On Wormhole Attacks in Under-Water Sensor Networks: A Two-Tier Localization Approach

Jiejun Kong, Zhengrong Ji, Weichao Wang, Mario Gerla, Rajive Bagrodia
Department of Computer Science
University of California
Los Angeles, CA 90095
{jkong,jizr}@cs.ucla.edu,wangwc@cs.purdue.edu,{gerla,rajive}@cs.ucla.edu

Abstract

Under-Water Sensor Network (UWSN) is a novel networking paradigm to explore the uninhabited oceans. However, the characteristics of this new network, such as huge propagation delay, floating node mobility, and limited acoustic link capacity, are significantly different from land-based sensor networks. In this paper we show that underwater denial-of-service attack imposes great threats to any UWSN. Without proper countermeasures, underwater sensor networking is a mission impossible.

We propose a localization based approach to answer the challenge. In our design, DUB and DDB, a pair of efficient *single-round* distance measuring schemes, are critical building blocks to realize our approach inspite of constrained node capability and floating node mobility. In addition, to cope with low/medium node mobiltiy, we propose a *two-tier localization* scheme to identify short-range wormholes instantly, and long-haul wormholes within a limited latency. Our simulation and implementation confirm the effectiveness of our design.

I. INTRODUCTION

The still largely unexplored vastness of the ocean, covering about two-third of the surface of earth, has fascinated humans for as long as we have records for. Its currents, chemical composition, and ecosystems are all highly variable at different locations and times. Recently, there has been a growing interest in monitoring the marine environment for scientifi c exploration, commercial exploitation and coastline protection. The ideal vehicle for this type of extensive monitoring is a scalable Under-Water Sensor Network (UWSN), which employs large amount of distributed, unmanned, and untethered underwater sensor nodes to locally gather information in a timely manner. The self-organizing, self-reconfi gurable network provides better supports in sensing, monitoring, surveillance, reconnaissance, underwater control, and fault tolerance.

The new UWSN paradigm is signifi cantly different from any existing land-based sensor network. First, UWSN relies on low-frequency acoustic communications because RF radio does not propagate well due to underwater energy absorption. Unlike wireless links amongst land-based sensors, each underwater acoustic link features large-latency and low-bandwidth. Second, most sensor nodes in land-based sensor networks are typically stationary. But majority of underwater sensor nodes, except some fi xed nodes mounted on the sea fbor, are with low or medium mobility due to water current and other underwater activities. Furthermore, UWSN is different from any existing small-scale Underwater Acoustic Network (UAN) [40] [35] [44]. An UWSN is a scalable sensor network, which relies on localized sensing and coordinated networking amongst large amount of low-cost sensors. In contrast, an existing UAN is a small-scale network relying on data acquisition strategies like remote telemetry or sequential local sensing. Therefore, neither land-based sensor network nor UAN techniques can meet a wide variety of underwater application demands to implement a *localized, precise, and large-scale sensing technology in a time-critical environment.*

Unfortunately, any UWSN is vulnerable to security threats. First, there is no clear line of defense in a scalable UWSN. Acoustic sound travels faster and *longer* in water than in air. The tetherless underwater acoustic link is open to any node within a sizable transmission range. An adversary can either decide to function as an “invisible” observer to *passively* analyze intercepted acoustic messages, or choose to *actively* disrupt and deny data forwarding,

Part of the work is funded by MINUTEMAN project. Contract/grant sponsor: Offi ce of Naval Research. Contract/grant number: N00014-01-C-0016.

multi-hop routing, or any other network services. Second, it is nearly infeasible to implement adequate physical countermeasures to protect *all* unattended sensor nodes. A limited number of sensor nodes can be captured, compromised, and re-inserted into the self-organizing UWSN. Therefore, encryption and authentication schemes that rely on the secrecy of individual keys are not effective means to counter these compromised network members. Any uncompromised "good" node in an UWSN must be prepared to operate in a collaborative mode that seeks to overwhelm compromised "bad" nodes by secured multi-party protocols. Third, many sensor network schemes demand cooperative participation of distributed sensor nodes. Adversary can explore this prerequisite to attack the network. For example, all sensor network services seek to optimize performance by minimizing/maximizing certain pre-defined routing metrics (e.g., hop-count, latency, delivery ratio). The quality of any collaborative network service is devastated if an adversary can falsely cheat the network by lying or wormhole tunneling, then disrupting the service and reducing routing performance to minimum.

In this paper, we study security attacks threatening underwater networks. We show that, no matter what kind of protocol stack we are building, any UWSN can be disabled by underwater denial-of-service attacks due to the unique characteristics of underwater acoustic channel.

1) *Wormhole attack* imposes severe threat to self-organizing networks where route discovery must use certain best-effort metrics. Though wormhole attack is first studied by Hu et al. [20] for radio networks, it has great impact on underwater acoustic networks as well. A wormhole attacker can use two separated attacking nodes to achieve the "best" routing metrics via an out-of-bound "wormhole" channel available only to the attacker, then (selectively) drops data packets once the wormhole link is selected as part of ad hoc routes. We show that low-cost wormhole links in the form of wired links or radio links surpass acoustic links in both link capacity and propagation delay, hence attackers can pay little cost to effectively disable data communication in an underwater network. As a result, the underwater sensor nodes and the command center wrongfully assume that no report has been filed or no command has been issued.
2) Narrow-band jamming also imposes serious threat to underwater communication. We show that *jam-and-replay attacks* [12][11] can effectively disrupt localization protocols in underwater environment.

Our contribution is two-fold. On one hand, we illustrate the significant impact of these two denial-of-service attacks against underwater communication. The underwater network pays the overhead of development, deployment, maintenance, and communication, but the network fails when the adversary comes in and launches denial-of-service attacks. Ironically, the network is useless at the moment when its service is needed to sense the adversarial activities. On the other hand, we realize a new localization framework to address these denial-of-service attacks in underwater environment with low/medium node mobility. We use efficient *single-round* distance measuring protocols that are resilient to jam-and-replay attacks, and a *two-tier localization* scheme that can identify and fix spatial anomalies caused by wormholes.

- *Two-tier localization* can be used in a scalable network to identify wormholes of various lengths. It requires a secure and efficient pairwise distance measurement protocol, which is fortunately feasible in underwater acoustic channel only using common hardware. In particular, here we propose DUB and DDB, a pair of secure protocols to measure distance bounds *in single-round using trapdoor one-way functions*. They are more efficient than previous proposals [9][37] and more suitable to be used in networks with random continuous mobility.
- *Self-reconfigurability* is also an important feature of our proposal. By our efficient localization schemes, any denial-of-service attacker's location can be precisely identified. Hence the network is able to heal itself by excluding the "bad" points, then due to deployment redundancy and self-organization the remaining "good" nodes continue to serve the cause.

The paper is organized as follows. Section II presents underwater wormhole attack and its severe threat to UWSN. Then related work is studied in Section III. In Section IV we devise DUB and DDB, a pair of distance bounding protocols required by the two-tier localization scheme described in Section V. We evaluate our design in Section VI. Finally Section VII concludes the paper.

II. Problem: Underwater DoS Attack

A. Underwater acoustic (UW-A) channel assumption

The communication characteristics of the UnderWater Acoustic (UW-A) channel are with following innate characteristics.

Narrow and low bandwidth The available bandwidth of the UW-A channel is limited and strongly depends on both range and frequency. UW-A channel's acoustic band is limited due to absorption with most acoustic systems operating below 30kHz. This fact has two significant impacts on underwater communication. First, the entire width of underwater acoustic frequency band is very narrow, so far the highest value reported is around 1MHz at the range of 60m radius [25]. The entire width of useful acoustic bands is only a small fraction of useful RF bandwidth. Therefore, underwater communications are very vulnerable to narrow-band jamming (partial-band jamming). Second, as surveyed in [26], research system or commercial system have highly variable link capacity and the attainable $range \times rate$ product can hardly exceed 40km-kbps. Long-range acoustic signal that operates over several tens of kilometers may have a capacity of only several tens of bits per second, while a short-range system operating over several tens of meters may have several tens of kilobits per second. Compared to radio or wired links, in both cases bit rates are significantly lower.

Very large propagation latency The signal propagation speed in the UW-A channel is only 1.5×10^3m/sec, which is five orders of magnitude lower than radio propagation speed 3×10^8m/sec in the air. The incurred huge latency exceeds the counterpart values in satellite radio communications. For example, the signal propagation latency between an underwater transmitter and a receiver that are 2 kilometers apart is comparable to the one between the earth and the moon in radio transmission. This huge propagation delay has great impact on network protocol design. As the huge end-to-end round trip time (RTT) becomes the performance bottleneck, many common network protocols do not work as expected if they are directly ported from radio networks.

B. Underwater sensor node assumption

Each UWSN node is a low-cost embedded system equipped with necessary sensing devices. Each sensor node is equipped with a speed sensing unit to detect the flowing speed of tangible water. Each sensor node is also equipped with a water pressure sensing unit, so it can estimate the current depth $d = \frac{P}{\rho}$ where P is measured pressure and ρ is the specific gravity of water. However, because the high-frequency RF radio used by Global Positioning System (GPS) is quickly absorbed by water, a scalable and low-cost positioning system like GPS is not available to underwater nodes.

An UWSN has at least one command center (sink) which disseminates commands to the network and meanwhile collects sensing data from the network. Except this imperative centralized control, the other components of the UWSN are self-organizing. We assume that network is dense enough such that there is no partition in the network and there is sufficient redundancy of paths between the sources and sink. This implies that in a network locality there are usually some redundant network members.

At physical layer, currently we assume omni-directional acoustic transmission and reception. Directional transmission and reception will be addressed in future work. We assume that majority of underwater nodes (including adversarial nodes) are connected with tetherless acoustic links, rather than wired links. In terms of both deployment and maintenance, it is relatively hard to handle multiple underwater nodes intertwined by wires. If there is any set of nodes wired together, we assume that the wired set only contains very limited amount of nodes (e.g., a non-scalable set comprised of tens of nodes), and the length of wire is within a reasonable range (e.g., from tens of meters to kilometers). These physical constraints apply to legitimate nodes as well as adversarial parties.

C. Underwater wormhole attack

We consider underwater wormhole attacks because they explore low bandwidth and slow propagation speed—two innate characteristics of underwater acoustic channel. In other words, they impose severe threats no matter what kind of protocol stack we are going to build for UWSN.

