Networks

Guangjie Han [1,2,*], Li Liu [1,†], Jinfang Jiang [1,†], Lei Shu [3,†] and Joel J.P.C. Rodrigues [4,†]

1 Department of Information and Communication Systems, Hohai University, 200 North Jinling Road, Changzhou 213022, China; liulihhuc@gmail.com (L.L.); jiangjinfang1989@gmail.com (J.J.)
2 Changzhou Key Laboratory of Sensor Networks and Environmental Sensing, Changzhou 213022, China
3 Guangdong Petrochemical Equipment Fault Diagnosis Key Laboratory, Guangdong University of Petrochemical Technology, Maoming 525000, China; lei.shu@ieee.org
4 Instituto de Telecomunicações, University of Beira Interior, Portugal and University of Fortaleza (UNIFOR), Ceará 60811-905, Brazil; joeljr@ieee.org
* Correspondence: hanguangjie@hhu.edu.cn; Tel.: +86-519-8519-1841; Fax: +86-519-8519-1838
† These authors contributed equally to this work.

Academic Editor: Jaime Lloret Mauri
Received: 14 December 2015; Accepted: 5 February 2016; Published: 16 February 2016

Abstract: Localization is one of the hottest research topics in Underwater Wireless Sensor Networks (UWSNs), since many important applications of UWSNs, e.g., event sensing, target tracking and monitoring, require location information of sensor nodes. Nowadays, a large number of localization algorithms have been proposed for UWSNs. How to improve location accuracy are well studied. However, few of them take location reliability or security into consideration. In this paper, we propose a Collaborative Secure Localization algorithm based on Trust model (CSLT) for UWSNs to ensure location security. Based on the trust model, the secure localization process can be divided into the following five sub-processes: trust evaluation of anchor nodes, initial localization of unknown nodes, trust evaluation of reference nodes, selection of reference node, and secondary localization of unknown node. Simulation results demonstrate that the proposed CSLT algorithm performs better than the compared related works in terms of location security, average localization accuracy and localization ratio.

Keywords: underwater wireless sensor networks; trust evaluation; collaborative secure localization

1. Introduction

Underwater Wireless Sensor Networks (UWSNs) have gained researchers' much attention in the past few years due to their great potential utility in many applications, such as ocean resource exploration, marine environment monitoring, ocean target surveillance, submarine tracking and disaster prevention [1,2]. In these applications, sensor node's accurate and reliable locations are required. In addition, some network system functions, e.g., network topology management and design of network communication protocols, also need sensor nodes' location information to achieve. Thus, the secure localization problem becomes one of the most important and fundamental issues in UWSNs. Many localization algorithms have been proposed for UWSNs [3]. However, few of them take location reliability or security into consideration, while UWSNs are always deployed in unattended and even hostile environment. Ensuring node safety is a basic and essential knowledge to improve node location accuracy and reliability. Therefore, in this paper, we study both node security and localization accuracy in the proposed secure localization algorithm.

A large number of security mechanisms have been proposed to ensure safety of sensor nodes. Traditional mechanisms, e.g., cryptography and authentication, can well resist external attacks, but cannot eliminate insider attacks effectively. In addition, the traditional mechanisms are not energy efficient for energy and resource limited UWSNs. Relatively speaking, trust management has been recently suggested as an innovative and energy efficient security mechanism. Although trust management mechanisms are widely studied in Internet, Aodhoc networks, P2P networks, social networks and Terrestrial Wireless Sensor Networks (TWSNs) for network security [4,5], they cannot be directly applied to UWSNs due to the unique characteristics of underwater environment, e.g., inevitable node movement, variable propagation delay, instable acoustic channel, poor underwater link quality and limited channel bandwidth. These factors mainly impact the success communication rates and the accurate trust assessments of underwater sensor nodes. This highlights the fact that it is critical to design a new trust model for UWSNs considering the unique characteristics of the acoustic communication channel and underwater environment.

In this paper, we propose a Collaborative Secure Localization algorithm based on Trust model (CSLT) for UWSNs. CSLT first uses trust model to ensure node safety and avoid the influence from malicious nodes, which ultimately reduces unknown nodes' localization error and enhances localization accuracy. Then, based on the collaboration of sensor nodes, localization ratio and localization accuracy can be further improved. The proposed CSLT consists of the following five sub-processes: trust evaluation of anchor nodes, initial localization of unknown nodes, trust evaluation of reference nodes, selection of reference node, and secondary localization of unknown node. In the first sub-processes, each anchor node pretends to be an unknown node to ask for localization and evaluate trust for each other. Only trusty anchor nodes can be used to localize unknown nodes. Then, the unknown nodes fail to be localized in the initial localization process can ask for secondary localization. Before the secondary localization, the trust values of reference nodes are calculated based on the cloud theory. Only trusty reference nodes are chosen to further localize the rest of unknown nodes until all the nodes are successfully localized.

The rest of this paper is organized as follows: Section 2 reviews existing related works. Section 3 presents the network model, the assumptions and the overview of CSLT. Section 4 describes the proposed trust model in detail. Section 5 gives a detailed analysis of simulation results. And finally, Section 6 makes a conclusion of this paper and discusses our future research works of secure localization in UWSNs.

2. Related Work

In our previous work [3], the current existing underwater localization algorithms are mainly classified into two categories: (1) stationary localization algorithms and (2) mobile localization algorithms. In this section, we first summarize several typical underwater localization algorithms, and then analyze existing research problems of them.

In stationary localization algorithms, all the sensor nodes are assumed to be static without influence from dynamic underwater environment. For example, in [6], an efficient Area Localization Scheme (ALS) is proposed for UWSNs, where anchor nodes send localization beacons with different energy levels to unknown nodes. The unknown nodes which receive beacons firstly record ID numbers of anchor nodes and the corresponding energy levels, then send the recorded information to sink node. After receiving the information from unknown nodes, the sink node tries to localize unknown nodes according to the corresponding energy level and the locations of anchor nodes. In [7,8], an Underwater Positioning Scheme (UPS) is proposed, which localizes unknown nodes by using 4 non-coplanar anchor nodes in three dimensional UWSNs. UPS does not require time synchronization because it uses TDoA (Time Difference of Arrival) technique to measure distances between sensor nodes. However, the localization delay of UPS is quite long, and the localization coverage is limited by the communication range of sensor nodes. In [9,10], an Underwater Sensor Positioning (USP) scheme is proposed in for sparse three-dimensional UWSNs. In USP, all the

sensor nodes are equipped with pressure sensors, thus they can obtain their own depth positions. Then, based on the projection technique, the three dimensional localization problem can be transformed into its two dimensional counterpart. In order to solve the problem of low localization coverage in large-scare UWSNs, the researchers also put forward many solutions, for example, in [11,12], the strategy of unknown node upgrade is proposed in a Large-Scale Hierarchical Localization (LSHL) approach. That is, the successfully localized unknown nodes can be upgraded as anchor nodes to help neighbor unknown nodes with localization. This strategy can well solve the limited localization coverage problem; however, the main drawback of LSHL is that the location error is accumulated.

In real applications, an absolutely stationary network does not exist. The underwater sensor nodes always freely float with ocean current. Therefore, in many research works, ocean current and sensor mobility are taken into account in localization algorithms. For example, in [13], a Collaborative Localization Scheme (CLS) is proposed for mobile UWSNs, where unknown nodes collaborate with each other to determine their positions autonomously without using any anchor nodes. In addition, in mobile UWSNs, mobile anchor node, e.g., Dive and Rise (DNR) anchor nodes [14,15], Autonomous Underwater Vehicles (AUVs) [16,17], mobile detachable elevator transceiver (DET) [18], are adopted to improve localization performance. DNR anchor nodes and AUV equipments are equipped with GPS. They can first obtain their positions on the ocean surface, then sink into water and broadcast their positions to localize unknown nodes. In order to avoid position change from ocean flow, the anchor nodes periodically rise to the surface to update their position information. Mobile anchor nodes can move not only in the vertical direction, but also in the horizontal plane. For example, in [19], a Range-free scheme based on Mobile Beacons (RSMB) is proposed for UWSNs, where a mobile anchor node moves on the sea surface at a constant speed following the random way-point (RWP) model and broadcasts localization beacons for unknown nodes. The unknown nodes localize themselves based on the projection technique. In [20,21], a novel Underwater localization approach based on Directional Beacons (UDB) is proposed for UWSNs, where a mobile AUV moves according to a predefined route navigated by compass and sends directional beacons to localize unknown nodes. Compared with stationary localization algorithms, mobile ones are more suitable for dynamic UWSNs.

