# Uncooperative Localization Improves Attack Performance in Underwater Acoustic Networks

Xiaoyan Lu, Michael Zuba, Jun-Hong Cui and Zhijie Shi
Department of Computer Science and Engineering,
University of Connecticut, Storrs, Connecticut 06269

***Abstract*—Underwater Acoustic Networks (UANs) have become a focus of interest for emerging scientific research and military applications. Recent work has shown that performance of existing security attacks are sensitive to network topology. In this paper, we utilize the mobility of Autonomous Underwater Vehicles (AUVs) to discover the topology of UANs by monitoring the broadcast patterns of geographic routing protocols. In this way, a mobile attacker can take advantage of the geographic information used in UANs to improve attack performance. We evaluate our approach in Aqua-Sim and results show that attack performance of jamming is significantly improved.**

***Index Terms*—Underwater Acoustic Networks, Localization, Security, Network Discovery**

## I. Introduction

Underwater Acoustic Networks (UANs) have gained a rapidly growing interest in the last decade. In UANs, distributed sensor nodes are deployed over vast spatial environments and linked together using acoustic communication. UANs can be utilized in applications such as underwater scientific exploration, commercial exploration and coastline protection. Since security is important in many applications, attack schemes and corresponding protection schemes towards UANs have been proposed in recent years. These works have shown that UANs are vulnerable to many types of attacks, including jamming attacks, wormhole attacks, and spoofing or cheating attacks, whereas performance of these attacks is not guaranteed if the network topology is unknown.

Exposing the network topology to malicious parties can help them to disrupt the network services or reduce the quality of services. For example, if the network topology is exposed to an mobile jammer, like an AUV, the jammer can choose the most critical node to jam and achieve global optimal attack performance. We elaborate on this potential attack with an example shown in Figure 1. Sensor nodes will use multicast communication to forward monitoring data from bottom to sink nodes on the surface. Due to sparse deployments, some nodes are likely to become bottlenecks of the network because they have to forward packets of many other nodes. Here, Node A, B, C, D, and E rely on node G, which is the bottleneck, to forward packets to sink nodes. If node G suffers from a jamming attack or has already been comprised, most of the packet delivery process will be terminated and data will never reach the sink node. If the network topology can been detected by an attacker, critical nodes like G, could be exploited. This makes the network vulnerable to security attacks. Attack performance on UANs can be significantly improved if the topology of UANs could be discovered by malicious adversary.

In this paper, we propose an uncooperative localization approach known as **L**ocalization of underwater sensor **N**odes via **T**ime **I**nterval (**LNTI**) which can efficiently localize sensor nodes by passively receiving underwater acoustic signals and detect complete network topologies through knowledge of forwarding sequences. During the process of network exploration, the mobile attacker, an AUV in our work, does not send any signals itself and silently listens to the broadcasts of nearby nodes. With this approach, an AUV maintains a low possibility of detection from network nodes. We then propose **P**acket-**D**elivery-**R**atio-based **D**etecting (**PDRD**), an approach that optimizes the movement path of a mobile attacker to minimize travel distance. LNTI can also be used to increase the effectiveness of various security attacks, such as jamming attacks. LNTI demonstrates how an attacker can gain network topology information in threat models to improve performance.

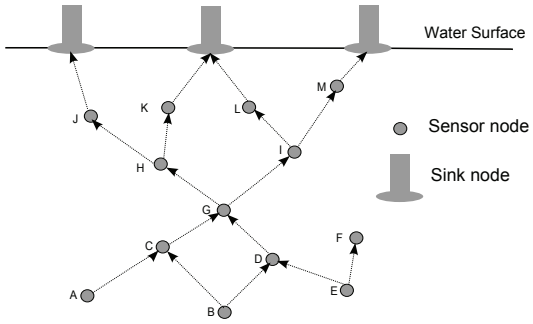


Fig. 1. Sample Network Topology

We use Aqua-Sim [1], a commonly used underwater acoustic network simulation tool based on ns-2, to validate the feasibility and accuracy of our approach. In addition, we analyze the possible range of error in the localization process caused by AUV self-localization deviation and error accumulation phenomenon in various node layouts.

Our contributions in this paper are as follows:

- A novel uncooperative localization scheme, known as LNTI, to localize nodes and detect network topologies in a passive manner by use of an AUV;
- An improved movement scheme for an AUV attacker based on packet delivery ratios, known as PDRD; and
- Show that existing security attacks, such as jamming attacks, are improved with use of LNTI.

The paper is organized as follows. Section II presents related work in underwater localization. In Section III we propose LNTI, a novel localization scheme to localize and detect network topologies. Section IV provides evaluation results of LNTI through simulations and attack approaches, such jamming attacks are also evaluated using LNTI. Finally

Section VII provides our conclusions and future work.

## II. Related Work

### A. Localization in UANs

Underwater localization can be classified into two categories: ranged based schemes and range-free schemes. It has been shown that the underwater power loss model makes RSS-based estimations ambiguous and that Doppler shift, which is introduced by node mobility, affects Angle-of-Arrival (AoA) algorithms [2]. Further, Time of Arrival (ToA) and Time Difference of Arrival (TDoA) have been proven to be more reliable when trying to obtain distance estimations. Therefore, range based localization schemes are regarded as the more feasible approach. In ranged based schemes, beacon messages are used for calculating ToA and TDoA in communication among sensor nodes. Recent work [2]–[7] requires interaction between the to-be-localized nodes and anchor nodes via beacon messages. Work in [8] proposed a method in which AUVs work together with sensor nodes to localize nodes. This requires cooperation between anchor nodes and AUVs.

However, cooperative localization via beacons is not feasible to use in attack scenarios where the attacker is trying to discover the network. First, sensor nodes are likely to encrypt messages for security concerns. An AUV attacker cannot obtain any information by listening to encrypted messages. Second, sensor nodes will not respond to messages sent by the AUV. If an AUV attacker broadcasts a probing packet to one node, this packet is likely to be identified as packet from an unauthorized source. Then the network can report such potential attack attempt. Therefore, proposed cooperative localization cannot be applied to attack schemes. This motivates us to adopt uncooperative localizing schemes. In Section III, we propose one such approach to localize nodes and detect the network topology. Our approach allows an AUV attacker passively listen to the network and localize sensor nodes. Even with encryption, our approach can still discover network node locations.