Attack 1: **(Underwater wormhole attack)** Compared to jamming, wormhole attack [20] is more "covert" in nature and harder to detect. A wormhole attacker tunnels messages received in one location in the network over a

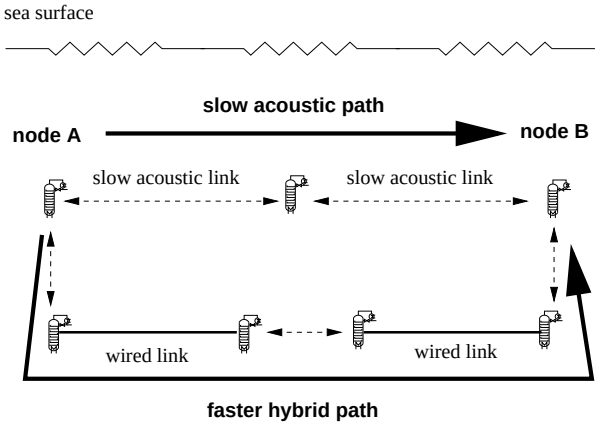


Fig. 1. **Underwater wormhole** (Underwater devices are connected by low-cost wire)

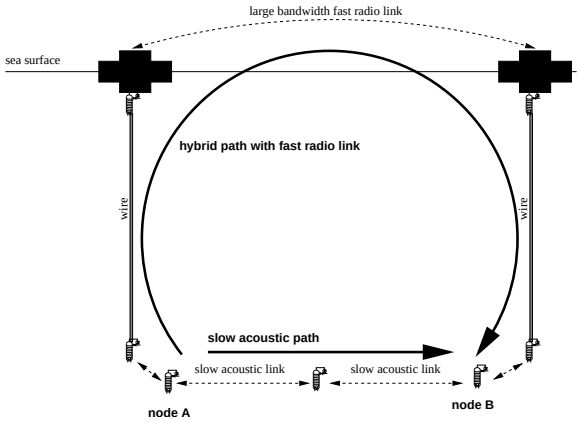


Fig. 2. **Surface-level wormhole** (Surface-level devices are connected by RF radio)

low latency link and replays them in a different location. This typically requires at least two adversarial devices colluding to relay packets along a fast channel available only to the attackers, so that a temporal-spatial "wormhole" is realized with respect to multi-hop routing. In the presence of "wormholes", the attacking nodes can selectively let routing messages get through. Then the "wormhole" link has higher probability to be chosen as part of multi-hop routes due to its excellent packet delivery capability. Once the attacking nodes know they are en route, they can launch "black hole" attack to drop all data packets or "gray hole" attack to selectively drop some critical packets.

As depicted in Figure 1 and 2, in underwater environment attackers can explore fast radio or wired links to significantly decrease propagation delay. Since a 150m wired/wireless link can gain ≈100ms delay advantage, a "hybrid path" features smaller propagation latency even though it is much longer than a "slow acoustic path". This makes the wormhole links favored by best-effort routing schemes. ■

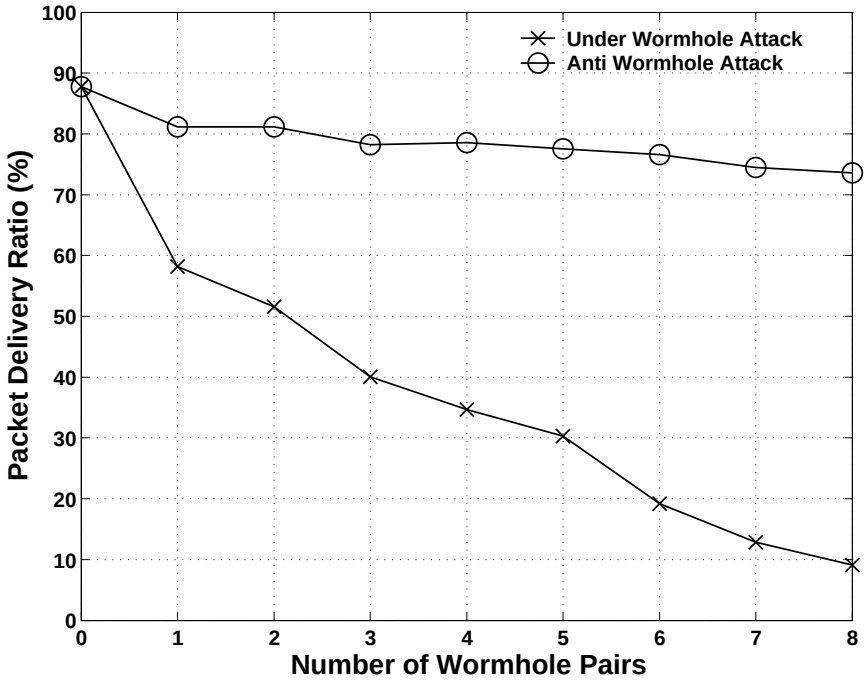


Fig. 3. **The impact of wormholes in underwater sensor network** (with black-hole attacking strategy)

We use pairwise CBR traffic flows to evaluate the impact of wormhole attack in a revised QualNet simulation environment [38] that is enhanced to simulate underwater acoustic channel. 350 sensor nodes are deployed in a

$500\times500\times100m^3$ space and simulated with continuous mobility speed set at the moderate value 1.5m/sec (about 3 knots). CSMA is used at link layer. At network layer, routing is implemented by AODV [33] with enlarged timeout values to cope with large propagation delay. We use 60m one-hop transmission range and 500kbps link rate (from [25]). The length of each pairwise wormhole is $\frac{4}{3}$ of one-hop range (80m). As depicted in Figure 3, the data delivery ratio rapidly decreases from about 90% to less than 10% when the number of pairwise wormholes increases from 0 to 8. In particular, data reports are delivered with lower than 50% probability when there are more than 2 wormholes. This means data reports are more likely to be lost than to be delivered when the enemy throws a few low-cost tiny devices into the network. Fortunately, once our two-tier localization scheme identifies the wormhole links and excludes them in data forwarding, the data delivery ratio can be restored to more than 70%. However, since wormholes replay many extra broadcast packets in the network, the data delivery ratio cannot be restored to the original level due to the *de facto* jamming effect.

D. Underwater wormhole attackers are more dangerous

In radio networks, a typical countermeasure against wormhole attackers is to verify neighbor relation. This is due to the fact that radio propagation speed is the maximum in physics. Hence wormholes shorter than one-hop transmission range impose little threat as the original transmission (which is to be replayed by the short-range wormhole devices) features better routing metrics. (1) Physical layer countermeasures, such as RF watermarking, seek to prevent wormholes by increasing the difficulties to capture the signal patterns. The data bits are transferred in some special modulating method known only to the neighbor nodes. (2) Packet leash is a solution proposed by Hu, Perrig and Johnson for wormhole detection [20]. The leash is the information added into a packet to restrict its transmission distance. It requires either geographical location service support, or time synchronization amongst neighboring nodes. In the geographical leashes, the location information and loosely synchronized clocks together verify the neighbor relation. In the temporal leashes, the TIK protocol efficiently bounds a packet's transmission distance given tightly synchronized clocks. (3) An approach to detect wormholes without clock synchronization is proposed by Capkun et al. [42]. Every node is assumed to be equipped with a nano-second hardware that can use variants of Brands-Chaum protocol [9] to securely measure one-hop distance bound. (4) Another approach is based on the use of directional antennas. In [19], neighboring nodes examine the directions of the received signals from each other and a shared witness. Only when the directions of both pairs match, the neighbor relation is confirmed.

In contrast, in underwater networks, wormholes shorter than one-hop transmission range also impose great threat, as long as the length of wormhole exceeds certain critical threshold that makes the wormhole link surpass other regular links in routing metrics. This is because radio propagation speed is negligible compared to acoustic signal propagation speed. For example, even when one-hop acoustic transmission distance is very long (e.g., 1km), a 150m wormhole link can gain 100ms propagation advantage whatsoever. This means secure neighborhood verification in underwater networks is *not* as effective as it is in radio networks. Therefore, in underwater networks we must do more. In this paper we adopt **a visualization approach to identify wormhole links if the links cause significant propagation anomaly exceeding certain critical threshold.** This design choice has considered the characteristics of wormhole attack in underwater networks.

E. Summary

In self-organizing networks, in particular those networks with node mobility and without geo-routing support, routing paths must be established by a dedicated route discovery procedure using certain routing metrics. The metrics used in route discovery should be *a priori* ones like hop count, end-to-end latency, link capacity, etc., but not *a posteriori* ones like measured packet loss ratio or intrusion detection reports. The *a posteriori* approach incurs a deadlock that is logically inconsistent with route discovery in self-organizing networks.

This offers abundant opportunities to wormhole attackers who can achieve a better *a priori* metric used in the network. They need not to (though they may) break cryptographic protection or to compromise network members, yet they can deplete meaningful communication between the command center and large amount of sensor nodes. On one hand, the sensor nodes may incorrectly believe the command center shows no interest in knowledge acquisition. On the other hand, the command center may misbelieve that there is no data collected from the sensing venues. If left unaddressed, the underwater sensor network pays every penny of development, deployment, maintenance and communication costs, but ironically becomes useless when it is needed at the most urgent moment.

III. Related work

MDS and its applications in ad hoc localization Multi-dimensional scaling was originally a technique developed in the behavioral and social science for studying the structure of objects. The inputs to MDS are the measures of the difference or similarity between object pairs [13]. The output of MDS is a layout of the objects in a low-dimensional space. In this paper, the input is the distance matrix between the sensors. The mechanism can reconstruct the network and calculate a virtual position for each sensor. We adopt the classical metric MDS in the proposed mechanism, in which the distances are treated as in a Euclidean space. More details of MDS can be found in [13][41].

MDS has been applied to solve the localization and positioning problems in wireless networks. In [39], a solution using classical metric MDS is proposed to achieve localization from mere connectivity information. The algorithm is more robust to measurement errors and requires fewer anchors than previous approaches. A distributed mechanism for sensor positioning using MDS has been presented in [22]. It develops a multi-variate optimization-based iterative algorithm to calculate the positions of the sensors. Another approach [7] for sensor network localization applies semi-definite programming relaxation to minimize the errors for fitting the distance measurements.