In above mentioned typical underwater localization algorithms, there are four problems: (1) Many localization algorithms require time synchronization. However, few of them research on the time synchronization problem; (2) Most existing algorithms ignore the influence of ocean mobility; (3) Some localization algorithms use mobile anchor nodes, but how to reasonably and effectively design the path planning of mobile anchor nodes is not resolved; (4) The problems of malicious attacks and the related security mechanisms are not considered in the localization process. In [22], Liu *et al*. firstly propose a Joint time Synchronization and Localization (JSL) algorithm. In JSL, the effect of depth information on the speed of sound and time synchronization is considered. However, in practical applications, the underwater acoustic velocity is not a constant, which varies with underwater environmental information, e.g., depth, temperature and salinity. In [23], Diamant *et al*. propose a new joint time synchronization and localization algorithm based on the uncertainty of acoustic velocity. However, the algorithm assumes that each sensor node is equipped with a directional navigation system, which is difficult to meet in practice. And in 2014, Diamant *et al*. further study the ranging and positioning problem in visual line of sight (LOS) and non line of sight (NLOS) environments [24]. Considering the mobility of underwater environment, Guo et al. firstly propose a novel Localization for Active-restricted UWSNs (LAR) [25]. In [26], Kim *et al*. propose a time Synchronization and Localization algorithm using Seawater Movement Pattern (SLSMP) to improve localization accuracy based on the unique characteristics of UWSNs, e.g., inevitable node movement and variable propagation delay. For the third problem, many path planning schemes of mobile anchor nodes have been proposed. For example, in [27], Han *et al*. firstly propose a path planning scheme based on triangle for a mobile anchor node to minimize the average localization error of unknown nodes. In [28], a cooperative path planning method is proposed for mobile UWSNs, which can be used

to locate and navigate underwater mobile AUV; however this method is only suitable for tracking one AUV at a time. For the forth problem, the research of malicious attacks and security mechanisms in the process of localization is still at the initial stage. Few study has been worked on the secure localization problem and a lot of research problems need to be solved. That is why we study the secure localization problem in this paper. In the next section, we will present our proposed localization scheme CSLT in detail.

3. Collaborative Secure Localization Algorithm

In this section, we first introduce the network model, related assumptions and definitions, then describe collaborative secure localization mechanisms and present the CSLT algorithm, which includes the following five sub-processes: (1) trust evaluation of anchor nodes; (2) initial localization of unknown nodes; (3) trust evaluation of reference nodes; (4) selection of reference node; and (5) secondary localization of unknown node.

3.1. Network Model and Assumptions

We assume there are three types of sensor nodes in the UWSNs: surface buoys, mobile AUVs, and unknown nodes, as shown in Figure 1. Surface buoys are floating on the ocean surface, which can directly obtain their positions by GPS and localize unknown nodes in their communication ranges. The AUV can first obtain its location on the surface, then dives into water to localization unknown nodes in the deep water. The sensor node which can first obtain its own location information and then help unknown nodes with localization is named as an anchor node. Therefore, both the surface buoys and the AUVs are anchor nodes. In this paper, we assume that all the anchor nodes can accurately obtain their positions from GPS as some previous underwater localization algorithms did. The GPS accuracy impacts on localization are not within the scope of this paper. All unknown nodes have the same initial energy level, the same capability of communication, computation and storage.

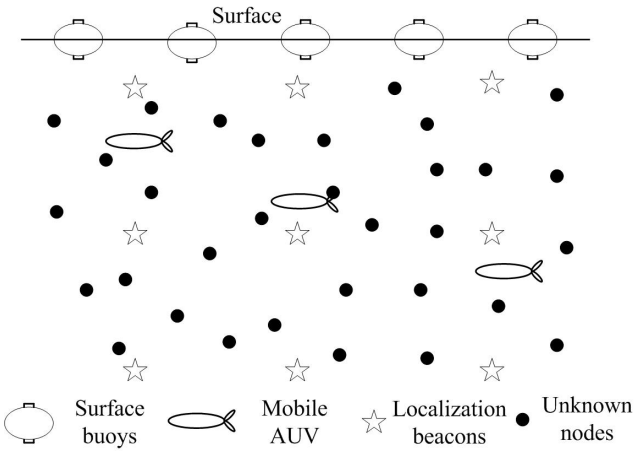


Figure 1. The structure of network model.

In the UWSN, there are n unknown nodes, denoted by $u_i \in S$, where $U = \{u_i\}_{i=1}^{n}$. Each unknown node u_i is randomly deployed at the position p_i with the communication range r. Only when the distance $d(p_i, p_j)$ between two neighbor node u_i and u_j satisfies $d(p_i, p_j) \leq r$, the two neighbor unknown nodes can directly communicate with each other. We call them one-hop neighbor nodes. Similarly, there are two-hop and multi-hop neighbor nodes. In this paper, two-hop neighbor nodes will be used in the secondary localization. In addition, there are many malicious attacks in the process of localization, as summarized in Table 1. All the malicious attacks are compared and analyzed in terms of existing countermeasures, attack behaviors and attack results.

Table 1. Analysis on malicious attacks against localization in Underwater Wireless Sensor Networks (UWSNs).

Layers	Attacks	Countermeasures	Attack Behaviors	Results
Physical Layer	Stealing	The perception mechanism for physical damage, encryption algorithm, *etc*.	Signal eavesdropping and tampering	packet error and packet loss
	Jamming	Multi-frequency communication, using different transmission priority, *etc*.	Send jamming signal on the working frequency	packet loss
Data Link Layer	Collision	Forward Error Correct (FEC) code.	Repeat to send messages	packet loss
	Exhaustion	Limit the transmission speed and retransmission times of packets	Send a lot of useless messages	packet loss
	Unfairness	Avoid using long packets, redistributing transmission priority of packets, *etc*.	Deliberately take up the channel	packet loss
Network Layer	DoS attacks	Detection of energy consumption	Repeatedly send many messages to exhaust energy	packet loss
	Selective forwarding	Multi-path routing, reputation and trust model, *etc*.	Selectively forward packets	packet loss
	Sybil	Identity authentication of sensor nodes	Have multiple identities	packet error
	Wormhole	Construction of network topology	Shorten distance	packet error
	Sinkhole	Traffic monitoring, identity authentication, multi-path routing, *etc*.	Maliciously tamper with routing	packet loss
Transport Layer	Flooding	Limit the broadcast range of sensor nodes	Establish false connections	packet loss
	Tampering	Data encryption and node authentication.	Tampering localization beacons	packet error

3.2. Overview of Secure Localization Algorithm CSLT

Before introduce our proposed algorithm, some definitions are presented at first.

Definition 1. localization beacon. In the process of localization, anchor nodes broadcast information to help unknown nodes with localization. All the broadcasted packets, which include coordinate information, ID information, trust values, *etc*., are named as localization beacons.

Definition 2. upgrade anchor node. A successfully localized unknown node can work as an anchor node to localize neighbor nodes. In this paper, the trusty and successfully localized unknown node can be selected as an anchor node, we named it as an upgrade anchor node.

Definition 3. reference node. All the anchor nodes and upgrade anchor nodes are collectively named as reference nodes. They can help unknown nodes with localization.

In order to maximize localization ratio and improve localization accuracy of underwater sensor nodes, we propose a multi-anchor nodes collaborative localization (MANCL) algorithm in [29]. The MANCL algorithm divides the whole localization process into four sub-processes: (1) unknown node localization process; (2) iterative location estimation process; (3) 3D Euclidean distance estimation process; and (4) 3D DV-hop distance estimation process.

In the first sub-process, anchor nodes broadcast their coordinates periodically. All the unknown nodes that receive the coordinates can estimate their distances to the corresponding anchor nodes. If an unknown node receives four (or more than four) non-coplanar coordinates from different anchor nodes, the unknown node can calculate its position based on a multilateral localization method. However, in large-scale UWSNs, not all the unknown nodes can be successfully localized in the first sub-process. For example, some unknown nodes may not receive enough (at least 4) beacons from anchor nodes, or receive beacons from coplanar anchor nodes. In this case, the unknown nodes cannot be localized. In order to localize all the unknown nodes in the UWSN, we propose use other distance estimation methods and localization algorithms to help unknown nodes with localization.

First, the successfully localized unknown nodes are used to further localize their neighbor nodes in the second sub-process. The successfully localized unknown nodes with higher trust values can be chosen as upgrade anchor nodes; Then, the upgrade anchor nodes within two hops are used to help residual unknown node with localization during the rest of localization sub-processes; In the third sub-process, the improved 3D Euclidean distance estimation process which consists of two mechanisms (a communication mechanism and a vote mechanism) is proposed to localize unknown nodes. In the communication mechanism, non-localized unknown nodes use localized sensor nodes within communication range to estimate their coordinates. In the vote mechanism, neighboring anchor nodes and upgrade anchor nodes vote to determine the coordinates of non-localized sensor nodes. Finally, in the 3D DV-hop distance estimation process, the two-hop anchor nodes are used to calculate coordinates of unknown nodes. Simulation results show that, the proposed MANCL algorithm can perform better than related works with regard to localization ratio, average localization error, and energy consumption. However, how to evaluate trust values for sensor nodes are not discussed in [29]. Therefore, in order to improve location security of underwater sensor nodes, we propose a trust model for sensor nodes' trust evaluation and apply the trust model in the secure localization.