### B. Geographic Routing

Depth-Based Routing (DBR) [9] is one of the pioneering works in underwater geographic routing. In DBR, nodes are equipped with a pressure sensor to determine their depth information. Using this information, DBR makes use of opportunistic routing to broadcast packets to all neighbors. Upon receipt of a packet, each node will check its depth with the depth of the previous sender, which is encoded in the packet. If the current node's depth is higher (physically) than the encoded depth, the node will forward the packet at the end of a holding time. Once the optimal node forwards the packet, other nodes who receive this packet will drop the packet since an optimal node has already forwarded the packet. The feasibility of water depth sensing, high packet delivery ratios and adaptability to network mobility makes DBR a competitive protocol. However, DBR is a greedy protocol and can result in void zones. A void zone is when a packet gets forwarded to an area in a local maxima and no path out of the area exists. Consequently, sink nodes on the surface will not receive these packets, which impacts packet delivery ratio.

### C. Vulnerabilities of UANs

Recent works [10]–[14] call attention to threats from external attacks. Additionally, AUVs have been proposed to move into deployment areas and attempt to locate bottlenecks in UANs. A well-designed attack through jamming UAN modems was proven to be effective through the use of real-world experiments [10]. Further, work in [14] proposed an attack model that sends spoofed packets to specific nodes to terminate packet delivery. However, performance of these attacks mainly depends on the attack location. In [14], at least 90% of the packet delivery is likely to be terminated if launched at an appropriate position. However, if the network topology is unknown and the AUV is randomly choose attacking locations, the performance is likely to be less effective at roughly 50% in most simulation cases. An AUV attacker passes through many attacking positions one-by-one to observe network transmissions. This is energy and time consuming. With node location and network topology obtained by an AUV attacker, this attack can cause much larger damage to the whole UAN.

## III. Localizing Nodes via Time Intervals

### A. Overview

LNTI is an uncooperative localization approach that can work on most UAN scenarios and protocols. In this work, we assume that the UAN is using a standard geographic routing protocol, namely DBR [9], that transmissions can be detected and that encryption is not used or has already been compromised. **It is important to note that our approach still works if these two assumptions are removed. We will discuss this in detail in Section III-E.** LNTI intends to integrate multiple sources of information to obtain localization of sensor nodes and the network topology. The output of LNTI is the location of sensor nodes and topology. The network topology is discovered by observing the forwarding paths between nodes and is important to help improve attack performance.

To formalize the problem, assume there are a total of $n$ nodes deployed in the network and node $i$ is located at $P_i = (x_i, y_i, z_i)$ where the 3-D coordinate system is illustrated by Figure 2 and the z-axis is the vertical depth. If node $i$ sends a packet to node $j$ and node $j$ is the intended next hop, we call node $j$ a forwarder of node $i$. We can then formalize the network topology by a set $E = \{(i,j)|$ *where node j is the forwarder of node i*$\}$. The formalized output of LNTI is:

$$OUTPUT : P_1, P_2, ...P_n, E \tag{1}$$

In order to obtain the above output, our analysis has **three** main methods. First, we make use of information embedded into the packet header by the routing protocol. Geo-routing protocols place the sender's depth information into the packet header and can also contain other location information such as locations of the original sender and intended destination [9], [15]. A passive observer can then decode and read such information. Second, we assume that the location of surface buoys are known. Finally, the AUV attacker can utilize the traveling time (speed of sound in water, a known constant) for localization.

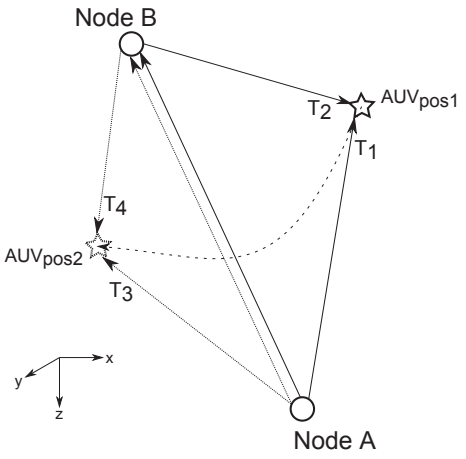


Fig. 2. One-Hop Scenario

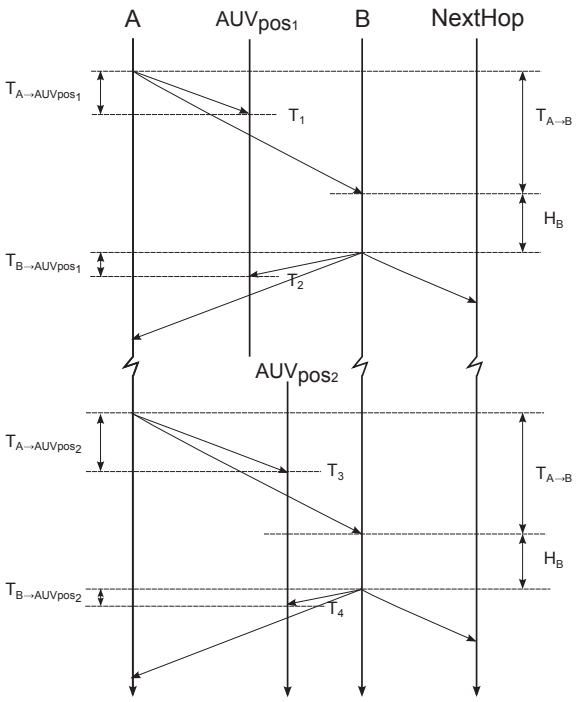


Fig. 3. Time Intervals

### B. Information in Packet Header

As mentioned earlier, geographic routing protocols might include location information in the packet header. Assume packet $m_1$ is transmitted from sender $s$ to receiver $r$ and packet $m_2$ is the packet forwarded from $r$ after replacing the depth information in packet, which used to be the depth of $m_1$. A passive attacker can read read the header of $m_1$ and $m_2$ and determine the following:

$$z_s = depth[s] \tag{2}$$

$$z_r = depth[r] \tag{3}$$

where $depth[s]$ is the depth of node $s$ and $depth[r]$ is the depth of node $r$. This was shown originally in [14].