Wormhole Detection Wormhole attack is proposed in wireless radio networks by Hu *et al* [20]. Physical layer countermeasures, such as RF watermarking, seek to prevent wormholes by increasing the difficulties to capture the signal patterns. If the data bits are transferred in some special modulating method known only to the neighbor nodes, they are resistant to the wormholes implemented by non-network members.

The adoption of directional antennas [28][10] by mobile nodes can improve security. A solution that uses such equipments to defend against wormholes has been presented in [19], where neighboring nodes examine the directions of the received signals from each other and a shared witness. Only when the directions of both pairs match, the neighbor relation is confirmed. SeRLoc [29] uses similar approach to counter wormhole attack and Sybil attack in wireless sensor networks. In SeRLoc some capable locator nodes are equipped with GPS and directional antenna. Wormhole links and malicious Sybil nodes can be detected upon sector-based location and distance estimation.

One approach to detect wormholes without clock synchronization is proposed by Capkun et al. [42]. Every node is assumed to be equipped with a special hardware that can use Brands-Chaum protocol to measure one-hop encounter. As mobile nodes can utilize encounter knowledge to estimate their locations, wormholes that travel anomalously long distance can be detected with non-trivial probability.

Packet leash is a solution proposed by Hu, Perrig and Johnson for wormhole detection [20]. The leash is the information added into a packet to restrict its transmission distance. In the geographical leashes, the location information and loosely synchronized clocks together verify the neighbor relation. In the temporal leashes, the packet transmission distance is calculated as the product of signal propagation time and the speed of light.

Secure distance bounding protocol Cryptographic distance bounding protocols were firstly studied by Brands and Chaum [9] to let one party (Verifier V) determine a practical upper-bound on the physical distance to the other party (Prover P). They observed that any signal propagates at a finite speed, and light can only travel about 30cm per nanosecond. Hence if current technology can realize hardware support to handle timings of a few nanoseconds, then the distance upper-bound between P and V can be derived from signal round trip time. The protocol requires multiple rounds of bit exchange between the Prover and the Verifier.

MAD protocol [42] is a multi-round protocol that mutually estimates the distance bound between a pair of nodes. MAD inherits the multiple rounds of bit exchange from Brands-Chaum protocol, but eliminates the distinction between the Prover and the Verifier. Both nodes are peers functioning as the Prover and the Verifier at same time.

Recently, Sastry et al. [37] proposed Echo, a distance bounding and location claim scheme using both ultrasound and radio signals. The Echo protocol is multi-round by the design. A round of message exchange in radio signal is used to prepare for distance bounding and location claim, then a round of message exchange in ultrasound signal measures the bounded distance. (1) As in the underwater acoustic channel, any distance bounding protocol using slow signals is vulnerable to wormhole attack. In particular, if a nearby adversarial node (within the distance bound) is wired together with another collaborative node (within reasonable distance measured in kilometers), then the former one is capable of letting the Verifier believe the latter one is within the distance bound. (2) But in the context of location claim, this perhaps is not an attack because at least one of the adversarial node must claim its location within the bounded region. Wormhole attack is not studied in [37].

More recently, Hubaux et al. [21] proposed a 3-round secure distance bounding protocol. An appealing feature of this protocol is its near-zero cryptographic processing delay in distance bound measurement. By trapdoor

commitment, cryptographic overheads are delayed to a round next to the distance measurement round, hence the protocol produces more precise results. However, this implies the protocol is inherently a multi-round protocol that is comprised of commitment and de-commitment rounds.

IV. Underwater pairwise distance measuring

Since denial-of-service attacks introduce anomalies into the network, we adopt an intrusion detection and intrusion recovery approach. Secure pairwise distance measuring described in this section functions as the building block of our range-dependent localization design. In the next section, measured distance values will be used in an automated detection framework to identify wormhole links, which are then excluded in packet forwarding.

A. Design assumptions

In pairwise distance measurement, a pair of peer nodes try to measure their physical distance in-between. Methods based on Received Signal Strength Indicator (RSSI) are vulnerable to acoustic interferences like noise, multi-path, and Doppler frequency spread. On the other hand, Angle-of-Arrival (AoA) systems require directional transmission/reception devices, which incur non-trivial extra cost. Therefore, we adopt a Time-of-Arrival (ToA) approach. Other than off-the-shelf acoustic modems, we do not rely on any special hardware.

We assume two one-hop neighbors have already known each other's authentic public key PK, or have agreed on a symmetric key K (Cryptographic key management will be elaborated in Section V-D). If both peers are uncompromised, then both of them are protocol-compliant. Pairwise distance can be precisely measured between two protocol-compliant nodes. Any protocol-compliant node *only* uses underwater acoustic signals during its pairwise distance measurement process.

B. Why single-round secure distance bounding protocol?

Although there are many existing secure distance bounding protocols as described in Section III, they are nevertheless *not suitable* in the underwater environment due to multi-round design.

First, each sensor node is constrained in energy reserve and communication capability. A multi-round protocol features extended execution time and multiplied communication energy consumption. Since the protocol is executed network-wide, the overall protocol expense is very large in a large-scale sensor network.

Second, as we described earlier, underwater sensor nodes are associated with low/medium mobility due to random water current motion. Given the fact that round-trip propagation latency is huge, the positions of a moving sensor node may change signifi cantly when a multi-round protocol is fi nished. Therefore, when nodes continuously move, any multi-round distance bounding/measuring protocol is *inaccurate* due to position deviations aggregated during the multi-round procedure, and *inefficient* because of the need to obtain precise results by more trials. In contrast, a 1-round scheme can produce instant and effi cient measurements.

Third, adversary can disrupt the distance measuring protocol as well. When under attack, a multi-round protocol likely stops at certain state and cannot continue. More seriously, the adversary can launch *jamming-and-replay attack* [11] to increase the measured distance value between two protocol-compliant nodes. Therefore, two protocol-compliant nodes should restart the distance measuring protocol whenever any jamming interference is detected during the measuring process, until a protocol execution during which no jamming interference is detected. This would incur very large overheads if a multi-round protocol is used.

Attack 2: **(Jam-and-replay attack)** Căpkun et al. [12][11] observed that an adversary may jam a legitimate transmission and be able to replay *the* transmission before the legitimate re-transmissions. They showed a *malicious distance enlargement attack* [11] where the adversary can use jam-and-replay strategy to disrupt distance bounding protocols.

The jam-and-replay attack requires the adversary to intercept the entire legitimate transmission before it can replay the message. Though proposed in radio networks, the attack is less realistic in electromagnetic channels. This is because signals propagate at light speed which cannot be surpassed, and the propagation delay is negligible compared to transmission delay. The attacker needs extra hardware like directional antenna, and must be placed in a delicate spatial setup between the sender and its receivers: (1) The adversary must be capable of receiving at one direction and transmitting at another direction at same time. This requires a delicate spatial setup amongst

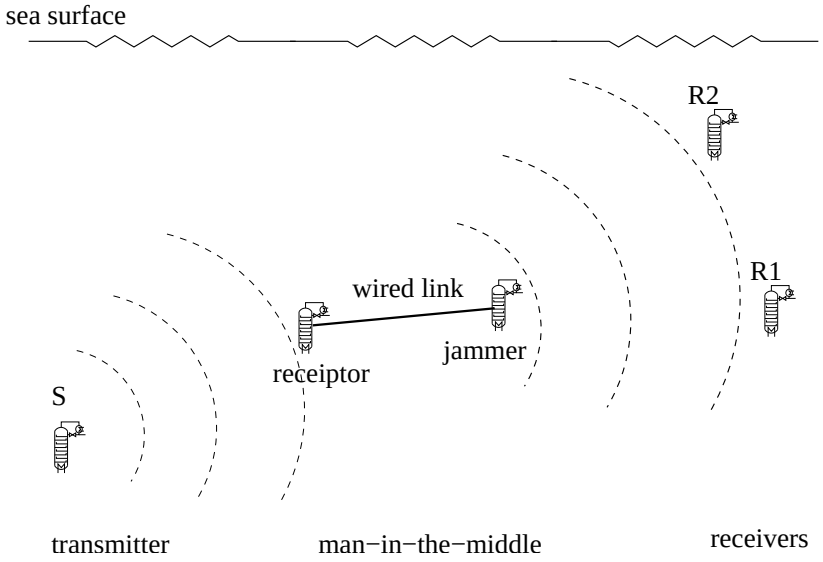


Fig. 4. **Jam-and-replay attack**

the sender, the receiver, and jammer, so that the jamming signals won't interfere with the jammer's own reception. (2) Otherwise, if the adversary cannot receive and transmit at same time, then it can only jam the last bit right after it receives the bit. Consider the non-trivial transmission latency (which is relatively large compared to radio propagation latency), the attacker's own processing delay may cost the only chance.

Unfortunately, we see the underwater acoustic channel offers jam-and-replay attackers a real stage. As depicted in Figure 4, the attacker can use two nodes to implement the attack, and no expensive hardware for directional reception/transmission is needed on the two nodes. Right after the receiptor node receives the last bit, it notifies the jammer node to start jamming (then both of them is capable of replaying). As an l-meter wired transmission can gain approximately $\frac{l}{1500}$-second propagation advantage to acoustic transmissions, there are still $\frac{w \cdot l}{1500}$ legitimate bits in the progress of propagation in an acoustic channel with bandwidth w. These bits are successfully jammed. ∎

Due to these critical reasons, it is clear that a simple 1-round protocol is better than its more complex multi-round counterparts in underwater environments.