Based on our previous work MANCL in [29], the proposed secure localization algorithm in this paper consists of the following five parts: (1) trust evaluation of anchor nodes; (2) initial localization of unknown nodes; (3) trust evaluation of reference nodes; (4) selection of reference node; and (5) secondary localization of unknown node, as shown in Figure 2.

In the first sub-process, the trust values of anchor nodes are calculated based on the main idea of the reference [30] to detect malicious anchor beacons. The anchor node which sends legal localization beacons is assigned with a higher trust value. Only trusty anchor nodes can be used to localize unknown nodes in the rest of processes. In the second sub-process, the unknown nodes are localized based on the multilateral localization method by using positioning reference information from trusty anchor nodes. However, not all the unknown nodes can be successfully localized in the second sub-process. Therefore, in the third sub-process, we first evaluate trust value for each successfully

localized unknown node. Then, the trusty and successfully localized unknown node can be selected as a reference node in the forth sub-process. Finally, in the fifth sub-process, we use two-hop trusty anchor nodes and reference nodes to help localize unknown nodes. How to calculate unknown nodes has been carefully discussed in [29]. Thus, in the next section, we mainly introduce how to evaluate trust values for sensor nodes, which is the most important part in the process of secure localization.

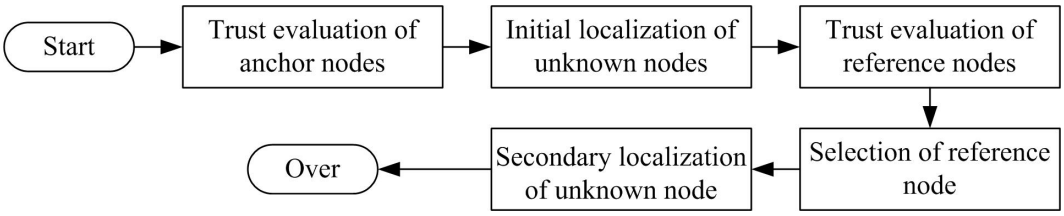


Figure 2. The five sub-processes in Collaborative Secure Localization algorithm based on Trust model (CSLT).

4. The Trust Evaluation Process

In this section, we introduce our proposed trust model in detail, including the overall architecture of the trust model, the process of trust calculation, trust combination and trust propagation. The structure of the trust model consists of four parts: (1) trust evidence generation; (2) trust calculation for one-hop neighbor nodes; (3) trust calculation for two-hop neighbor nodes; and (4) trust update.

In UWSNs, sensor nodes always freely move with ocean current. It is generally known that the movement of current in seashore environments changes continuously and demonstrates certain semi-periodical properties. That is, the movement of sensor nodes in the ocean current also obeys certain semi-periodical properties. It is hard to describe the semi-periodical properties since they change with different underwater environment. For simplicity's sake, we adopt a sliding time window concept [31] to periodically predict positions and calculate trust values for sensor nodes. Due to dynamic underwater environment, historical trust values should be taken into account to dynamically update trust relationship in time. In this paper, based on the sliding time window, we update sensor nodes' trust values as follows. As shown in Figure 3, each time window T consists of several units t. During each time slot t, packets redare exchanged between two neighbor nodes, trust evidences can be collected to evaluate trust of sensor nodes. After a unit of time elapses, the window slides one time unit forward. Then, in the next time window $t+1$, the historical trust values can be used to update new trust values, thereby dropping the recorded information during the last time window t.

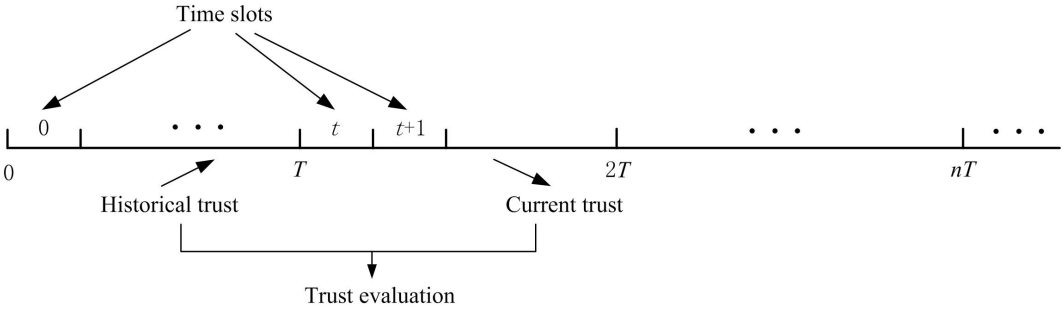


Figure 3. A sliding time window.

4.1. Trust Evidence Generation

In the first part of trust model, trust evidences are collected. As analyzed in the Table 1, there are many malicious attacks against localization and the main attack results can be classified into two categories: heavy packet loss and packet error. On one hand, malicious nodes can selectively

forward or discard localization beacons, and they also can be selfish nodes refusing to take part in the localization process. In this case, unknown nodes may fail to localize themselves due to missing beacons, which introduces high packet loss. On the other hand, malicious nodes can monitor localization beacons from normal anchor nodes, then modify the beacons or send wrong localization information to mislead unknown nodes' localization, which introduces high packet error. Therefore, packet loss and packet error are taken as two main trust evidences in the CSLT algorithm to detect malicious anchor beacons and calculate trust values of sensor nodes. If packet error of loss is detected, the related sensor nodes will be assigned with a lower trust values and will not be used in the localization process. The trust model is not used to detect malicious node, but used to choose sensor nodes with higher trust level to participate into localization to ensure localization ratio and accuracy. As a kind of intrusion tolerance technology, the trust model is used to ensure network security allowing existence of malicious node, which is a little different from the intrusion detection technology. The intrusion detection technology is always used to detect and remove malicious nodes. However, in the trust model, the malicious nodes are kept in the network while may not be used until they become trust ones.

At the beginning of localization, there are only three types of sensor nodes in the UWSN: surface buoys, mobile AUVs, and underwater unknown nodes. A real number from 0 to 1 is used to denote the trust value, 1 means completely trust and 0 means the opposite. We assume that all the anchor nodes are trusty at the beginning of network deployment, and set their trust value to 1. Then, based on the main idea of [30], we calculate trust value for anchor nodes according to packet loss and packet error. In the process of unknown nodes' initial localization process, only one-hop anchor nodes are used. Therefore, we first introduce trust evaluation for one-hop neighbor nodes. Then, in the process of unknown nodes' secondary localization process, two-hop anchor nodes and reference nodes are used. Thus, we will further present trust evaluation for two-hop neighbor nodes.

4.2. Trust Calculation for One-Hop Neighbor Nodes

In this subsection, the trust relationship between one-hop neighbor nodes is established by using the habit of human psychological cognition for reference, in which direct experience is the priority for evaluation and judgement. For example, in social network, if two people are friends or they are very familiar with each other, they can directly get assessment on each other's trust level based on their daily communications. Otherwise, trust relationship between strangers needs recommendations from the third parties. Therefore, in the process of secure localization in UWSNs, if two neighbor anchor nodes have enough information for each other, that is there are enough trust evidences for evaluating trust relationship, we only need to calculate direct trust as final trust. Otherwise, only when the trust evidence is not sufficient for direct trust evaluation, neighbor nodes' recommendations are required. This not only limits the number of information exchange between neighbor nodes, reduces the communication overhead and the complexity of the algorithm, but also greatly improves the accuracy of trust evaluation, and avoids the impact caused by malicious nodes in the process of trust recommendation, so that the trust evaluation between one-hop neighbor nodes is more true and reliable.

In the process of trust calculation for one-hop neighbor nodes, there are two main types of trust evaluation: direct trust evaluation and recommendation trust evaluation, as shown in Figure 4. If an anchor node **a** wants to obtain the trust value of another anchor node **b**, the evaluated anchor node **b** is named as a target node. The evaluating anchor node **a** which is responsible for trust evidence collection and trust evaluation is named as a sponsor node. Based on communication behaviors between anchor nodes, a sponsor anchor node can assign a target anchor node with different trust values. If there are direct communications between anchor nodes, direct trust is calculated. Otherwise, recommendation trust can be computed based on other anchor nodes' recommendations. The anchor node which is selected as a trusted third party to provide recommendations is named as a recommender, just like $\{m_1, m_2, m_3, \cdots\}$ in the Figure 4.