### C. Localization Design

UANs are broadcast in nature and therefore many nodes will be applicable to forward a packet from a sender. However, in most cases, such as in DBR, selection constraints will try to enforce a single forwarder. Consider there is an AUV in the transmission range of both the sender and selected forwarder. This AUV will receive same the packet twice, once from the sender and once from the forwarder. The AUV is then able to calculate the time interval between reception of these two packets. This time interval is related to the relative 3-D positions between the sender, forwarder, and AUV. This relationship can be reflected by one mathematical equation with use of an on-board Inertial Measurement Unit (IMU) on the AUV. LNTI assumes in such mathematical equations that the coordinates of the sender and forwarder are unknown variables and the coordinates of the AUV are known variables. If the AUV moves to several different positions and collects enough time intervals, LNTI has enough independent equations to obtain the coordinates of the sender and receiver.

Consider the scenario in Figure 2 where sensor $B$ is the optimal forwarder of sensor $A$ and an AUV is in range of both nodes. Figure 3 illustrates a series of broadcasting events among sensor $A$ and $B$. Firstly, $A$ is broadcasting a data packet. After the propagation time $T_{A\to B}$, $B$ receives the packet from $A$. This packet is also detected by the AUV, who is silently listening at location $pos_1$. The time that the AUV receives this packet is $T_1$. $B$ is the optimal forwarder of $A$ with depth $d_B$ and has the shortest hold time $H_B$. Node $B$ then forwards the packet and the AUV will be able to receive this packet at time $T_2$.

From the packet perspective, after being sent by sensor $A$, the AUV will receive this packet after the following periods. First, $T_{A\to B}$, the propagation time between sensor $A$ and sensor $B$. Second, the hold time $H_B$ during which this packet was queued in sensor $B$. Third, $T_{B\to AUV_{pos_1}}$, the propagation time between sensor $B$ and the AUV attacker, which depends on the where the AUV is positioned. The amount of time is: $T_{A\to B} + H_B + T_{B\to AUV_{pos_1}}$. At the same time, sensor $A$ will also directly send this packet to the AUV attacker. Without forwarding, this period only last $T_{A\to AUV_{pos_1}}$, which is propagation time between sensor $A$ and AUV attacker.

The AUV is equipped with an embedded inertial clock that records the time when it receives the same packet for both times, which are $T_1$ and $T_2$ respectively. The AUV can calculate the time difference by using the following:

$$T_2 - T_1 = T_{A\to B} + H_B + T_{B\to AUV_{pos_1}} - T_{A\to AUV_{pos_1}} \tag{4}$$

After receiving a pair of packets with same data from nodes $A$ and $B$, the AUV will begin to move from it's original position $pos_1$ to another location $pos_2$. In order to stay in the transmission range of node $A$ and $B$ with high probability, the AUV will only cover a short distance. Since the packet forwarding on node $A$ and $B$ is unpredictable, the AUV will wait at $pos_2$ until the above forwarding sequence is repeated. The AUV receives a packet from node $A$ and $B$ at $T_3$ and $T_4$. We assume that the propagation time $T_{A\to B}$ and the holding time $H_B$ remain the same. Again, we have the following:

$$T_4 - T_3 = T_{A\to B} + H_B + T_{B\to AUV_{pos_2}} - T_{A\to AUV_{pos_2}} \quad (5)$$

We then subtract Equation 5 by Equation 4 and multiply the speed of sound in water on both sides. This provides us with the following:

$$[(T_4 - T_3) - (T_2 - T_1)]V_{speed} = [D_{B\to AUV_{pos_2}} - D_{B\to AUV_{pos_1}}] + [D_{A\to AUV_{pos_1}} - D_{A\to AUV_{pos_2}}] \quad (6)$$

where $V_{speed}$ is the speed of sound underwater, $D_{B\to AUV_{pos_1}}$ is the distance between $B$ and $pos_2$, $D_{B\to AUV_{pos_2}}$ is the distance between $B$ and $pos_2$, $D_{A\to AUV_{pos_1}}$, $D_{A\to AUV_{pos_2}}$ are the distance from $A$ to $pos_1$, $pos_2$ respectively. Since the AUV has calculated the location of node $B$ and the IMU provides the AUV with its location. The value of $D_{B\to AUV_{pos_2}} - D_{B\to AUV_{pos_1}}$ is then obtainable. In this way, after staying in two positions, the AUV will be able to calculate the value of $D_{A\to AUV_{pos_1}} - D_{A\to AUV_{pos_2}}$ by Equation 6. With consequent movement, the AUV receives packets at $pos_1$, $pos_2$,...$pos_n$ at a total of $n$ different positions. Consequently, the AUV collects a series of independent equations as follow:

$$D_{A\to AUV_{pos_i}} - D_{A\to AUV_{pos_{i+1}}} = \sqrt{(x_A - x_i)^2 + (y_A - y_i)^2 + (z_A - z_i)^2} - \sqrt{(x_A - x_{i+1})^2 + (y_A - y_{i+1})^2 + (z_A - z_{i+1})^2} \quad (7)$$

where $i = 1, 2, .., n-1$, $x_A, y_A, z_A$ are the locations of node $A$ under the axis system illustrated by Figure 2, $(x_j, y_j, z_j)$ are the coordinates of position $j$ where $j = 1, 2...n$. With $n$ larger than 3, $x_A, y_A, z_A$ can be solved. If $n \geq 4$, the AUV will use the first three equations to solve $x_A, y_A, z_A$ and the other equations can be used to improve the accuracy of this solution.