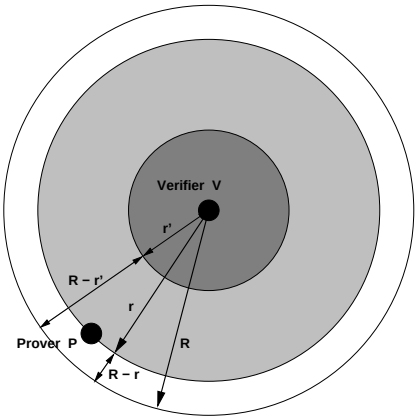


Fig. 5. **Pairwise distance measurement**

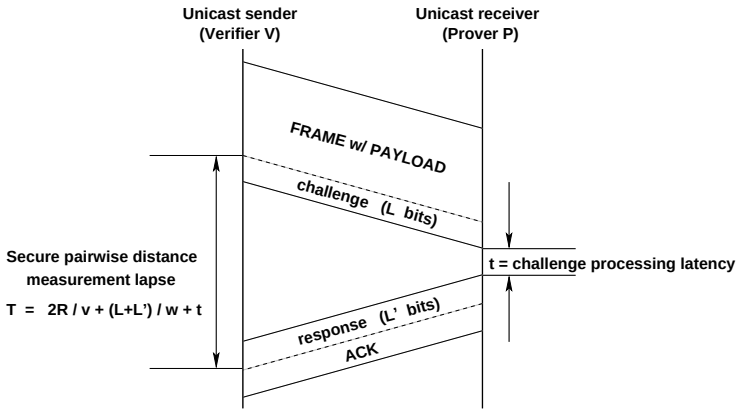


Fig. 6. **Distance upper-bound measurement for any unicast sender** (assuming CSMA)

C. DUB: a 1-round protocol measuring Distance Upper-Bound

DUB is a 1-round distance bounding protocol based on one-way function, which is a fundamental cryptographic primitive. DUB is suitable to be piggybacked on any unicast packet transmission.

Intuitively, a function $f : X \rightarrow Y$ is a *one-way function* if it is "easy" to obtain image for every element $x \in X$, but "computationally infeasible" to find preimages given any element $y \in Y$. A function f is a *trapdoor one-way function* if f is a *one-way function* and it becomes feasible to find preimages for $y \in Y$ given some *trapdoor information*. More formally, one-way function and trapdoor one-way function have strict definitions in modern cryptography. The chance to invert an one-way function is negligible (i.e., sub-polynomial) for a Probabilistic Polynomial-Time (PPT) adversary (see Appendix IV-E).

(DUB: 1-round Distance Upper-Bound measuring)
Prerequisite: For a pair of protocol-compliant Prover P and Verifier V, their signal propagation speed is v, and their channel bandwidth is w. V knows P's authentic public key PK_P with respect to a well-known trapdoor one-way function f.

01 V chooses an L'-bit random nonce x and computes an L-bit $challenge = f_{PK_P}(x)$ in polynomial-time. V piggybacks the challenge at the end of a unicast packet to the Prover P;
02 V's measurement timer starts at the moment when the first bit of $f_{PK_P}(x)$ is transmitted;
03 P uses its trapdoor key SK_P to compute $response = x$ by inverting the one-way function in polynomial-time. P piggybacks the response x at the beginning of the ACK packet;
04 V's measurement timer stops at the moment when the last bit of x is received;
05 The timer returns value T. V computes the distance upper-bound $R = \frac{(T-(L+L')/w)\cdot v}{2}$.

Similar to existing distance bounding protocols, DUB explores round trip time in measuring the upper-bound of pairwise distance. As depicted in Figure 5, a pair of nodes can estimate their distance upper-bound by a challenge-response protocol. Let's assume DUB is implemented at MAC layer and cross-layer processing delay in a sensor node's protocol stack is negligible. The Verifier V selects a random nonce x, computes $f_{PK_P}(x)$, and sends out $f_{PK_P}(x)$ (of L bits long given the known f) as a challenge at time t_0, then the Prover P receives the challenge at time $\frac{r}{v} + \frac{L}{w}$. If the latency of processing the challenge is t, and P sends back the response immediately, then V will receive the response (of L' bits long given the known f) at time $t_0 + \frac{2r}{v} + \frac{L+L'}{w} + t$. In particular, if P's processing latency $t < \frac{2(R-r)}{v}$, then P is able to prove that it is within the distance upper-bound R of the Verifier V.

DUB's protocol execution is depicted in Figure 6. In sensor networks, due to constrained capability of each low-cost sensor node, *we recommend the use of purely symmetric-key based crypto-schemes, such as symmetric-key encryption schemes*. Therefore, the PK_P and SK_P in the above protocol specification are replaced by a single symmetric key K_{PV} shared between P and V (and now $L = L'$).

D. DDB: a 1-round protocol measuring Distance Dual Bounds

DDB is a superset of DUB. It measures not only the upper-bound, but also the lower-bound between two protocol-compliant nodes. This requires the Verifier V to know the maximum processing delay t_{max} that is needed to compute its challenge even on the slowest node in the network. In theory, the worst lower-bound is 0, when the Prover P is at the same site of the Verifier V and P computes the response x using exactly $\frac{2R}{v}$ time. If a Prover P' cannot find out the response x in less than or equal to $\frac{2R}{v}$ time, then P' cannot prove its presence within the radius R no matter where P' is. A probabilistic polynomial-time (PPT) adversary must be such an unsuccessful P'.

On the other hand, if the maximum processing latency $t_{max} < \frac{2R}{v}$, then the lower-bound r depends on this t_{max} (as we enforce the policy that any protocol-compliant node will not introduce any extra delay during the 1-round distance measurement). DDB's protocol specification is same as the one of DUB, except in DDB the Verifier V also computes the distance lower-bound

$$r = \frac{(T - (L + L')/w - t_{max}) \cdot v}{2}.$$

As depicted in Figure 5, if t is larger, then the Prover P must be at the circle of a smaller radius r' (the darkgray area). This implies an uncompromised Prover P should use a lightweight implementation of one-way function as long as it is guaranteed that a cryptanalyst cannot invert the lightweight implementation in $\frac{2R}{v}$ time (given nowadays most powerful hardware). Fortunately, this goal can be achieved. Nowadays advanced encryption algorithms, including the well-known Data Encryption Standard (DES [31]) and Advanced Encryption Standard (AES [32]), are block cipher algorithms based on Feistel structures and Substitution-Permutation Networks (SPN) [16]. Security complexity in these algorithms is achieved by many rounds of permutation and substitution. In particular, (i) the algorithms must achieve one-way property so that it is easy to obtain ciphertext from plaintext, but not vice versa; (ii) the algorithms must resist ciphertext-only attacks, known-plaintext attacks, chosen-plaintext attacks, adaptive chosen-plaintext attacks and their advanced variants like differential cryptanalysis [4] and linear cryptanalysis [30]; and (iii) the algorithms must resist brute-force attack on key enumeration and other attacks on keys such as related-key cryptanalysis [3].

TABLE I

SECURITY COMPLEXITY OF RC5, 128-BIT KEY AND BLOCK SIZE ("$>$" DENOTES THE CASE WHEN THE ATTACK IS IMPOSSIBLE EVEN AT A THEORETICAL LEVEL)

rounds	4	8	12	16	20	24	28
differential cryptanalysis (chosen plaintext)	2^{19}	2^{42}	2^{58}	2^{83}	2^{106}	2^{123}	$>$
differential cryptanalysis (known plaintext)	2^{74}	2^{86}	2^{94}	2^{106}	2^{118}	$>$	$>$
linear cryptanalysis (known plaintext)	2^{47}	2^{95}	2^{119}	$>$	$>$	$>$	$>$

TABLE II

SECURITY COMPLEXITY OF RC5, 64-BIT BLOCK SIZE (SUMMARIZED FROM VARIOUS CRYPTANALYSIS ON RC5)

rounds	4	6	8	10	12	14	16
differential cryptanalysis (chosen plaintext)	2^{17}	2^{24}	2^{35}	2^{46}	2^{54}	2^{63}	$>$
differential cryptanalysis (known plaintext)	2^{41}	2^{45}	2^{50}	2^{56}	2^{60}	$>$	$>$
linear cryptanalysis (known plaintext)	2^{40}	2^{60}	$>$	$>$	$>$	$>$	$>$

For these modern block cipher algorithms, processing overhead is adaptable by increasing or decreasing the number of substitution-permutation rounds. Related cryptanalysis is presented in many literatures. In this work we use RC5 as the example. RC5 has been extensively scrutinized since it was proposed in 1994 [36]. In 1995 RC5 became an IETF standard encryption scheme widely used on the Internet [1]. Since then many cryptanalytic results of RC5 have been published. As claimed by the designer a novel feature of RC5 is its flexibility. Applications can choose a variable word size, a variable number of rounds, and a variable-length secret key. In particular, we explore the feature of variable number of rounds to decrease processing overhead (In Table I for 128-bit block size & Table II for 64-bit block size). The summary of the data requirements for a successful attack against RC5 with a variable number of rounds is provided in [45] based on various cryptanalysis [23][27][18][5][6][24][8].

Depending on the value R, it is clear that we can use a smaller round value from the tables so that even the most powerful hardware on earth today cannot break this reduced-round RC5 variant in $\frac{2R}{v}$ time. Now the lower-bound r is measured more precisely because a protocol-compliant Prover P's processing latency is minimized. Figure 7 shows corresponding encryption performance on an iPAQ3670 PocketPC with Intel StrongARM 206MHz CPU. In our simulation study we used $8\mu s$ processing delay for a 8-round reduced RC5 cipher operating on 128-bit block size. Thus the difference between R and r is only 0.012m — a quantity similar to the size of sensor nodes like Crossbow Motes.