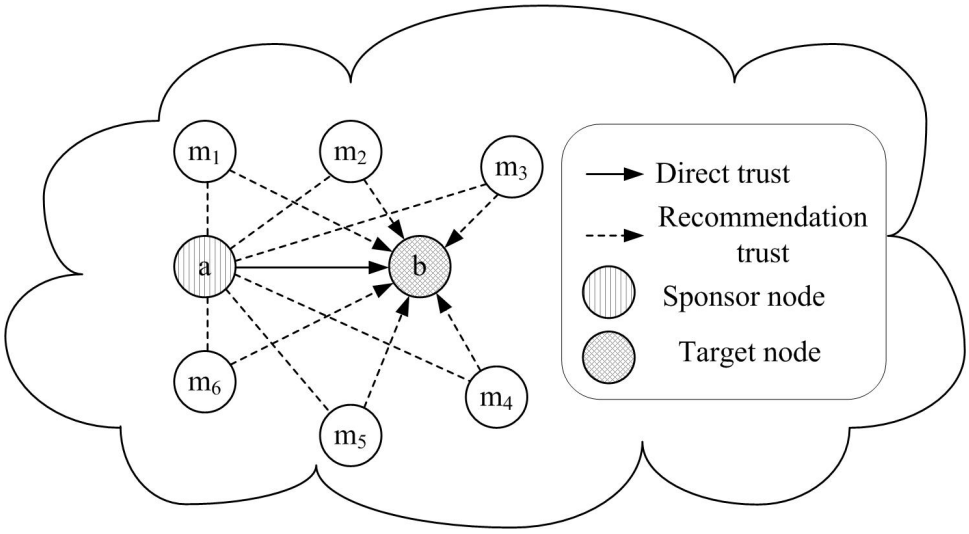


Figure 4. Trust calculation for one-hop neighbor nodes.

4.2.1. Direct Trust Calculation for One-Hop Neighbor Nodes

If there are enough information interactions between neighbor nodes, direct trust can be calculated based on their communication behaviors. In this subsection, direct trust is calculated based on two trust evidences: packet error and packet loss. In current trust models, the packet loss is widely used as important trust evidence [32]. Thus in this paper, the statistics of packet loss is also used as follows.

It is generally known that underwater acoustic communications are characterized by high bit error and temporary loss of connectivity. Therefore, in UWSNs, the packet loss is always caused by three reasons: unreliable acoustic channel, inevitable node movement and malicious nodes. In order to accurately obtain the packet loss from malicious nodes, we first need to analyze the packet loss caused by acoustic communication channel and node movement. In the acoustic channel, the data packet loss is mainly caused by high Bit Error Rate (BER) which is directly related with the signal-to-noise ratio (SNR) of the channel. Therefore, the SNR of the acoustic channel is first analyzed as:

$$SNR(l,f) = \frac{P/A(l,f)}{N(f)\Delta f} \tag{1}$$

where P is the acoustic signal power. Δf is the noise bandwidth of the receiver node. $N(f)$ is the the overall power spectral density of noises. $A(l,f)$ is the path loss of the acoustic signal. There are four kinds of the ocean background noise: turbulence, shipping, waves and thermal noise. We use $N_t(f)$, $N_s(f)$, $N_w(f)$ and $N_{th}(f)$ to denote the power spectral density of turbulence, shipping, waves and thermal noise, respectively.

$$\begin{cases} 10\log N_t(f) = 17 - 30\log f \\ 10\log N_s(f) = 40 + 20(s-0.5) + 26\log f \\ \quad - 60\log(f+0.03) \\ 10\log N_w(f) = 50 + 7.5w^{1/2} + 20\log f - 40\log(f+0.4) \\ 10\log N_t h(f) = -15 + 20\log f \end{cases} \tag{2}$$

Therefore, we can obtain $N(f) = N_t(f) + N_s(f) + N_w(f) + N_{th}(f)$. In addition, the path loss $A(l,f)$ is calculated by $A(l,f) = A_0 l^k a(f)^l$, where A_0 is a normalization constant. l is the communication distance between two nodes. k is the energy propagation coefficient. In general, for the spherical spreading, $k = 2$. $a(f)$ is the absorption coefficient in underwater environment and f is the frequency of the acoustic signal.

Based on the SNR in Equation (1) and the modulation mode of acoustic communication, the average bit error rate (BER) can be calculated by $BER(l,f) = \Phi^M(SNR(l,f))$, where M denotes the used modulation mode. Then, the packet loss caused by unreliable acoustic channel can be obtained as:

$$P_{loss1} = \Psi^F(b, BER(l,f)) \tag{3}$$

where F denotes the forward error correction (FEC) mechanism. b is the length of the packet.

To study the packet loss caused by node movement, we adopt a Meandering Current Mobility (MCM) model [33] to describe the mobility of ocean current and underwater sensor nodes. MCM exploits the fact that the ocean current is a stratified, rotating fluid. Therefore, compared with the current movement in the horizontal direction, the vertical movement of ocean can be negligible. The ocean current is described as an incompressible two-dimensional flow, which is denoted by a stream function ψ. ψ consists of two components of the divergenceless velocity: $u = -\frac{\partial \psi}{\partial y}, v = \frac{\partial \psi}{\partial x}$. u is the zonal (eastward) component of the velocity and v is the meridional (northward) one. The node movement is calculated based on the solution of Hamiltonian ordinary differential equations: $\dot{x} = -\partial_y \psi(x,y,t), \dot{y} = -\partial_x \psi(x,y,t)$. Therefore, we can judge whether two nodes **a** and **b** are neighbor nodes or move out of the communication range r according to the movement trajectory. If two node cannot directly communicate with each other, we think the packet loss is infinite. Other, if two sensor nodes are neighbors, the packet loss caused by node movement is 0. That is:

$$P_{loss2} = \begin{cases} 0, d_{ab} < \mathrm{r} \\ \infty, d_{ab} \geq \mathrm{r} \end{cases} \tag{4}$$

In each time slot, all anchor node broadcast information for their neighbor nodes and record the number of broadcasted packets n. The anchor nodes which receive the information also record the number of successfully received packets $n_{s-anchor}$. The number of all the loss packets is $n - n_{s-anchor}$. Because a part of packet loss is caused by unreliable acoustic channel P_{loss1}, the number of loss packets caused by malicious nodes should be $n_f = n - n_{s-anchor} - P_{loss1}$. Thus, the number of successfully received packets n_s should be corrected as $n_s = n - n_f = n_{s-anchor} + P_{loss1}$. In the next time slot, if two neighbor nodes are still be neighboring, we obtain $P_{loss2} = 0$. Otherwise, if two neighbor nodes move out of the communication range, we obtain $P_{loss2} = \infty$. In this case, the packet loss caused by malicious nodes n_f is not updated and keeps the calculated value in the last time slot. Therefore, even if the receiver node cannot receive any packets, the sender node will not be erroneously assigned with a low trust value.

According to packet loss, we use the main idea of [34] based on Bayesian Formulation to evaluate trust relationship. In [34], the reputation of a sensor nodes is first calculated based on the beta distribution, which is indexed by two parameters (α, β) and can be expressed using the gamma function $\Gamma(\cdot)$ as $P(x) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1}, \forall 0 \leq x \leq 1, \alpha \geq 0, \beta \geq 0$. The reputation of node j evaluated by node i is given as $R_{ij} = Beta(\alpha_j + 1, \beta_j + 1)$, where α_j and β_j represents the cooperative and non-cooperative interactions between node i and j, respectively. The trust of a sensor node is the statistical expectation of the reputation function and is calculated as:

$$T_{ij} = E(R_{ij}) = E(Beta(\alpha_j + 1, \beta_j + 1)) = \frac{\alpha_j + 1}{\alpha_j + \beta_j + 2} \tag{5}$$

Therefore, based on n and n_s, and according to the reference [34], in which trust is denoted by $(\alpha_j + 1)/(\alpha_j + \beta_j + 2)$, the trust of an anchor node j can be calculated by node i as

$$T_{ij} = \frac{n_s + 1}{n_s + n_f + 2} = \frac{n_s + 1}{n + 2} \tag{6}$$

In UWSNs, packet loss caused by unreliable acoustic channel and inevitable node movement is heavy. Getting statistics like packet loss as trust evidence is not reliable enough in underwater environment. Therefore, in this paper, we further propose using packet error to evaluate trust for sensor nodes based on the main idea of [30]. In [30], the main idea is to make use of the known locations of anchor nodes and the constraints that the locations must satisfy with the measurements (e.g., distance, angle) derived from the localization beacon signals. The anchor node which performs malicious node detection is named as detecting node. The detecting node first sends a localization request message to the target anchor node. The target node will send back a localization beacon packet which contains its own location information upon receiving the request message. Once the detecting node receives the beacon packet, it first estimates the distance between them. In addition, because the detecting node both knows its own location and receives the target node's location, it can also calculate the distance between them. Finally, the detecting node compares the estimated distance and the calculated one. If the difference between them is larger than the maximum distance error, the detecting node can infer that the position information in the received beacon packet must be wrong. Similarly, in this paper, each anchor node broadcast their location information to neighbor nodes. They pretend to be unknown nodes to localize each other. According to the broadcasted coordinates, each anchor node can calculate the distances l_{ij} to its neighbor nodes. At the same, the distances l_c can be obtained by sound-ranging techniques, e.g., ToA (Time of Arrival), TDoA (Time difference of arrival), RToF (Round Trip time of Flight). For two neighbor anchor nodes i and j, we calculate their distance by

$$l_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \tag{7}$$

If $|l_{ij} - l_c| > l_{th}$, where l_{th} is the maximum ranging error, the received packet can be judged as including wrong coordinate information.