On-demand packet forwarding may cause collisions in the receiving stage of nodes and the AUV. However, $T_1$, $T_2$, $T_3$ and $T_4$ are short time intervals, and DBR utilize an implicit Clear-To-Send. The AUV can hardly face such collisions and once it receives such a pair of packets, the AUV can assume that node $B$ is the optimal forwarder of node $A$ with high probability. In Section IV we show that collisions have little influence on our scheme.

While moving from one position to the another, an acoustic modem equipped onto an AUV will stay in listening mode. Once a pair of packets from node $A$ and $B$ are received, the AUV can keep recalculating the coordinates of $A$ and compare them with the initial obtained result. If the Euclidean Distance between the refreshed location and the former location is beneath a predefined threshold, the AUV will update the location of node $A$ by averaging these two results.

Considering the mobility of underwater sensor nodes, the AUV attacker will be able to track the movement of sensor node A before moving out of the transmission range of sensor A and B. In relative constant environment, this mechanism will increase accuracy of the result. We note that in our work, we do not explicitly consider mobile nodes.

After detecting the location of node $A$, the AUV will move beneath $A$ and localize the node which forwards packets to $A$. By doing this recursively, the path of network traffic formed by optimal forwarders can be detected. However, in dense deployments, a data packet may be forwarded through multiple routes. In order to detect the topology of the whole network with minimal energy consumption, the AUV should not detect these paths one by one. In Section III-D, we propose a parallel detection approach for the AUV.

### *D. Attack Movement Strategy*

A movement strategy for underwater attackers was originally introduced in [14]. This algorithm finds a good attacking position by passively listening for packet transmissions along planes in the network. If only one position in the plane has network traffic, the attacker has found a bottleneck. Without information of network topology, the attacker has to pass through all possible positions in an exhaustive manner. In this section we propose an improved movement algorithm, known as Packet-Delivery-Ratio-based Detection (PDRD), for an attacker to move smartly for network discovery. By minimizing the movement distance, the time for exploring the entire network topology is reduced and energy is significantly saved.

*1) Overview:* PDRD calls LNTI as a sub-process in localizing sensor nodes. We assume that the locations of the gateway or buoy nodes are known. This assumption is realistic as these nodes sit above the water surface and can be located with satellite or ship surveillance. With the knowledge of buoy node locations, the AUV attacker swims directly towards the nearest sink from its launching location. After the AUV attacker arrives at the area under this sink node, LNTI will be run to detect communication with this sink. LNTI provides the locations of a pair of senders and inserts their locations into a *Position Table*. The position table stores the 3-D axis positions of nodes. The AUV attacker will choose one optimal node from the position table using an estimation function. Then the AUV will swim underneath this optimal node and use LNTI to localize with all nodes that are sending packets to this optimal node. This process can then be repeated to discover the rest of the network.

*2) Packet-Delivery-Ratio-based Detecting (PDRD):* Through passively listening to the acoustic channel, the AUV attacker can count the packet delivery ratio. Figure 4 illustrates a sample sub-graph of a UAN. The packet delivery ratio over each link among nodes is illustrated by a number. Each node will send out data generated by local sensors and forward data received from other nodes. The PDR of the receiver can generally represent the importance of a node as a larger packet delivery ratio implies that this node forwards or sends more packets than others. The attacker intends to move towards such nodes first because these nodes could be potential bottlenecks. For example, in Figure 4, assuming the AUV has localized node $A$ and $C$, it should then make a decision as to which node to swim towards. The link between $A$ and $B$ has a larger PDR than the link between $C$ and $B$. This implies that node $A$ is a forwarder of more nodes than node $C$. In order to discover more nodes, the AUV should swim to node $A$. To obtain the priority of nodes for localization, we define the estimation function $f(N_i)$ as

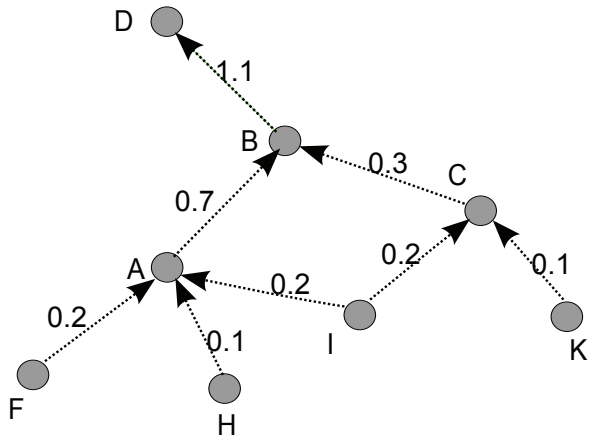


Fig. 4. A Packet Delivery Ratio Distribution

Equation 8 where the PDR of $N_i$ as receiver is $PDR_{N_i}$ and $Dist_{N_i}$ is the moving distance from the AUV to node $N_i$.

$$f(i) = \frac{PDR_i}{Dist_{N_i}} = \frac{PDR_i}{\sqrt{(x_{AUV} - x_i)^2 + (y_{AUV} - y_i)^2 + (z_{AUV} - z_i)^2}} \quad (8)$$

The Packet Delivery Ratio based Detection (PDRD) Algorithm can be seen as follows, where $SINK$ is the set of sink nodes:

1: **for all** $s \in SINK$ **do**
2: $PT \leftarrow PT \cup \{s\}$
3: **end for**
4: **while** $PT \neq \emptyset$ **do**
5: **for all** $i \in PT$ **do**
6: $f_i \leftarrow \frac{PDR_i}{\sqrt{(x_{AUV}-x_i)^2+(y_{AUV}-y_i)^2+(z_{AUV}-z_i)^2}}$
7: **end for**
8: $target = \min_i \{f_i | i \in PT\}$
9: AUV swims to area under node $target$
10: Call LNTI Process
11: **for all** Node $j$ localized by LNTI **do**
12: $PT \leftarrow PT \cup \{j\}$
13: **end for**
14: $PT \leftarrow PT \setminus \{target\}$
15: **end while**

### *E. Discussion*

LNTI allows an AUV attacker to discover the network topology in different scenarios. Our simulation in Aqua-Sim assumes that no packet encryption is used and that buoy/gateway node locations are known. However, LNTI can still perform well without these assumptions. First, let us assume there is packet encryption in the network layer. LNTI can use at least 3 equations in Equation 7 instead of 2 to obtain the horizontal coordinates and depth coordinates. Further, if the buoy or gateway node's location is unknown, the AUV attacker can use at least 6 equations in Equation 7 to obtain the 3-D coordinates of both the sender and receiver. In order to obtain more equations, the AUV must move to more locations. Therefore, without these two assumptions, the AUV attacker will consume more energy and provide a slightly less accurate solution. From a pure mathematical aspect, LNTI can still use 7 to obtain node locations and detect the network topology.