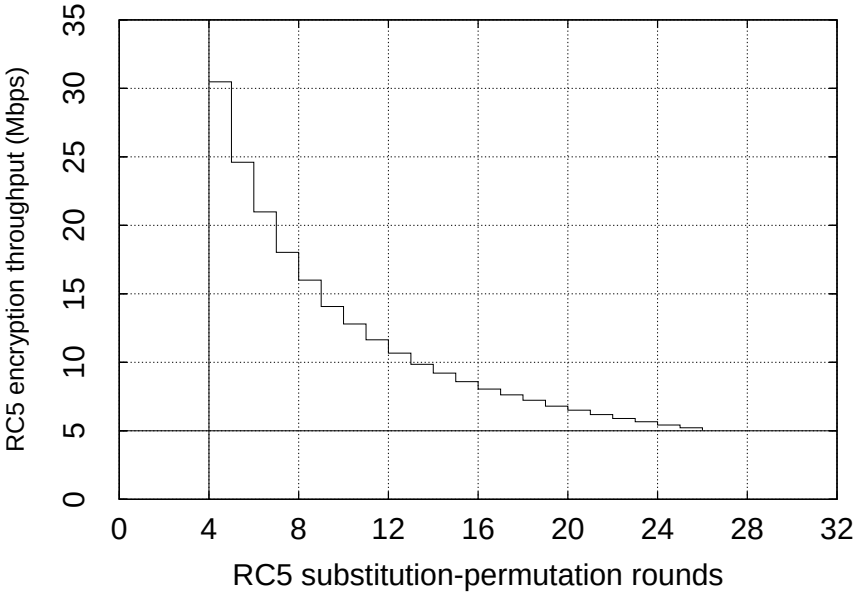


Fig. 7. **RC5's encryption performance on iPAQ3670 PocketPC** (processing delay = data size / throughput)

E. Cryptanalysis of DUB and DDB

The concept of one-way function is defined on polynomial relation between the input length and output length. For a Probabilistic Polynomial-Time (PPT) adversary, its chance to invert an one-way function is negligible (i.e., sub-polynomial). Here we follow the common definition [17]:

Definition 1: **(Negligible):** A function $\mu : \mathbb{N} \rightarrow \mathbb{R}$ is *negligible* if for every positive polynomial $P(\cdot)$ and all sufficiently large n's,

$$\mu(n) < \frac{1}{P(n)}. \blacksquare$$

Definition 2: **(One-way Function):** Let $\mathbb{Z}_2^*$ denote binary strings with arbitrary positive length. A function $f : \mathbb{Z}_2^* \mapsto \mathbb{Z}_2^*$ is a (strong) *one-way* function if the following two conditions hold:

1) *Easy to compute*: There exists a deterministic polynomial-time algorithm A such that on input x it outputs $f(x)$, i.e., $A(x) = f(x)$.
2) *Hard to invert*: The probability to invert the function is negligible. That is, for every probabilistic polynomial-time algorithm A', every positive polynomial $P(\cdot)$, and all sufficiently large n,

$$\mathsf{Pr}[A'(f(U_n), 1^n) \in f^{-1}(f(U_n))] < \frac{1}{P(n)}$$

where U_n denotes a random variable uniformly distributed over $\mathbb{Z}_2^n$, and the auxiliary input 1^n gives the length of the desired output n in unary notation. $\blacksquare$

The f_K function in our notation denotes a collection of one-way functions that are indexed by a truly random variable K (intuitively the trapdoor key). As $P \stackrel{?}{=} NP$ is an open problem, the existence of one-way function and collection of one-way functions is not proven. Yet a number of conjectured collections of one-way functions are routinely used in cryptologic research, such as Discrete Logarithm, RSA function, Rabin function, and AES. The f function in our notation can be replaced by one of these conjectured one-way functions that have widely been used in practice.

First we formally state the definitions and goals of cryptanalysis. The distance bounding protocols are cryptographic Interactive Proofs (see Appendix IV-E) when the set of bounded distance values are treated as a language. The concept of "Interactive Proof" is the foundation of useful notions like Zero-Knowledge Proof.

Definition 3: An *Interactive Proof* for a language L is a protocol PV for a *Prover* P and a *Verifier* V such that:

- *Completeness*: If $a \in L$ then P has less than negligible chance of not convincing V that $a \in L$

$$\forall c > 0, \exists N_0 \; s.t. \; \forall a \in L \text{ where } |a| > N_0$$

$$\mathsf{Pr}_{coins\ of\ P,V}[PV(a)\ makes\ V\ accept] \; > \; 1 - \frac{1}{|a|^c}$$

- *Soundness*: If $a \notin L$ then every adversarial P' has negligible chance of convincing V that $a \in L$

$$\forall P', \forall c > 0, \exists N_0 \; s.t. \; \forall a \notin L \text{ where } |a| > N_0$$

$$\mathsf{Pr}_{coins\ of\ P',V}[P'V(a)\ makes\ V\ accept] \; < \; \frac{1}{|a|^c}$$

$\mathbb{IP}$ is defined to be the class of languages which have Interactive Proofs. ∎

Definition 4: An *Upper-bound Pairwise Distance Proof* for a language L is an Interactive Proof for a *Prover* P and a *Verifier* V such that the language L denotes the range $[0..R]$ of pairwise distance $(R \in \mathbb{R}+)$. A *Dual-bound Pairwise Distance Proof* for a language L is an Interactive Proof for a *Prover* P and a *Verifier* V such that the language L denotes the range $[r..R]$ of pairwise distance $(r \in \mathbb{R}+, r \leq R)$. ∎

Definition 5: A *Compliant Upper-/Dual-bound Pairwise Distance Proof* for a language L is an Upper-/Dual-bound Pairwise Distance Proof where the Prover P and the Verifier V are protocol-compliant and signal propagation is also protocol-compliant. ∎

Suppose there is no wormhole in the system, now we prove that DUB is a protocol providing Compliant Upper-bound Pairwise Distance Proof, and DDB is a protocol providing Compliant Dual-bound Pairwise Distance Proof.

Theorem 1: DUB is a protocol providing Compliant Upper-bound Pairwise Distance Proof if a trapdoor one-way function f_K is used and only the Prover knows the trapdoor key K.

Proof: For the Prover P knowing the trapdoor key K,

- $a \in L$: In other words, $a \in [0..R)$ or $a < R$ where a is the current distance between the Prover P and verifier V. Because $\frac{2(R-a)}{v}$ is by its nature a polynomially bounded value, by the "easy to compute" definition of one-way function and trapdoor one-way function, the Prover P can invert function f and computes the response x in less than this polynomial-time t. In DUB, the Verifier V's timer

$$T < \frac{2a}{v} + \frac{L + L'}{w} + \frac{2(R-a)}{v} = \frac{2R}{v} + \frac{L + L'}{w}$$

  Hence the upper-bound R is greater than the value computed by V:

$$R > \frac{(T - (L + L')/w) \cdot v}{2}.$$

  With probability 1, V is convinced that P is at most R away. The completeness of DUB is proven.
- $a \notin L$: In other words, $a \notin [0..R)$ or $a \geq R$. A protocol-compliant node cannot overcome the propagation delay $\frac{2R}{v}$ to send back computed response. If P sends back a random guess before it receives the challenge, then the probability of guessing the correct response is $\frac{1}{2^{L'}}$, which is a negligible value when L' is large enough. The soundness of DUB is proven.

For protocol-compliant P' who doesn't know the trapdoor key, the probability to compute a correct response x is (1) negligible by the "hard to invert" definition of one-way function if it is within the distance upper-bound, or (2) negligible by random guess if it is outside of the distance upper-bound. In either case DUB is secure against such P'. ∎

Theorem 2: DDB is a protocol providing Compliant Dual-bound Pairwise Distance Proof if a trapdoor one-way function f_K is used and only the Prover knows the trapdoor key K.

Proof: The proof follows the DUB's proof and a pair of protocol compliant nodes won't introduce any extra latency during the 1-round measurement process. If any external interference is detected during the 1-round process, the 1-round protocol is restarted until an un-interfered round is accomplished. ∎

F. Applying reduced-round RC5

Table I shows RC5's strength for 128-bit block size, and Table II shows the case for 64-bit block size. In DUB and DDB, an adversary can launch chosen plaintext attack (in issuing his own random challenges), thus the security strength value is the minimal one across the three rows.

Since a reduced-round cipher is used in DUB/DDB execution, the adversary may invert the reduced-round cipher and reveal the used cipher key after $\frac{2R}{V}$ delay but before the end of the network lifetime. The following hash-chain design prevents a powerful adversary from breaking the master key K_{PV} shared between P and V.

The Verifier V and the Prover P do not directly use the master key K_{PV} in DUB/DDB executions. Instead, they use a symmetric key one-way function f (e.g., RC5) to compute an efficient one-way hash chain such that:

$$H_0 = K_{PV} \oplus N,\ H_i = f_{K_{PV}}(H_{i-1}),\ i = 1, \cdots, n.$$

Here N is a 128-bit nonce agreed between P and V. This nonce is publicly exchanged when needed. When the hash chain is used up, a new public nonce is exchanged and a new chain is generated.

The hash chain is used in the reverse order of its generation. At first, H_n is used as the trapdoor key in DUB/DDB execution, then $H_{n-1}, \ldots, H_i, \ldots, H_1$. And a new chain is generated right after the current H_1 is used. To avoid replay attack, an element in a hash chain is used only once. To address gaps caused by packet loss, the challenge in DUB/DDB implementation is prefixed with the current index i (so the Prover P knows which chain element to use). To save the hash computation time, the Prover P should cache several next elements in the hash chain so that a short list lookup will get the element (to be used as the cipher key in reduced round RC5). In the ideal case when there is no packet loss, the Prover P only needs to cache the immediately next element H_{i-1} after current round i.

G. Vulnerabilities of DUB and DDB

Upon a successful protocol execution in the absence of jamming interference and wormholes, DUB and DDB can correctly measure pairwise distance between a pair of protocol-compliant nodes. However, any compromised and non-compliant network member can either increase or decrease the measured distance:

- *Distance increment*: A compromised Prover P intentionally inserts a chosen period of latency before it sends back the response. Then the Verifier V will measure an enlarged pairwise distance.
- *Distance decrement*: A compromised Prover P' can connect with a remote node P via a faster wormhole (e.g., wire or wireless radio). Due to the existence of P' and the faster wormhole, the Verifier V will measure a decreased pairwise distance towards the remote Prover P.

In addition, the distance decrement attack is also feasible for a pair of external wormhole attackers P' and P'' in the middle of two protocol-compliant nodes P and V. P' and P'' can shorten the measured distance between P and V. These vulnerabilities caused by malicious network members and wormholes are addressed in the next section. We allow incorrect pairwise distance values to be measured when there are malicious nodes, but the anomalous points can be identified and isolated.

V. Two-tier Localization for Wormhole Detection and Recovery

According to the physical length of a wormhole, the wormhole can be classified as either a *short-range wormhole* (e.g., shorter than 300m) or a *long-haul wormhole* (e.g., longer than 300m). In this section, we describe a *two-tier wormhole detection* approach to address both sorts of wormholes. In particular, a short-range wormhole can be quickly identified and isolated in a local neighborhood (of a flexible k-hop range), and a long-haul wormhole is identified by the command center who is capable of acquiring global network topology knowledge.

Our approach leverages localization designs in sensor networks. More importantly, we address low/medium node mobility that is rare in land-based sensor networks. As sensor nodes are randomly moved by unpredictable water current, the relatively small neighborhood around a short-range wormhole may change significantly. Nonetheless, even with mobility, long-haul topological metrics (such as hop count and end-to-end latency between two distant points) do not vary significantly. Therefore, our two-tier design will be capable of quickly identifying short-range wormholes to compete with node mobility, and identifying long-haul wormholes within a limited delay proportional to network scale (i.e., diameter).