In UWSNs, the bit error rate (BER) of underwater acoustic channel is very high, thus the wrong coordinate information may be caused by BER. We cannot directly judge whether the neighbor node is trusty or not based on the result of a calculation from Equation (6). Therefore, we propose that node i record the number of correct packets and wrong packets from node j as n_c and n_r, respectively. In each time period T, we obtain the number of neighbor node's cooperative and non-cooperative behaviors as

$$\begin{cases} n_1 = n_s + n_c \\ n_2 = n_f + n_r \end{cases} \tag{8}$$

Therefore, based on packet loss and packet error, the trust of node j is calculated by

$$T_{ij} = \frac{n_1 + 1}{n_1 + n_2 + 2} \tag{9}$$

In each time period T, node i can calculate trust value of node j for N time.

How to combine the N calculated trust values to evaluate the trust relationship is the essential problem to research in the trust model. In underwater environment, the acoustic communication and the behaviors of packet exchanges are uncertainty, thus the calculated N calculated trust values are different. The usually used average method and the median method cannot deal with the uncertainty characteristic of acoustic communication. Thus, in this subsection, we adopt cloud theory to calculate the sensor node's direct trust based on the N trust values, since cloud theory are well used to describe uncertainties relationship, e.g., fuzziness and randomness [35]. For any trust attribute x, if $\forall x \in X$, where X is a trust evaluation domain denoted with accurate value, there is a mapping μ satisfies that

$$\mu : X \to [0,1], x \to \mu(x) \in [0,1] \tag{10}$$

then, the distribution of x in the domain X is called trust cloud.

Cloud model has three digital features (E_x, E_n, E_e). E_x is the excepted value of the attribute, which reflects the central trust value. E_n is the entropy of the attribute, which reflects the trust ambiguity of E_x. E_e is the hyper entropy of the attribute, which reflects the uncertainty of E_n.

For any x_i, we can obtain (E_{xi}, E_{ni}, E_{ei}) as follows:

- Step 1. Computing the mean value $\bar{x_i}$ and the variance S^2 of x_i, $\bar{x_i} = \frac{1}{n}\sum_{i=1}^{n} x_i$, $S^2 = \frac{1}{n-1}\sum_{i=1}^{n}(\bar{x_i} - x_i)^2$.
- Step 2. Computing E_{xi}, $E_{xi} = \bar{x_i}$.
- Step 3. Computing E_{ni}, $E_{ni} = \sqrt{\frac{\pi}{2}} \times \frac{1}{n}\sum_{i=1}^{n} |E_{xi} - x_i|$.
- Step 4. Computing E_{ei}, $E_{ei} = \sqrt{S^2 - {E_{ni}}^2}$.

Therefore, according to the N calculated trust values T_{ij}, we can obtain the direct trust $T_d(E_x, E_n, E_e)$ based on the excepted value, the entropy and the hyper entropy of the attribute T_{ij}.

4.2.2. Recommendation Trust Calculation for One-Hop Neighbor Nodes

If there are not enough information interactions between two neighbor nodes, the trust relationship between them needs to be established based on the third party nodes' recommendations. As shown in Figure 4, the first step of recommendation calculation is to select reliable recommender nodes among all the neighbor nodes. If node **a** wants to obtain the recommendations of node **b**, it first broadcasts recommendation request to all the common neighbor nodes of them. The neighbor nodes which have the trust value of node **b** will reply related acknowledgment packet to node **a**. The reliable recommenders are selected among the reply nodes according to the following principle: (1) the selected recommender should be trusty; (2) the recommendation value should be reliable. Whether a recommender is trusty or not can be easily judged by its trust value. The reliability of a recommendation value is decided by the familiarity degree between the recommender and the sponsor node. In general, people are more dependent on more familiar things and think they are reliable. Similarly, the more frequently two neighbor nodes communication with each other, the higher credibility of the recommendation trust value is. That is, the reliability of a recommendation value is judged by the familiarity among neighbor nodes.

If there are m recommenders selected for target node, we can obtain m recommendation values as $\{T_{r1}(E_{x1}, E_{n1}, E_{e1}), T_{r2}(E_{x2}, E_{n2}, E_{e2}), \cdots, T_{rm}(E_{xm}, E_{nm}, E_{em})\}$. Therefore, the total recommendation trust $T_r(E_x, E_n, E_e)$ can be calculated by

$$T_r = T_{r1} \oplus T_{r1} \oplus \cdots \oplus T_{rm} \tag{11}$$

$$T_r = T_{r1}(E_{x1}, E_{n1}, E_{e1}) \oplus T_{r2}(E_{x2}, E_{n2}, E_{e2}) \oplus \cdots \oplus T_{rm}(E_{xm}, E_{nm}, E_{em}) \tag{12}$$

$$\begin{cases} E_x = \frac{1}{m}\prod_{i=1}^{m} E_{xi} \\ E_n = \min(\frac{1}{m}\sum_{i=1}^{m} E_{ni}, 1) \\ E_e = \min(\frac{1}{m}\sum_{i=1}^{m} E_{ei}, 1) \end{cases} \tag{13}$$

4.3. Trust Calculation for Two-Hop Neighbor Nodes

There are no direct interactions between non-neighbor nodes; therefore, the trust relationship between two-hop neighbor nodes needs to be established based on the trust recommendations from the third intermediate nodes. As shown in Figure 5, the trust evaluation process of non-hop neighbor

nodes can be described as follows. First, for multi-hop neighbor node, several intermediates nodes are selected to obtain recommendation trust. The principle to select the multi-hop intermediates nodes is the same as the recommender selection in previous sub-section. Then, a trust routing path is established to propagate trust from the sponsor node to the target node. The trust attenuates along with the growing routing path. The longer the path is, the greater attenuation of trust is. Therefore, the shortest path should be selected to route recommendations. Finally, the indirect trust is calculated based on all the recommendations.

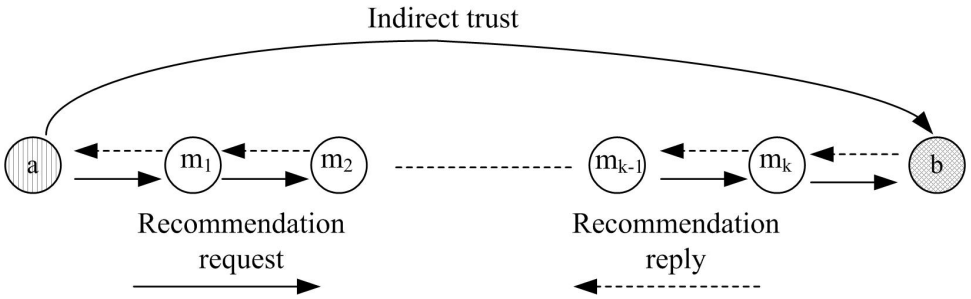


Figure 5. Trust calculation for two-hop neighbor nodes.

If there are k anchor nodes on the trust propagation path, we can obtain k recommendation values as $\{T_{ind1}(E_{x1}, E_{n1}, E_{e1}), T_{ind2}(E_{x2}, E_{n2}, E_{e2}), \cdots, T_{indk}(E_{xk}, E_{nk}, E_{ek})\}$. Therefore, the indirect trust $T_ind(E_x, E_n, E_e)$ can be calculated by

$$T_{ind} = T_{ind1} \otimes T_{ind1} \otimes \cdots \otimes T_{indk} \tag{14}$$

$$T_{ind} = T_{ind1}(E_{x1}, E_{n1}, E_{e1}) \otimes T_{ind2}(E_{x2}, E_{n2}, E_{e2}) \otimes \cdots \otimes T_{indk}(E_{xk}, E_{nk}, E_{ek}) \tag{15}$$

$$\begin{cases} E_x = \prod_{i=1}^{k} E_{xi} \\ E_n = \min(\sum_{i=1}^{k} {E_{ni}}^2, 1) \\ E_e = \min(\sum_{i=1}^{k} E_{ei}, 1) \end{cases} \tag{16}$$

In this paper, only two-hop anchor nodes and reference nodes are used in the secure localization, therefore, $k = 2$. However, the proposed trust model is also suitable for other networks where $k > 2$.