Another item to note is that LNTI does not work with nondeterministic holding times. This is because LNTI relies on Equation 7 which is obtained by eliminating the deterministic holding time. In DBR based protocols, the holding time is determined by a linear equation using the depth difference between the sender and receiver, which are static values. Other protocols that forward a packet with no holding time can also be treated as deterministic holding times and still work with LNTI. Nondeterministic or random hold times can prevent LNTI from discovering network topology and can be considered as one feasible protection against LNTI. However, nondeterministic hold times are likely to make MAC protocol design challenging. In RTS/CTS-based MAC protocols, after RTS/CTS signal exchanges, the data channel has to be occupied for a nondeterministic period time. Therefore neighboring nodes are blocked from accessing this channel for more time and the end-to-end delay is increased. In scheduling-based MAC protocols, a nondeterministic schedule has to be determined among neighboring nodes. This requires a more complex scheme to output collision-free schedules because nodes are not able to always use the next continuous available time slot.

TABLE I
DEPLOYMENT SETTINGS

| ID | Position | Type |
|---|---|---|
| 1 | $(0, 0, 0)$ | Buoy node on sea surface |
| 2 | $(200, 110, -800)$ | Normal Underwater Sensor Node |
| 3 | $(200, 310, -1600)$ | Normal Underwater Sensor Node |
| 4 | $(510, 210, -2400)$ | Normal Underwater Sensor Node |
| 5 | $(520, 520, -3200)$ | Source Node generating data packet |

## IV. PERFORMANCE EVALUATION

In this section, we evaluate the performance of LNTI under different network settings. All simulations are conducted in Aqua-Sim [1], a professional underwater network simulator based on ns-2. This simulator considers the dynamic nature of the underwater acoustic channel and can accurately simulate network conditions. Additionally, we also perform simulations in C++ to evaluate the jamming attack performance with LNTI and improvement on moving distance of PDRD.

### *A. A Sample of LNTI*

Here we present a sample to demonstrate the feasibility of LNTI. The speed of the AUV attacker is set to be 6 m/s. The transmission range of both the AUV and sensor nodes is 1500 meters. There is a sensor deployed on the seabed with a depth of 3200 meters that generates data packets with a rate of 0.1 data packets per second. All sensor nodes are deployed in static positions. The locations and types of every sensor node are listed in Table I.

Under the same coordinate system as Figure 2, the AUV is initially deployed at $(-200, -180, 300)$. The AUV attacker will start to move until it receives the first pair of packets. After being in several locations and receiving packets, the AUV attacker manages to calculate the position of sensor node 2, 3

TABLE II
LOCALIZATION PROCESS OF AUV ATTACKER

| Packet ID | Total Time (s) | Hanging Time (s) | Moving Time (s) | Sender ID | AUV status |
|---|---|---|---|---|---|
| 0 | 15.55 | 15.55 | 0 | 2 | Wait at $(-200, -180, 300)$ |
| 0 | 19.69 | 19.69 | 0 | 1 | Move to $(-90, -0.98, -300)$ |
| 1 | 60.39 | 25.48 | 34.91 | 2 | Wait at $(-90, -0.98, -300)$ |
| 1 | 64.54 | 29.63 | 34.91 | 1 | Move to $(75, -110, -400)$ |
| 2 | 107.14 | 35.400 | 71.73 | 2 | Wait at $(75, -110, -400)$ |
| 2 | 111.44 | 39.70 | 71.73 | 1 | Localize Node 2 successfully. Move to $(300, 210, -1000)$ |
| 3 | 235.95 | 45.20 | 190.75 | 2 | Wait at $(300, 210, -1000)$ |
| 3 | 240.84 | 50.08 | 190.75 | 1 | Move to $(20, 0, -1100)$ |
| 4 | 302.36 | 51.11 | 251.24 | 3 | Wait at $(20, 0, -1100)$ |
| 4 | 306.52 | 55.28 | 251.24 | 2 | Move to $(275, 0, -1200)$ |
| 5 | 357.80 | 61.05 | 296.75 | 3 | Wait at $(275, 0, -1200)$ |
| 5 | 362.07 | 65.32 | 296.75 | 2 | Move to $(300, 210, -1000)$ |
| 6 | 416.24 | 71.12 | 345.12 | 3 | Wait at $(300, 210, -1000)$ |
| 6 | 420.32 | 75.20 | 345.12 | 2 | Localize Node 3 sucessfully. Move to $(220, 0, -1900)$ |
| 7 | 586.08 | 86.82 | 499.26 | 4 | Wait at $(220, 0, -1900)$ |
| 7 | 590.26 | 90.99 | 499.26 | 3 | Move to $(275, 200, -2000)$ |
| 8 | 634.21 | 96.68 | 537.52 | 4 | Wait at $(275, 200, -2000)$ |
| 8 | 638.51 | 100.99 | 537.52 | 3 | Move to $(300, 410, -1800)$ |
| 9 | 692.67 | 106.77 | 585.89 | 4 | Wait at $(300, 410, -1800)$ |
| 9 | 696.76 | 110.87 | 585.89 | 3 | Localize Node 4 successfully |

and 4. Without any interference in the channel and assuming the speed of sound underwater is uniformly 1500 m/s in the target area, we have found that the AUV attacker can localize every sensor perfectly with 100% accuracy. The status of the AUV attacker in every step is listed in Table II. From this localization sample we can observe that the AUV attacker can localize sensors via time intervals without identifying packet contents or transmitting any probe packets.