A. Localization via Multi-Dimensional Scaling

We rely on techniques to estimate node positions using only the measurements of pairwise distances between neighboring nodes. As described in Section IV, secure pairwise distance information is acquired by running the DDB protocol. Furthermore, it is assumed that surface level sensor nodes on buoys are equipped with GPS to know their exact locations. These nodes serve as "anchors".

The problem of finding the positions of all the nodes given a few anchor nodes and pairwise distance information is called the localization problem. Multi-Dimensional Scaling (MDS), a technique originally developed in the behavioral and social science for studying the structure of objects, is used in our design to tackle the localization problem. The inputs to MDS are the measurements of the difference or similarity between object pairs. The output of MDS is a layout of the objects in a low-dimensional space. In this paper, the input is the distance matrix between one-hop neighbors. The mechanism can reconstruct the network and calculate a virtual position for each sensor. We adopt the classical metric MDS in the proposed mechanism, in which the distances are treated as in a Euclidean space. It was shown in [39] that classical metric MDS can achieve localization from connectivity estimation. The algorithm is more robust to measurement errors and requires fewer anchors than previous approaches. A distributed mechanism for sensor positioning using MDS has been presented in [22]. It develops a multi-variate optimization-based iterative algorithm to calculate the positions of the sensors. Another approach [7] for sensor network localization applies semidefinite programming relaxation to minimize the errors for fitting the distance measurements.

B. Wormhole detection

In a secure underwater sensor network, each sensor node seeks to understand its k-hop neighborhood where k is a flexible parameter selected by the node itself. A low-end node may choose a smaller k, while a high-end node would choose a larger k. The k-hop neighborhood around the node is called *k-sphere* in this paper.

After selecting its own k, the sensor node seeks to visualize its k-sphere by MDS. Meanwhile, the command center seeks to visualize the entire network by MDS. Both require collecting one-hop pairwise distance reports, which are treated as a specific kind of event report in our design. Since each sensor has a water speed sensing unit, it estimates its current motion speed v_m and computes an adaptive period $T = \frac{R}{v_m}$ using its transmission radius R. The period approximates the needed time to float out of the node's 1-hop neighborhood. During the period, the sensor opportunistically piggybacks DDB protocol in a unicast transmission towards each active neighbor, thus collects the current pairwise distance reports. Here we use RC5 encryption algorithm and choose $L = L' = 64$-bit (the first 64-bit generated from RC5 encryption), so that each DUB/DDB execution incurs 8 bytes overhead in challenge and another 8 bytes overhead in the corresponding response. The measured distance is a 16-bit value (in 1m unit length).

On each sensor, if any physical event is sensed and reported, the sensor becomes active. By limited-scope flooding which is robust against packet loss on wormhole links, an active sensor disseminates its pairwise distance (PD) report:

$$\langle PD, id, k, k_{TTL}, (d_1, id_1), (d_2, id_2), \ldots, (d_n, id_n) \rangle$$

where PD is the packet classifier, id is the sensor's unique id (currently 16-bit), k and k_{TTL} (both are 4-bit) are related to k-sphere formation, and the remaining part holds a list of pairwise distance values towards its neighbors $(id_1, id_2, \cdots, id_n)$. Intuitively, if D is the average network density, every PD report averagely incurs about $32 \cdot D + 24$ bits overhead. At first glance, this scheme may incur excessive communication overhead (when node mobility is high). Fortunately, there is no need to report unchanged pairwise distance values since the most recent report. Thus the list is shortened to hold only those values for new neighbors and old neighbors with a significant distance change (defined as larger than d_{change} =15 meters in our current design) since the last PD report. If the list is empty, then the entire PD report is spared.

In each report k_{TTL} is initialized to a value k_{TTL}^{init}. At per forwarding stop, the k_{TTL} field is decreased by 1. And PD reports with $k_{TTL} = 0$ are dropped. At the beginning, k_{TTL}^{init} is set as the node's own k. As the node forwards other pairwise distance reports, it sets the k_{TTL}^{init} to be the largest $(k - k_{TTL})$ in those passing-through reports during the most recent $\frac{k_{TTL}^{init} \cdot R}{v_m}$ period. The time period approximates the needed time to move out of the node's current k_{TTL}^{init}-sphere. This way, when a node with large k value floats out of a neighborhood, the k_{TTL}^{init} values on the other nodes will eventually decrease due to the soft-state design.

By this design, in an active region, an active node's pairwise distance value eventually reaches all active nodes that need the report to form their k-spheres. For those nodes with smaller k's, they will receive reports from nodes with larger k's. Such reports are suppressed immediately by comparing the k embedded in the report and the receiving node's own k value.

To decrease communication overheads, distance reporting to the command center is limited to a subset of sensor nodes. The qualified candidate nodes are those who have not received a larger k embedded in passing-through distance reports than its own k within the most recent $\frac{k_{TTL}^{init} \cdot R}{v_m}$ period. These nodes are the most capable nodes with maximal k-spheres. If two or more capable nodes have selected the same k value and also within k-hop of each other, then they can see each other in their k-spheres. Here the capable node with the lowest ID wins the chance of reporting to command center. It compresses the representation of its k-sphere and sends the compressed result to the command center every $\frac{k_{TTL}^{init} \cdot R}{v_m}$ period.

Now that all local k-spheres are formed and the command center also has the overall network topology knowledge in a limited delay. Both types of wormholes are hence detectable:

- Since both ends of a short-range wormhole would fall in certain node's k-sphere, MDS-VoW [43] can be used to detect the wormhole within the corresponding k-sphere. This k-hop localized approach uses fresh distance reports to cope with the changing environment caused by node mobility.
- MDS-VoW is used at the command center to detect long-haul wormholes. In this case the distance reports are less fresh due to potentially large communication delay in a scalable network with long multi-hop path. Fortunately, due to "distance effect" [2], the topological metrics between the two distant ends of a long-haul wormhole do not vary significantly with respect to low/medium mobility.

C. Intrusion recovery

We then explore the self-reconfigurable nature of sensor networking. In sensor networking, alternative paths can be found due to redundancy in deployment. To exclude long-haul wormholes, the command center uses scoped flooding to disseminate authenticated commands to sensor nodes which are within one-hop of the identified wormholes, and the command explicitly states those wormhole links (e.g., the link between node A and B is via wormhole). To exclude short-range wormholes, the detecting sensor uses scoped-flooding to distribute an authenticated intrusion detection report within its entire k-sphere. All notified nodes will stop forwarding to or receiving from the identified wormhole links.

D. Discussions

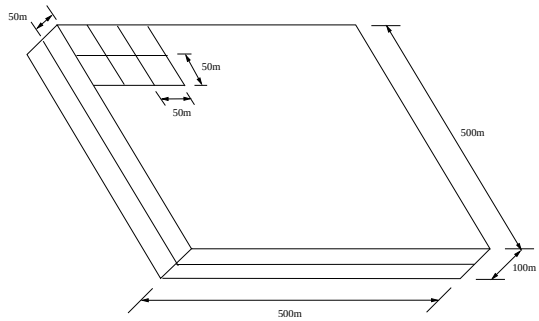
Key management *We assume every packet is protected with point-to-point secure channel (e.g., IPsec ESP with authentication enabled) so that message privacy and message integrity are ensured per hop.* It is argued in many literatures [34][15] that expensive public key cryptography is not suitable in sensor networks. Instead we can employ Key Pre-distribution Schemes (KPS) to reach pairwise key agreement amongst sensor nodes [15]. In particular, in our simulation study we use Du's probabilistic KPS scheme [14] with 95% pairwise key agreement probability. With 5% probability a physically existing link cannot reach key agreement, and is hence ignored.

Energy efficiency Our localization based approach is consistent with energy efficiency designs, where sensor nodes can switch to inactive modes to save energy expense. In our design autonomous nodes can freely join/activate and leave/deactivate, then currently active sensor nodes run the pairwise distance measurement and localization schemes for intrusion detection. Our design does not rely on the participation of inactive sensor nodes.

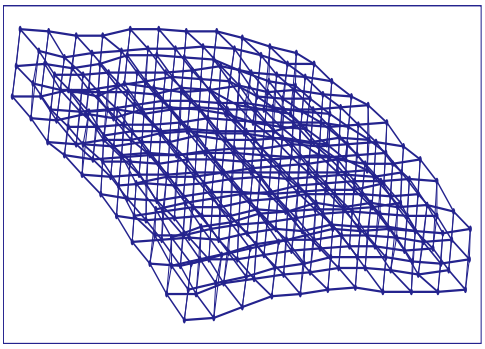
Stationary and high node mobility scenarios For those sensor nodes fixed on seabed, the command center evaluates their real positions based on all received MDS reports. Once their fixed locations are identified, they become anchor nodes and help other non-anchor nodes to achieve more precise location estimation. For few nodes with very high node mobility (which is very unlikely because it is extremely hard to achieve high speed in relatively viscous water), the nodes can increase their d_{change} to a larger value, so that their distance reports are spared if distance change is less than d_{change} since the most recent report. This trades protocol precision with efficiency.

Directional transmission/reception Like directional antenna in radio networks, directional sound ray devices incur extra hardware cost, thus question is raised against their deployment on low-cost sensor nodes when the network

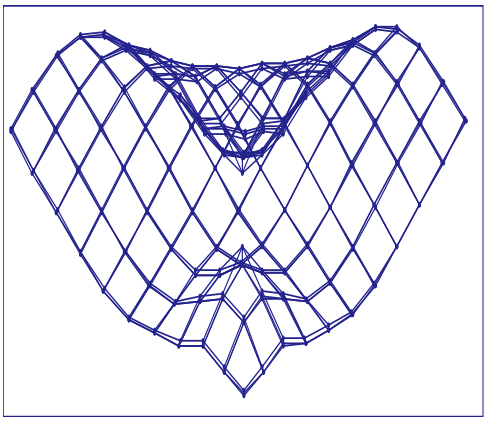
scale is large and even a little increment in unit device may result in tremendous overhead. However, since technology may realize low-cost directional methods in an underwater environment in the near future, we are studying both attacks and countermeasures that use directional communication at the physical layer.