4.4. Trust Update

In order to timely and accurately update trust values, a new trust value T_{new} is calculated based on the historical trust T_{old} and the calculated trust in current time period T_{now}:

$$T_{new} = \omega_{old} T_{old} + \omega_{now} T_{now} \tag{17}$$

where ω_{old} and ω_{now} are the weight values of T_{old} and T_{now}, $\omega_{old} + \omega_{now} = 1$. The two weight values are decided by the number of neighbor node's cooperative behaviors. If the number of neighbor node's cooperative behaviors in current time period n_{1new} is higher than that in the last time period n_{1old}, we obtain $0.5 \leq \omega_{old} < 1, 0 \leq \omega_{1new} < 0.5$. The historical trust is mainly used as reference for trust update in order to prevent malicious nodes from intentionally and rapidly increasing their own trust values by camouflage or lying. Otherwise, $0 \leq \omega_{old} < 0.5, 0.5 \leq \omega_{1new} < 1$. The current calculated trust is mainly used as reference to punish the behaviors of malicious nodes.

5. Simulation Results and Discussions

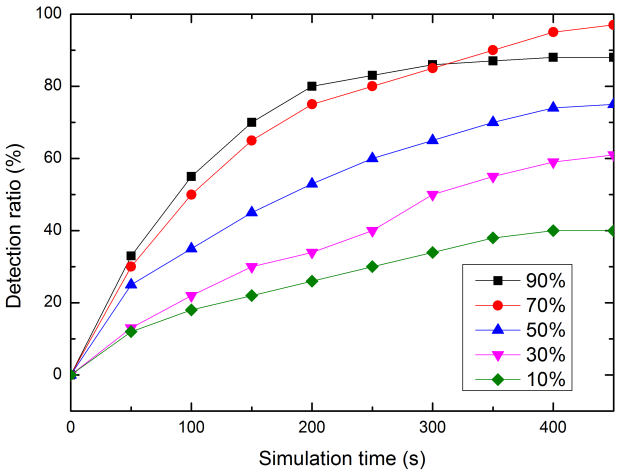
In this section, the performance of the proposed secure localization algorithm is evaluated. The algorithm was implemented using MATLAB. In the experiments, the deployment area is set to 500 m × 500 m × 500 m. There are 500 unknown nodes randomly deployed in the 3D space. The communication range of unknown nodes is set to 100 m. Other parameters used in simulations are listed in Table 2. The performance of CSLT is compared based on the following three metrics: (1) detect ratio of malicious nodes, which is used to evaluate the security of CSTL; (2) localization accuracy, which is one of the most important evaluation indicators of localization algorithms; (3) localization ratio, which is used to evaluate whether all the unknown nodes can be successfully localized; (4) energy consumption, which is used to evaluate energy efficient of the proposed algorithm in energy-limited UWSNs.

Table 2. Simulation Parameters.

Parameters	Value
Simulation region size	500 m × 500 m × 500 m
The number of unknown nodes	500
Communication range	100 m
Node placement	Randomly deployed
Initial trust value	1
Acoustic channel bandwidth	100 Kbps
The modulation mode for acoustic communication	BPSK modulation
Mobility model	The Meandering Current Mobility (MCM) model

5.1. Comparison of Detect Ratio

In our proposed CSLT, the weight values chosen for trust update are not constants, which are decided based on the knowledgeable of current network situation and directly impact the performance of CLST. Thus, we first simulate the weight value's on the algorithm performance, e.g., the detect ratio of malicious nodes. As shown in Figure 6, the detection ratio of malicious nodes rises step by step along the simulation progresses. When $n_{1new} > n_{1old}$, choosing ω_{old} as $0.5 \leq \omega_{old} < 1$ can detect more malicious nodes. This is because all the malicious nodes which intentionally to increase their values can be effectively detected. When $n_{1new} < n_{1old}$, choosing ω_{old} as $0 \leq \omega_{old} < 0.5$ can performance better. This is because, in this case, mainly using the current calculated trust as reference to update trust can well punish the behaviors of malicious nodes.



(**a**)

Figure 6. *Cont.*

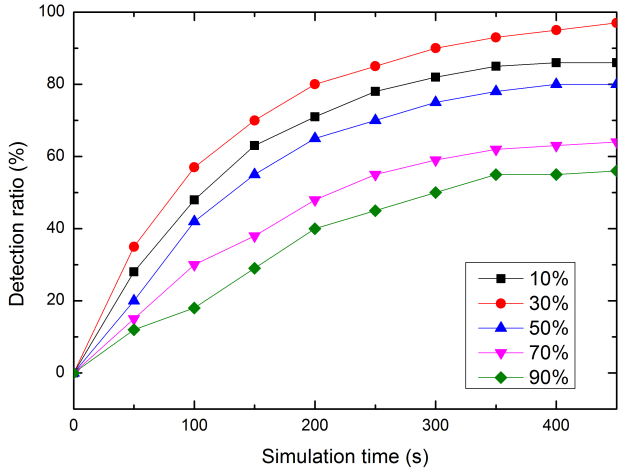


Figure 6. The performance of detection ratio. (**a**) $n_{1new} > n_{1old}$; (**b**) $n_{1new} < n_{1old}$.

Our secure localization is proposed based on MANCL [29], ReTrust [31], and RFSN [34], thus CSLT is compared with the three references. As shown in Figure 7, nine types of malicious nodes are detected. They are (1) signal interference attacks; (2) link collision attacks; (3) DoS attacks; (4) selective forwarding attacks; (5) Sybil attacks; (6) wormhole attacks; (7) sinkhole attacks; (8) flooding attacks and (9) packet tampering attacks. Simulation results show that our proposed CSLT can well detect the nine types of malicious nodes with more than 95% detection ratio. However, we cannot find malicious node with 100%. This is because some malicious nodes which cause packet error or loss of the surrounding nodes' instead of in their own communication cannot be efficiently found out. MANCL cannot detection all the malicious attacks because it does not use any secure mechanism in the process of localization. RFSN and ReTrust are only effective against selective forwarding attacks, since they just consider packet loss to evaluate trust for sensor nodes. Therefore, they cannot detect the rest types of malicious nodes, e.g., Sybil attacks, wormhole attacks and packet tampering attacks. However, ReTrust works better than RFSN in terms of malicious node's detection ratio. This is because in RFSN, only direct trust are calculated and only one-hop neighbor nodes' behaviors can be monitored, while in ReTrust, neighbor nodes' recommendation are also taken into account to evaluate trust. Relatively specking, ReTrust is much more reliable and robust against malicious attacks than RFSN.

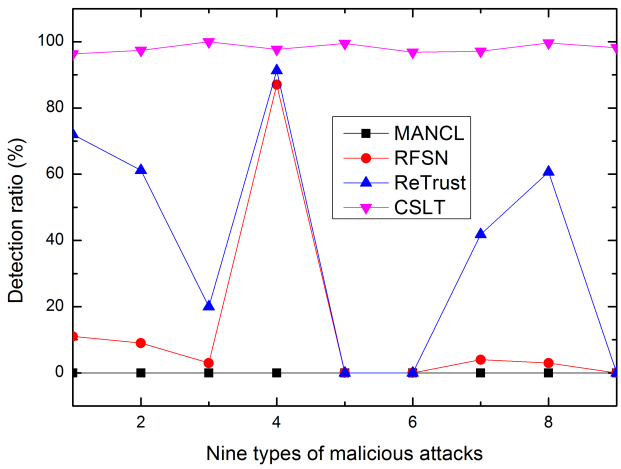


Figure 7. Comparison of detect ratio.

5.2. Comparison of Localization Accuracy

Localization accuracy is one of the most important evaluation indicators of localization algorithms. In this paper, the localization accuracy is denoted by the relative error between the actual location and the calculated node position. As shown in Figure 8a, the ratio of malicious nodes varies from 5% to 30% with increments of 5%. The impact of malicious node ratio on localization accuracy is first evaluated. Simulation results show that localization errors increases with the increasing number of malicious nodes, since more malicious nodes introduce more attacks and interferences on localization. However, CSLT still out performs other algorithm in terms of localization accuracy.