### B. Metrics and Methodology

In a constant and ideal environment, the AUV attacker can resolve the location of every sensor with 100% accuracy. Now the major focus is how well LNTI works in a more realistic scenario where errors occur and need to be considered. In location sensitive attacks, like jamming attacks, effects of localization errors in LNTI have an impact on attack effectiveness. To make sure such effect will not influence attack enhancement by LNTI, we have conducted simulations in more realistic scenarios to measure localization error. In terms of localization error, the impact from the dynamic underwater environment is one of the major attributes. The AUV attacker relies on Equation 7 to calculate the position of sensor nodes. However, the speed of sound may vary with depth and temperature of the water. It is impossible for the AUV to monitor the exact speed of sound in a timely manner. The use of high performance IMUs can also incur errors during the self-localization process when the movement distance is high. Further, compounded errors could occur during the localization process because the AUV attacker uses the solution of the optimal forwarder's position to localize other nodes. In this section, we use simulation results to analyze how the AUV attacker handles these errors and provide an accuracy measurement.

*1) Impact of AUV's self-localization capability:* Specific test methods are as follows: dynamically generate possible layouts of a pair of nodes in the water. Assume the AUV attacker already obtained the location of the lower node but does not know its accurate location. This is due to moving for a long distance underwater in which the IMU unit in the AUV attacker may accumulate errors. LNTI is used to calculate the location of the deeper node in each layout. The solution obtained by the AUV attacker is compared with the correct position to obtain the deviation distance.

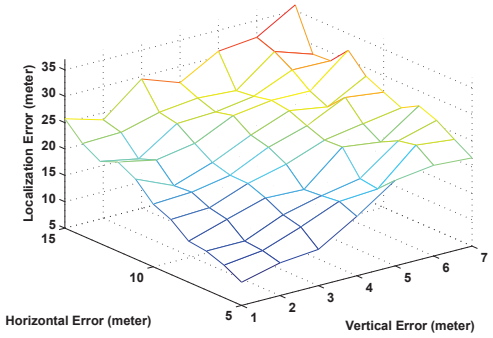


Fig. 5. Error in One-Hop Scenario

Figure 5 illustrates how the performance of LNTI is influenced by the AUV attacker's self-localizing capability. The x-axis stands for the deviation of the AUV's self-localization in a horizontal direction and the y-axis stands for deviation in vertical direction. In the horizontal plane, the deviation range is set from 5 meters to 15 meters and in vertical direction, deviation caused by the depth sensor in AUV is from 1 meter to 7 meter. The z-axis presents the corresponding deviation distance in localizing the deeper node. For every integrity value of the AUV's self-localizing error in the x,y-axis and z-axis, the deviation distance is measured under 100 different randomly generated layouts to obtain the average value.

From Figure 5, it shows the deviations of AUV's self-localizing in the horizontal plane and vertical direction and the direct impact on LNTI localization. The impact of the horizontal deviation is more significant. In general, the deviation distance between the solution and the correct answer is between $[10, 25]$ meters.

*2) Impact of Error Accumulation:* Besides analyzing the impact of the AUV's self-positioning capability, it is also required to analyze the cumulative error after continuously detecting multiple pairs of nodes. This is due to the fact that LNTI must calculate the position of the optimal forwarder's position as pre-known condition before LNTI can localize a node. Therefore, if a deviation exists in localizing the optimal forwarder, then there must be an error in localizing this node. Unfortunately, this effect will continue to accumulate errors on a hop-by-hop basis. Therefore, the more nodes the AUV localizes, the larger the positioning error.

Figure 6 shows a more detailed analysis of the error-accumulation effect. The x-axis stands for deviation distance between the optimal forwarder's location and the AUV-calculated result in the horizontal plane. The y-axis stands for the deviation distance between the optimal forwarder's location and the AUV-calculated result in the vertical direction.

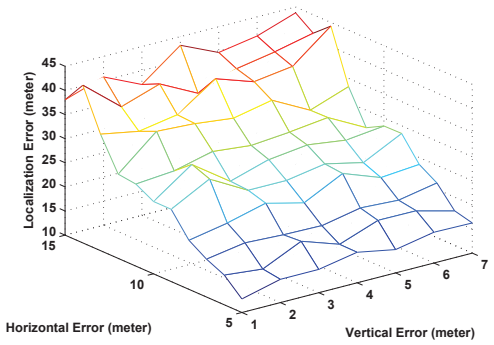


Fig. 6. Error in Multi-Hop Scenario

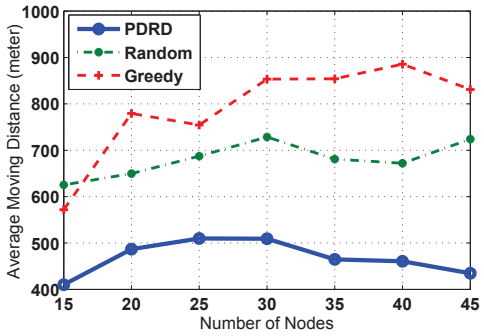


Fig. 7. Average Moving Distance in Localizing per node

In the horizontal plane, the deviation range is set to be 5-15 meters and in the vertical direction, deviation caused by the depth sensor in the AUV is 1-7 meters. The z-axis stands for the absolute deviation distance of the result. It shows in normal cases where the AUV localizes a sensor hundreds of meters deeper than itself with horizontal error less than 10 meters, the accumulated error is no more than 30 meters. This is in an acceptable range for applications in water no more than 3000 meters because data could be transmitted to the water surface in several hops. In addition, it shows the localization result is more sensitive to the optimal forwarder's deviation in the horizontal plane.

In Figure 6, the reason that the vertical error has no influence on localization is because the AUV attacker can obtain accurate depth information from the packet header. Therefore, the AUV attacker uses this information instead of the result from solving the associated equation. Compared to the vertical error, the horizontal error has more significant impact.