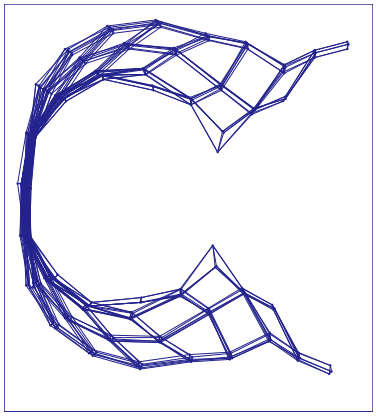


(a) Original sensor layout: an $11\times11\times3$ grid



(b) Global reconstructed network by command center when no wormhole exists.





(c) Global reconstructed network by command center when a long-haul wormhole exists: front and side.

Fig. 8. Grid Deployment: Impacts of wormholes on global network reconstruction.

VI. Evaluation

A. Constructing the two-tier structure

As described in Section V, each sensor node opportunistically disseminates and acquires pairwise distance vectors within its k-hop neighborhood, so that both reconstruction and detection can be conducted locally. Meanwhile any node with a local maximum k will encode its local MDS map and send it to the command center for global visualization.

B. Conducting MDS-VoW

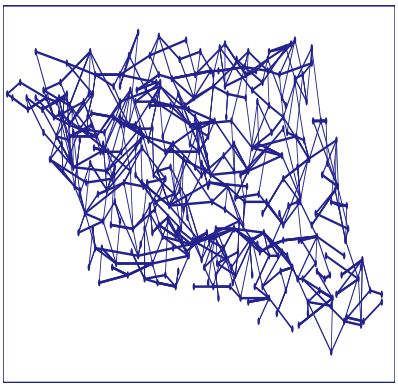
After each active sensor opportunistically disseminates and acquires pairwise distance vectors within its k-hop neighborhood, it then builds the distance matrix using the Dijkstra's algorithm and feeds the result to MDS, which will rebuild the k-hop neighborhood and generate a virtual position for every sensor in scope. The global visualization is executed in a similar way at the command center, but with less fresh pairwise distance vectors. To illustrate the impacts of wormholes on network reconstruction, we use the following random deployment to demonstrate the visual effects.

Grid deployment This set of experiments clearly shows the impacts of wormholes. In the grid deployment, we put 11x11x3 = 363 sensors with 60m transmission range in a 500x500x100m^3 area. The sensors are placed in 3

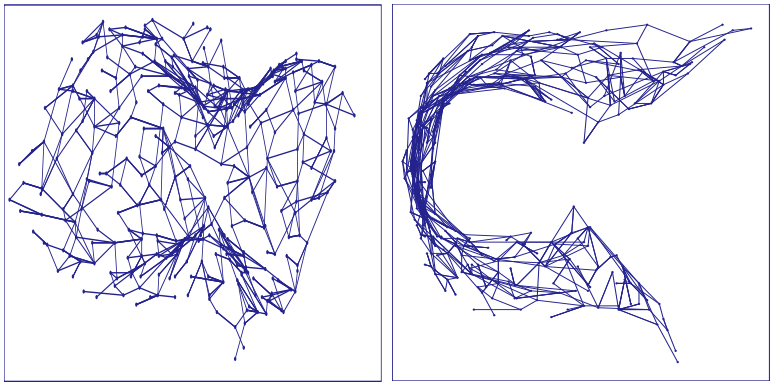
layers, with each layer containing 121 sensors. The size of the grid in the same layer is $50m$. The distance between two neighbor layers is $50m$. The layout is shown in Figure 8.

Figure 8.(a) shows the original layout. Figure 8.(b) shows the global reconstruction conducted by the command center when no wormhole exits in the network (the [-$15m$, +$15m$] distance errors have been added). Figure 8.(c) shows the global reconstruction conducted by the command center when a wormhole exists in the network.

Random deployment For the random placement, we put 350 sensors in a 500x500x $100m^3$ area randomly and roughly uniformly. The average degree of redundancy in deployment is 18.6. Figure 9.(a) shows the global reconstruction conducted by the command center when no wormhole exists. Figure 9.(b) shows the case when a wormhole exists in the network.



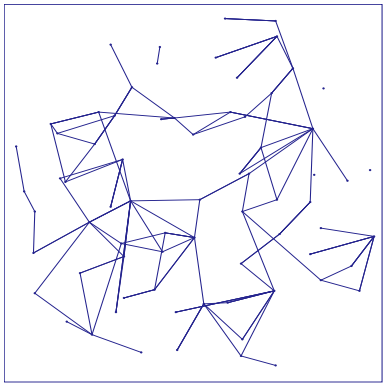
(a) Global reconstruction when no wormhole exists



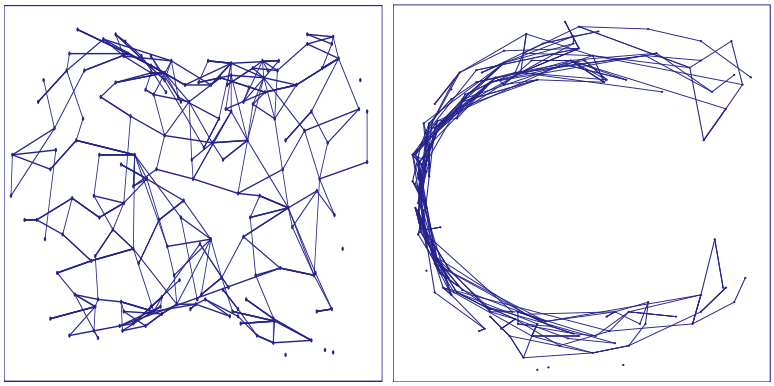
(b) Global reconstructed network by command center when a wormhole exists: front and side

Fig. 9. Impacts of long-haul wormhole (lines drawn on measured distance)

Figure 10 shows the results of local reconstruction. We set the radius of a k-sphere $k_i = 5$. Figure 10.(a) shows the local reconstruction of a k-sphere when no wormhole exists in it. Figure 10.(b) shows the reconstructed network when both ends of the wormhole are in the k-sphere and the wormhole span is 8 hops. Since more random nodes will be included as k-hop neighbors due to the existence of wormhole link, the k-sphere in Figure 10.(b) is denser than the original one.



(a) Reconstructed k-sphere when no wormhole exists



(b) Reconstructed k-sphere when both ends of wormhole are in the k-sphere: front and side

Fig. 10. Impacts of short-range wormhole

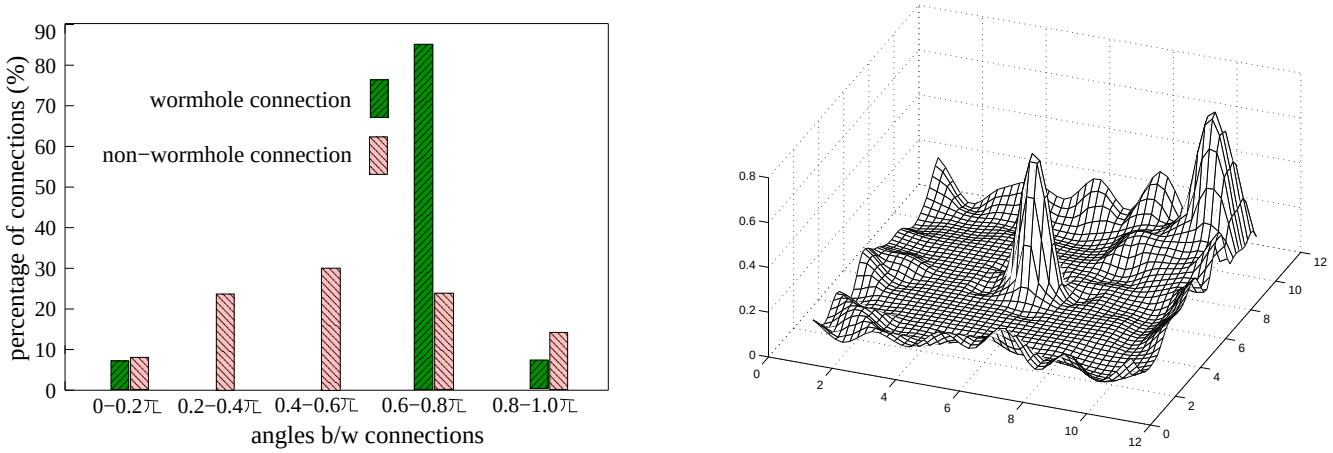
C. Wormhole Detection

The distortion (thus the existence of a wormhole) can be detected by computing the curvature along the reconstructed network surfaces. Once we discover that there are fake neighbor connections in the k-sphere, the

detection mechanism will be activated to locate the ends of the wormhole. Since a wormhole will pull two faraway sensors to each other, the other neighbor connections will form a cone structure at each end of the wormhole, as shown in Figure 9.(b) and 10.(b). This cone structure can be detected by the distribution of the angles between the examined connection and its neighbor connections, as shown in Figure 11.(a). We define the $counter$ of a connection xy as the percentage of its neighbor connections that have an angle $\geq 0.6\pi$ to it. We also define the *wormhole indicator* (WI) of a sensor x as:

$$WI_x = max\{\ counter_{xy} \mid x,\ y\ are\ neighbors\} \tag{1}$$

Figure 11.(b) shows the values of wormhole indicators for the sensors in a k-sphere. We find that the two ends of the wormhole have large WI values and can be easily identified as exceeding a threshold.



(a) anomaly on angle distribution

(b) wormhole indicators for the sensors

Fig. 11. Locating wormhole using the $wormhole\ indicator$.

Wormhole detection in MDS is a probabilistic procedure. Using the WI values to locate wormholes may introduce false positive alarms. For example, the cone structure could have been caused by the water current or underwater geographic features instead of a wormhole. We have adopted two methods to control the false alarms: (1) We use the average difference between the measured distances and the rebuilt connections to examine whether a k-sphere contains a wormhole. If the cone structures are formed naturally, the difference will be small and no detection operation will be conducted. (2) For the connections removed by previous wormhole detection, we can conduct another round of MDS by adding them back to the k-sphere individually. Through examining whether they cause the distortions, we can recover some of the wrongly accused connections.

D. Impact of wormholes and countermeasures

In Figure 3 (Section II) we already showed how the number of wormhole links affect underwater data delivery ratio. Figure 12 shows the same experiment, except we plot the number of traffic flows that are not completely disconnected by wormhole attacks. The trend is very similar to Figure 3. The simulation study shows all traffic flows are not disconnected if the two-tier localization based countermeasure is applied.