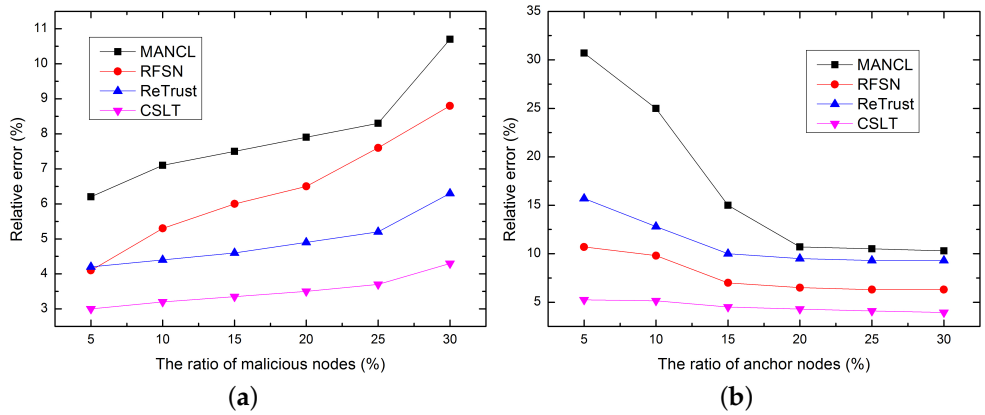


Figure 8. Comparison of localization accuracy. (**a**) Impact of malicious node ratio; (**b**) Impact of anchor node ratio.

In addition, the impact of anchor node ratio on localization accuracy is evaluated in Figure 8b. Simulation results show that with the increase number of anchor nodes, the average localization errors of all the algorithms decrease rapidly. This is because more localization beacons can be provided by more anchor nodes to localize unknown nodes. Most unknown nodes can be successfully localized in the initial localization process. Only a small part unknown nodes need to be localized in the secondary localization process. The accumulated localization errors from upgrade anchor node can be greatly reduced, which ultimately improves localization accuracy.

5.3. Comparison of Localization Ratio

In this sub-section, the localization ratio is compared, which is defined as the percentage of successfully localized unknown nodes. As shown in Figure 9, the localization ratio decreases as the increasing number of malicious nodes, and increases with the growing number of anchor nodes. Obviously, more unknown nodes can be localized with more anchor nodes. In addition, more packet error and packet loss will be introduced by more malicious nodes. In this case, some unknown nodes cannot receive enough localization beacons to localize themselves, which greatly reduces the localization ratio. However, our proposed CSLT has higher localization ratio than the compared algorithm, this is because, in CSLT, a reliable trust model is proposed to ensure the security of sensor nodes, and a secondary localization process is also helpful to improve localization ratio.

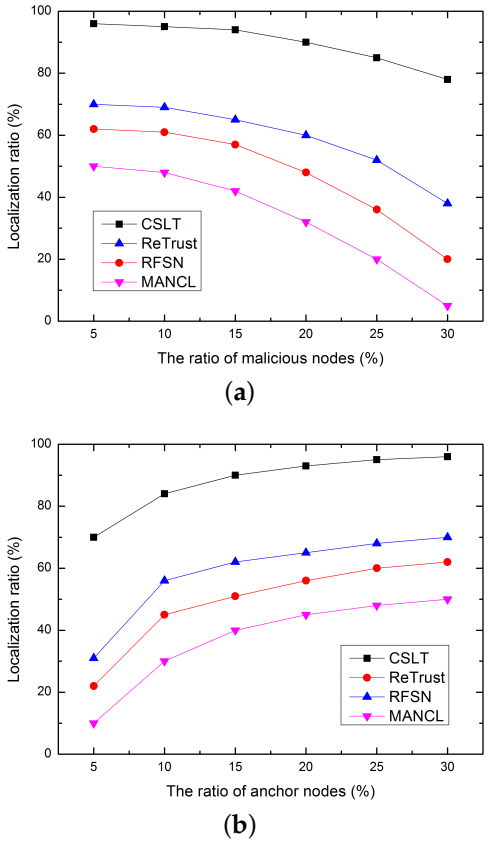


Figure 9. Comparison of localization ratio. (**a**) Impact of malicious node ratio; (**b**) Impact of anchor node ratio.

5.4. Comparison of Energy Consumption

Finally, the energy consumption of each algorithm is compared. As shown in Figure 10, our proposed CSLT consumes more energy than the compared algorithms, e.g., MANCL, ReTrust, and RFSN. In order to detect malicious nodes, CSLT needs to collect trust evidences and calculates trust values for sensor nodes, which introduces more communication overheads and consumes more energy. However, CSLT can well protect the network and ensure node security. In addition, CSLT performs better than the three compared related works in terms of location security, average localization accuracy and localization ratio. That is to say, we sacrifice some energy to improve network security, and ultimately to improve performance of secure localization.

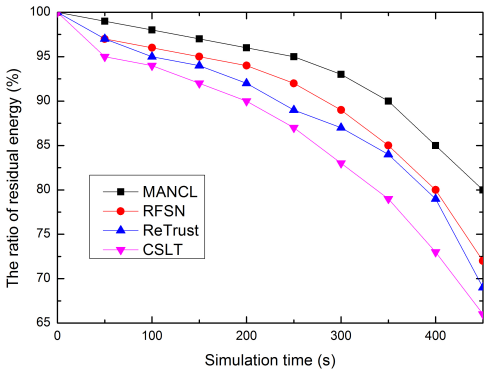


Figure 10. Comparison of energy consumption.

6. Conclusions

In this paper, we propose a collaborative secure localization algorithm based on the trust model for UWSNs. CSLT includes five sub-processes: trust evaluation of anchor nodes, initial localization of unknown nodes, trust evaluation of reference nodes, selection of reference node, and secondary localization of unknown node. Based on the trust model, the trust values of the one-hop anchor nodes and the two-hop reference nodes are calculated. Then, only trusty anchor nodes and references nodes are selected to localize unknown nodes to avoid impact from malicious nodes. Simulation results indicate that CSLT can achieve a high detect ratio of malicious nodes. In addition, the localization security including localization accuracy and localization ratio is improved in UWSNs. However, there are many remaining issues that need to be further studied for secure localization in UWSNs. First, we cannot find each type of malicious nodes with 100%. For example, some malicious nodes may not mostly cause packet error or loss in their own communication but the surrounding nodes'. Is this case, we just use the trust model to avoid the attacks from the malicious nodes. The influenced surrounding nodes are assigned with lower trust values, since their communication behaviors are heavily impacted by surrounding real malicious node. They are not chosen to localize to unknown node to avoid the influence from nearby malicious node. However, the real malicious nodes cannot be detected efficiently. In our simulation, the number of this kind of malicious node is relatively small. If most malicious nodes launch this kind of malicious attack, our trust model may not work very well. So we will further study new trust model to solve this problem in the future research. In addition, we use MATLAB to evaluate the performances of the proposed algorithm in order to easily compare our new algorithm with our previous work in [29]. To make our simulation results more reliable, we will further study the new platforms, e.g., NS, Aquasim, etc., for underwater environment. Last but not least, we assume that all the anchor nodes can accurately obtain their positions from GPS as some previous underwater localization algorithms did. While in real application, it is hard for the anchor nodes to accurately obtain their positions from GPS, and the position accuracy of anchor nodes is heavily influence localization accuracy of unknown nodes. Therefore, we will further to study the GPS accuracy impacts in our future work.

Acknowledgments: This work was supported in part by the Qing Lan Project, in part by the National Science Foundation of China under Grant 61572172,and Grant 61401107, in part by the Natural Science Foundation of Jiangsu Province of China under Grant BK20131137,in part by the Open Fund through the Guangdong Provincial Key Laboratory of Petrochemical Equipment Fault Diagnosis under Grant PEFD2015-06, in part by the Educational Commission of Guangdong Province, China, under Project 2013KJCX0131, in part by the Guangdong High-Tech Development Fund under Grant 2013B010401035, in part by the 2013 Special Fund of Guangdong Higher School Talent Recruitment, and part by the Instituto de Telecomunicações, Next Generation Networks and Applications Group (NetGNA), Covilhã Delegation, Portugal and by National Funding from the FCT âĂŞ Fundação para a Ciência e a Tecnologia through the UID/EEA/500008/2013 Project.

Author Contributions: Guangjie Han researched the literatures, conceived the study concepts, designed the calibration method, carried out the simulation, analyzed the simulation results, and took charge of the entire manuscripts. Li Liu and Jinfang Jiang assisted with the integrity of the entire study, provided the crucial intellectual support, and revised the manuscript. Lei Shu contributed to the manuscript preparation and drafted the paper. Joel J.P.C. Rodrigues contributed to modify and polish the revised manuscript.