Assume that the average transmission depth of two nodes is 1000 meters. Through the localization process running four times, in order to localize the position a sensor node with depth of 5000 meters, the worst deviation distance is at 120 meters. This is indeed a considerable error. However, if the AUV can guarantee a better positioning capability, each node can be positioned on a horizontal plane of a distance not more than 5 meters, then locate one. The same node, 5000 meters underwater, will have an error of 60 meters. Accuracy of the AUV's self-positioning plays an important role on the result accuracy.

*3) Estimated Power Consumption:* Although advances in propulsion and energy storage technology have led to the increasing endurance of AUV methods [16], an AUV should try to save power in the attacking tasks. Especially when considering the complexity of the underwater environment and the limited time for finishing a task. If the AUV runs out of power, then it can not swim back to the base to report any information it obtained. This leads to failure of the whole task. Another consideration is the time limitation in finishing such a task. The time duration of detecting the network topology is an important indicator for performance of LNTI in potential sensitive detection applications. Based on the above consideration, this section presents an estimation on energy consumption of LNTI by counting the amount of travel distance of LNTI.

Based on the moving strategy in Section III-D, we measured the moving distances of an AUV in different network topologies. The specific experimental method is as follows: with a given number of underwater sensor nodes and floating buoy nodes, different water spaces are used for randomly deployment which consequently leads to different deployment densities. We then calculate the average distance the AUV covers before localizing all the underwater nodes. In the process of network topology generation, cross section of the deployment water is always rectangular and coordinates of the network nodes are subject to normal distribution.

In a 1000x1000x1000 $meter^3$ square water space, the relation between moving distance and the number of nodes is illustrated in Figure 8. DBR is the protocol assumed to run here with a transmission range of 600 meters. We randomly generate the network topology by assigning each node a random location. If a node cannot forward to a buoy node, it will be deleted by the simulator. After deleting all the nodes not connected to buoy nodes, the simulator starts to count the number of remaining nodes. This is to make sure that nodes are all deployed at locations where they can forward packets to a buoy node. It is more similar to real-world case and helps maintain network connectivity. The z-axis stands for the moving distance, the x-axis is for the underwater nodes and the y-axis is for buoy nodes. The moving distance increases roughly proportionally with the number of nodes. Since PDRD assumes buoy nodes have been localized, the number of underwater nodes has a more dominate influence on moving distance.

Figure 9 illustrates the simulation result of a network that consists of 3 buoy nodes and 15 underwater nodes. The x-axis stands for the depth of the sensor deployment space and the y-axis is for side length of the square cross-section. The moving distance is represented by the z-axis. It shows that the moving distance is generally proportional to the side length of the cross-section of the deployment space. The larger the cross-section area of the deployment space is, the longer the AUV attacker should move.

Based on the simulation result, it can be concluded that network density and deployment space both have influence on the moving distance of the AUV.

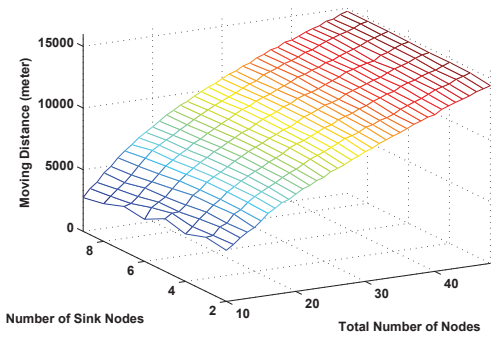


Fig. 8. Simulation results of Distance

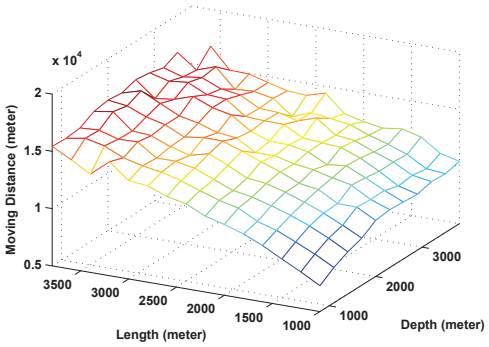


Fig. 9. Simulation results of Distance

*4) Jamming Attack Enhancement by LNTI:* In order to evaluate how LNTI increases the attack performance, we have run extensive simulations using jamming attacks. A jamming attack is capable of physically interrupting the reception of underwater signals. The AUV attacker can estimate the acoustic channel and then broadcast a jamming signal to the receiver. Therefore the receiver is not able to decode the packet or communicate with the sender. Jamming different nodes has a different impact on the whole network. In UANs, since RF radio is only equipped on buoy nodes, only these buoy nodes can communicate with an offshore data center. Every underwater node must forward packets to the buoys node otherwise the offshore data center can not receive the data. One node is likely to have multiple routes to the buoy node, depending on the scheme that is applied in the network layer. However, these routes may share some common nodes as forwarders. If we consider the example from Figure 1 again, we know that jamming these bottleneck nodes will produce the most damage.

However, if the AUV attacker has no information about network topology, it is difficult to find these critical nodes. The AUV attacker has to randomly select a jamming location. On the contrary, the LNTI approach provides the AUV attacker with locations of sensor nodes and the network topology. Thus, the AUV attacker can select a critical node to jam which leads to the maximum number of nodes the become isolated.

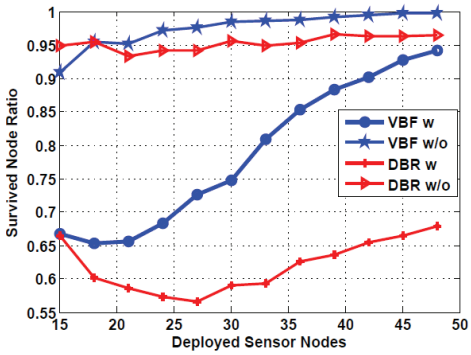


Fig. 10. Survival Rate during Jamming

Compared with randomly jamming a node, LNTI significantly increase attack performance.