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

References

1. Erol-Kantarci, M.; Mouftah, H.T.; Oktug, S. A survey of architectures and localization techniques for underwater acoustic sensor. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 487–502.
2. Tan, H.; Diamant, R.; Seah, W.K.G.; Waldmeyer, M. A survey of techniques and challenges in underwater localization. *Ocean Eng.* **2011**, *38*, 1663–1676.
3. Han, G.; Jiang, J.; Shu, L.; Xu, Y.; Wang, F. Localization algorithms of underwater wireless sensor networks: A survey. *Sensors* **2012**, *12*, 2026–2061.

4. Omar, M.; Challal, Y.; Bouabdallah, A. Certification-based trust models in mobile ad hoc networks: A survey and taxonomy. *J. Netw. Comput. Appl.* **2012**, *35*, C268–C286.
5. Sherchan, W.; Nepal, S.; Paris, C. A survey of trust in social networks. *ACM Comput. Surv. (CSUR)* **2013**, *45*, 1–33.
6. Chandrasekhar, V.; Seah, W.K. An Area Localization Scheme for Underwater Sensor Networks. In Proceedings of the IEEE 61st Vehicular Technology Conference, Stockholm, Sweden, 30 May–1 June 2005; pp. 2835–2839.
7. Cheng, X.; Shu, H.; Liang, Q. A Range-Difference Based Self-Positioning Scheme for Underwater Acoustic Sensor Networks. In Proceedings of the International Conference on Wireless Algorithms, Systems and Applications (WASA), Chicago, IL, USA, 1–3 August 2007; pp. 38–43.
8. Cheng, X.; Shu, H.; Liang, Q.; Du, D.H. Silent positioning in underwater acoustic sensor networks. *IEEE Trans. Vehicul. Technol.* **2008**, *57*, 1756–1766.
9. Teymorian, A.Y.; Cheng, W.; Ma, L.; Cheng, X. Poster Abstract: An Underwater Positioning Scheme for 3D Acoustic Sensor Networks. Available online: http://wuwnet07.engr.uconn.edu/wipposters/WUWNet07-Teymorian-1.pdf (accessed on 10 February 2012).
10. Cheng, W.; Teymorian, A.Y.; Ma, L.; Cheng, X.; Lu, X.; Lu, Z. Underwater Localization in Sparse 3D Acoustic Sensor Networks. In Proceedings of the 27th IEEE Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 236–240.
11. Teymorian, A.Y.; Cheng, W.; Ma, L.; Cheng, X.; Lu, X.; Lu, Z. 3D underwater sensor network localization. *IEEE Trans. Mob. Comput.* **2009**, *5*, 1610–1621.
12. Cheng, W.; Thaeler, A.; Cheng, X.; Liu, F.; Lu, X.; Lu, Z. Time-Synchronization Free Localization in Large Scale Underwater Acoustic Sensor Networks. In Proceedings of the 29th IEEE International Conference on Distributed Computing Systems Workshops, Montreal, QC, Canada, 22–26 June 2009; pp. 80–87.
13. Mirza, D.; Schurgers, C. Collaborative localization for fleets of underwater drifters. In Proceedings of the OCEANS, Vancouver, BC, Canada, 29 September–4 October 2007; pp. 1–6.
14. Erol, 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, QC, Canada, 9–14 September 2007; pp. 97–100.
15. Erol, M.; Vieira, L.F.M.; Caruso, A.; Paparella, F.; Gerla, M.; Oktug, S. Multi Stage Underwater Sensor Localization using Mobile Beacons. In Proceedings of the 2nd International Conference on Sensor Technologies and Applications, Cap Esterel, France, 25–31 August 2008; pp. 25–31.
16. Erol, M.; Vieira, L.F.M.; Gerla, M. AUV-Aided Localization for Underwater Sensor Networks. In Proceedings of the International Conference on Wireless Algorithms, Systems and Applications (WASA), Chicago, IL, USA, 1–3 August 2007; pp. 44–54.
17. Waldmeyer, M.; Tan, H.P.; Seah, W.K.G. Multi-Stage AUV-Aided Localization for Underwater Wireless Sensor Networks. In Proceedings of the 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA), Singapore, 22–25 March 2011; pp. 908–913.
18. Waldmeyer, M.; Tan, H.P.; Seah, W.K.G. A Hierarchical Localization Scheme for Large Scale Underwater Wireless Sensor Networks. In Proceedings of the 11th IEEE International Conference on High Performance Computing and Communications, Seoul, Korea, 25–27 June 2009; pp. 470–475.
19. Lee, S.; Kim, K. Localization with a Mobile Beacon in Underwater Sensor Networks. In Proceedings of the IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), Hong Kong, China, 11–13 December 2010; pp. 316–319.
20. Luo, H.; Zhao, Y.; Guo, Z.; Liu, S.; Chen, P.; Li, L.M. UDB: Using Directional Beacons for Localization in Underwater Sensor Networks. In Proceedings of the 14th IEEE International Conference on Parallel and Distributed Systems (ICPADS), Melbourne, Australia, 8–10 December 2008; pp. 551–558.
21. Luo, H.; Guo, Z.; Dong, W.; Hong, F.; Zhao, Y. LDB: Localization with directional beacons for sparse 3D underwater acoustic sensor networks. *J. Netw.* **2010**, *5*, 28–38.
22. Liu, J.; Wang, Z.; Zuba, M.; Peng, Z.; Cui, J.; Zhou, S. JSL: Joint Time Synchronization and Localization Design with Stratification Compensation in Mobile Underwater Sensor Networks. In Proceedings of the 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), Seoul, Korea, 18–21 June 2012; pp. 317–325.

23. Diamant, R.; Lampe, L. Underwater Localization with Time-Synchronization and Propagation Speed Uncertainties. *IEEE Trans. Mob. Comput.* **2013**, *12*, 1257–1269.
24. Diamant, R.; Tan, H.; Lampe, L. LOS and NLOS Classification for Underwater Acoustic Localization. *IEEE Trans. Mob. Comput.* **2014**, *13*, 311–323.
25. Guop, Y. Localization for Active-Restricted 3D Underwater Sensor Networks. *J. Softw.* **2013**, *24*, 33–40.
26. Kim, S.; Yoo, Y. SLSMP: Time Synchronization and Localization Using Seawater Movement Pattern in Underwater Wireless Networks. *Int. J. Distrib. Sens. Netw.* **2014**, doi:10.1155/2014/172043.
27. Han, G.; Xu, H.; Jiang, J.; Shu, L.; Hara, T. Path Planning using a Mobile Anchor Node based on Triangulation in Wireless Sensor Networks. *Wirel. Commun. Mob. Comput.* **2013**, *13*, 1324–1336.
28. Tan, Y.; Gao, R.; Chitre, M. Cooperative Path Planning for Range-Only Localization Using a Single Moving Beacon. *IEEE J. Ocean Eng.* **2014**, *39*, 371–385.
29. Han, G.; Zhang, C.; Liu, T.; Shu, L. MANCL: A multi-anchor nodes collaborative localization algorithm for underwater acoustic sensor networks. *Wirel. Commun. Mob. Comput.* **2014**, doi:10.1002/wcm.2561.
30. Liu, D.; Ning, P.; Du, W. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks. In Proceedings of the 25th IEEE International Conference on Distributed Computing Systems, Columbus, OH, USA, 6–10 June 2005; pp. 609–619.
31. He, D.; Chen, C.; Chan, S.; Bu, J.; Vasilakos, A.V. ReTrust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks. *IEEE Trans. Inf. Technol. Biomed.* **2012**, *16*, 623–632.
32. Han, G.; Jiang, J.; Shu, L.; Niu, J.; Chao, H. Management and applications of trust in Wireless Sensor Networks: A survey. *J. Comput. Syst. Sci.* **2014**, *80*, 602–617.
33. Caruso, A.; Paparella, F.; Vieira, L.; Erol, M.; Gerla, M. The Meandering Current Mobility Model and its Impact on Underwater Mobile Sensor Networks. In Proceedings the 27th Conference on Computer Communications, the INFOCOM 2008, Phoenix, AZ, USA, 13–18 April 2008; pp. 1–9.
34. Ganeriwal, S.; Balzano, L.K.; Srivastava, M.B. Reputation-based framework for high integrity sensor networks. In Proceedings of the 2nd ACM Workshop on Security of Adhoc and Sensor Networks, Washington, DC, USA, 25–29 October 2004; pp. 66–77.
35. Li, D.; Liu, C.; Du, Y.; Han, X.; Chao, H. Artificial Intelligence with Uncertainty. *J. Softw.* **2004**, *15*, 1583–1594.