In a 1000x1000x2000 $meter^3$ water space, we conduct simulations on each deployment density with randomly generated node locations for 500 runs. The transmission range of nodes and the AUV attacker is 600 meters. Each node has a packet rate proportional to its depth (i.e. 0.0005*depth) such that buoy nodes with depth 0 do not send packets and nodes with depth 2000 meter have a packet rate of 1 packet/sec. In Figure 10 we illustrate how LNTI increases the jamming performance. The x-axis is the number of underwater nodes (minus the 3 buoy nodes) deployed. The y-axis shows the proportion of surviving nodes which are able to send packets to buoy nodes. We adapt VBF [15] and DBR, two classic UAN geo-routing protocols to test the improvement of the attack using LNTI. The VBF protocol sets the Vector Radius to 300 meters and each node sends a packet three times, setting each of the three buoy nodes as the destination each time. The DBR protocol uses depth information to forward packets to a random buoy node. If the AUV attacker randomly selects a jamming location, 95% of the nodes can still send packets to buoy nodes. The jamming does not cause large damage to the network. However, with LNTI, only 65% of nodes survive if the number of deployed nodes is less than 22. With the growth of the number of deployed nodes, random jamming has no significant influence. The VBF protocol, with its multipath properties for routing each packet, almost suffers no damage. On the contrary, jamming with LNTI makes only 60% of the nodes in the VBF protocol functional. However, the VBF protocol suffers less in dense deployments. This is because many paths exist to the buoy nodes and a single attacker can not stop them all.

In protocol design, we should consider that multipath routing can help reduce damage caused by jamming attacks. Every node, instead of having one static forwarder, should have multiple dynamic forwarders. This approach will improve network robustness by reducing the number of critical nodes.

## V. Conclusion

In this paper we have presented an uncooperative localization approach, known as LNTI, for UANs. This approach is capable of localizing network nodes passively in a network and obtaining the network topology of the deployment area. This information can be used to improve the attack performance of various security attacks, such as jamming attacks and spoofing attacks. Further, we have proposed an improved AUV

attacker movement scheme, known as PDRD, to move the AUV efficiently while detecting the network topology. Finally, we show that using LNTI a malicious attacker can improve its attack performance. We have shown this through applying LNTI to jamming attacks.

## ACKNOWLEDGMENT

This work is supported by the U.S. National Science Foundation (NSF) under Grant No. 1228936. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

## REFERENCES

[1] P. Xie, Z. Zhou, Z. Peng, H. Yan, T. Hu, J.-H. Cui, Z. Shi, Y. Fei, and S. Zhou, "Aqua-Sim: An NS-2 Based Simulator for Underwater Sensor Networks," in *Proc. of MTS/IEEE OCEANS*, 2009.

[2] X. Cheng, H. Shu, and Q. Liang, "A Ranged-Difference Based Self-Positioning Scheme for Underwater Acoustic Sensor Networks," in *Proc. of the International Conference on Wireless Algorithms, Systems, and Applications (WASA)*, 2007, pp. 38–43.

[3] Z. Zhou, Z. Peng, J. Cui, Z. Shi, and A. Bagtzoglou, "Scalable Localization with Mobility Prediction for Underwater Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 3, pp. 335–348, 2011.

[4] Y. Zhang and L. Cheng, "A Distributed Protocol for Multi-hop Underwater Robot Positioning," in *Proc. of IEEE International Conference on Robotics and Biometrics (ROBIO)*, 2004, pp. 480–484.

[5] K. Chen, Y. Zhou, and J. He, "A Localization Scheme for Underwater Wireless Sensor Networks," *International Journal of Advanced Science and Technology*, vol. 4, pp. 9–16, March 2009.

[6] M. Erol, L. F. M. Vieira, and M. Gerla, "Localization with Dive'N'Rise (DNR) beacons for underwater acoustic sensor networks," in *Proc. of the 2nd ACM Workshop on Underwater Networks (WUWNet)*, 2007.

[7] P. Carroll, S. Zhou, H. Zhou, X. Xu, J.-H. Cui, and P. Willett, "Underwater Localization and Tracking of Physical Systems," in *Journal of Electrical and Computer Engineering*, 2012.

[8] M. Erol, L. F. M. Vieira, and M. Gerla, "AUV-Aided Localization for Underwater Sensor Networks," in *Proc. of the International Conference on Wireless Algorithms, Systems, and Applications (WASA)*, 2007.

[9] H. Yan, Z. Shi, and J.-H. Cui, "DBR: Depth-Based Routing for Underwater Sensor Networks," in *Proc. of IFIP Networking*, 2008.

[10] M. Zuba, Z. Shi, Z. Peng, and J.-H. Cui, "Launching Denial-of-Service Jamming Attacks in Underwater Sensor Networks," in *Proc. of the 6th ACM International Workshop on Underwater Networks (WUWNet)*, 2011.

[11] M. Goetz, S. Azad, P. Casari, I. Nissen, and M. Zorzi, "Jamming-Resistant Multi-path Routing for Reliable Intruder Detection in Underwater Networks," in *Proc. of the 6th ACM International Workshop on Underwater Networks (WUWNet)*, December 2011.

[12] J. Kong, Z. Ji, W. Wang, M. Gerla, and R. Bagrodia, "On wormhole attacks in underwater sensor networks: A two-tier localization approach," in *UCLA Computer Science Department Technical Report 04005*, 2004.

[13] R. Zhang and Y. Zhang, "Wormhole-Resilient Secure Neighbor Discovery in Underwater Acoustic Networks," in *Proc. of the 29th IEEE International Conference on Computer Communications (INFOCOM)*, 2010.

[14] M. Zuba, M. Fagan, J.-H. Cui, and Z. Shi, "A Vulnerability Study of Geographic Routing in Underwater Acoustic Networks," in *Proc. of the First IEEE Conference on Communications and Network Security (CNS)*, 2013, pp. 245–253.

[15] P. Xie, J.-H. Cui, and L. Lao, "VBF: Vector-Based Forwarding Protocol for Underwater Sensor networks," in *Proc. of IFIP Networking*, 2006, pp. 228–235.

[16] G. Griffths, J. Jamieson, S. Mitchell, and K. Rutherford, "Energy storage for long endurance auvs," in *Proc. ATUV Conference, iMarEST*, 2004.