In Figure 13 we study the impact of wormhole's physical length. We deploy a single stationary wormhole in the network and vary its length from $\frac{4}{3}R$ to $8R$ (R is the one-hop transmission range). The length extension drops data delivery ratio lower initially, but then the attack's impact is ameliorated. This effect can be justified by Figure 1 and 2, where acoustic signal must travel the distance between the sender/receiver to a wormhole end. When wormhole's length is too long and both ends reach network boundaries, this distance helps mitigating wormhole attacks for random network traffic.

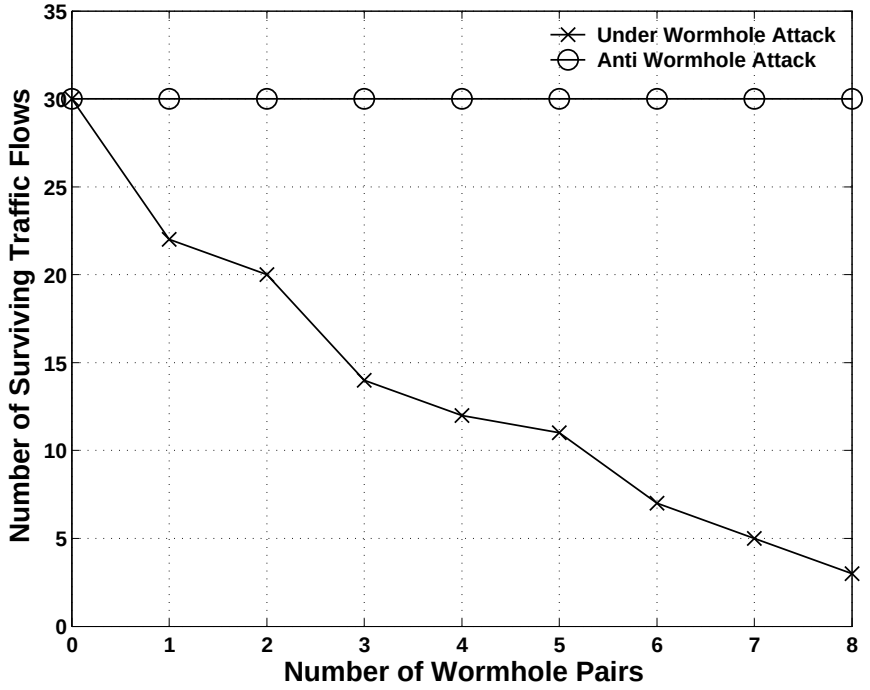


Fig. 12. **Impact of # of wormholes on survived traffic flows**

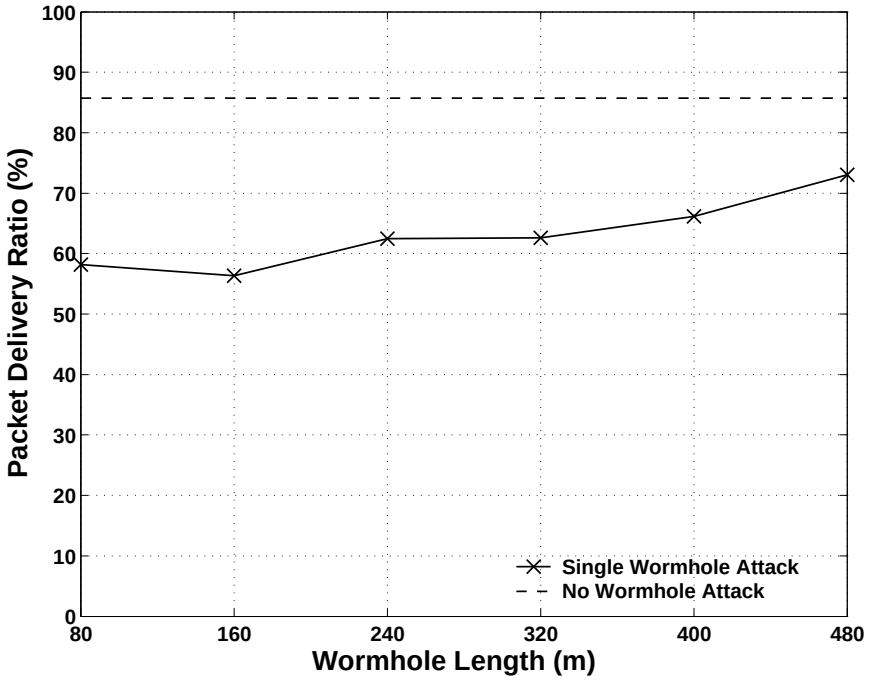


Fig. 13. **Impact of wormhole length**

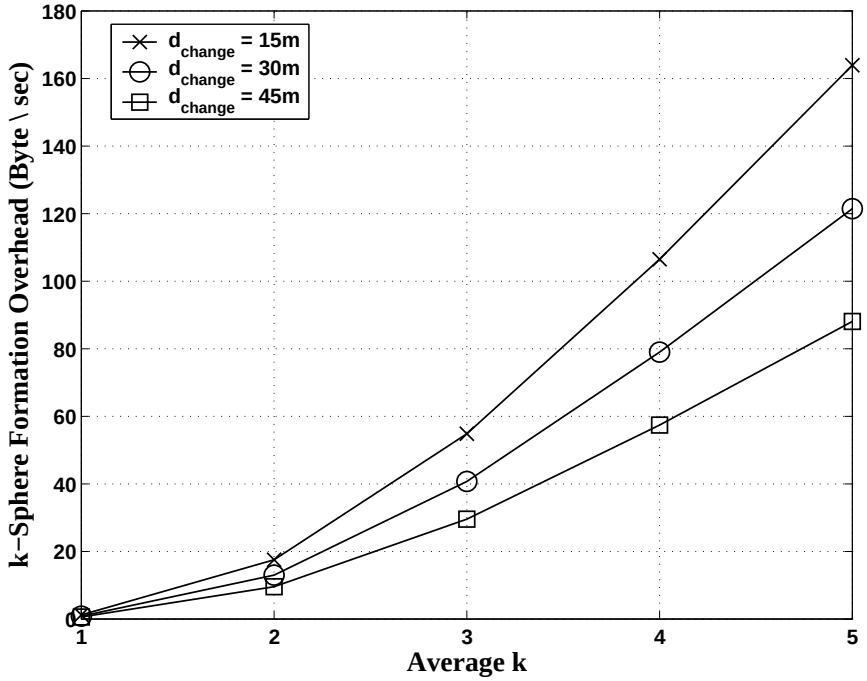


Fig. 14. **Forming k-spheres**

Figure 14 shows the incurred communication overhead for k-sphere formation. During the entire simulation study, we use random way point mobility model with motion speed range 1m/sec–1.5m/sec (approximately 2–3 knots). In such a sensor network with low/medium node mobility, when the average k value in the network increases linearly from 2 to 5 (for $d_{change} = 15m$), the associated communication overhead for k-sphere formation increases from 17 Byte/sec to 163 Byte/sec—a roughly quadratic increment. This is because PD reports are disseminated in a k-sphere whose size increases roughly quadratically[1]. In addition, the incurred communication overhead is also determined by another critical parameter d_{change}. For any pair of sensor nodes, if their pairwise distance change is less than this threshold value since last report, then the newly measured distance is ignored and not disseminated to other nearby nodes. This sacrifices the protocol's precision, but results in less communication overheads. In case $k = 5$, the per-node overhead decreases from 163 Byte/sec to 88 Byte/sec. In a real UWSN deployment, since we can estimate the average k value on available sensor devices, the simulation result can be used to select an appropriate d_{change} given k and communication overhead requirement (which is typically related to energy efficiency concerns).

VII. Conclusion

In this paper, we seek to show that security must be unified into underwater sensor networking in the design phase, but not grafted on as afterthoughts to the architecture. In the Internet, it is argued by security experts that the Internet security suite is added as an after-the-fact intrusion, and the related security problems (e.g., distributed denial-of-service attack, spoofing, spamming) have not been fully answered. In underwater sensor network, we argue that the security attack is an even more pressing problem. We have showed that various kinds of denial-of-service attacks can effectively disable a deployed underwater sensor network.

We adopt an intrusion detection and intrusion recovery approach to answer the challenge. We employ various localization techniques to precisely identify each denial-of-service attacker's location and to isolate them. Secure pairwise distance measurement is the fundamental building block of our design. We propose single-round secure distance bounding protocols, namely DUB and DDB, to implement efficient distance measurement. We prove that DUB and DDB provide valid cryptographic Interactive Proofs between two protocol-compliant nodes. Based on

[1]The size increment should be cubic in a cubic space, but we decided to simulate a somehow "flat" underwater network (2000x2000x200m^3) to approximate the real world scenario. It is well-known that ocean's depth, at most 11km in Mariana Trench and averagely 4km, is much smaller than the length and width.

pairwise distance values, two-tier localization is able to locate short-range and long-haul wormholes in the network. After the wormholes are excluded, the remaining self-organizing sensor nodes provide promised network services as usual. In the foreseeable future, we are looking forward to seeing more and more underwater security attacks and more efficient countermeasures to answer the challenges.

REFERENCES

[1] R. Baldwin and R. Rivest. The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms. `http://www.ietf.org/rfc/rfc2040.txt`, 1996.

[2] S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward. A Distance Routing Effect Algorithm for Mobility (DREAM). In *ACM MOBICOM*, pages 76–84, 1998.

[3] E. Biham. New Types of Cryptanalytic Attacks Using Related Keys. In *Advances in Cryptology–EUROCRYPT'93*, pages 487–496. Spring-Verlag, 1994.

[4] E. Biham and A. Shamir. *Differential Crypanalysis of the Data Encryption Standard*. Spring-Verlag, 1993.

[5] A. Biryukov and E. Kushilevitz. From Differential Cryptoanalysis to Ciphertext-Only Attacks. In *CRYPTO*, pages 72–88, 1998.

[6] A. Biryukov and E. Kushilevitz. Improved Cryptanalysis of RC5. In *EUROCRYPT*, pages 85–89, 1998.

[7] P. Biswas and Y. Ye. Semidefinite Programming for Ad Hoc Wireless Sensor Network Localization. In *ACM IPSN*, pages 46–54, 2004.

[8] J. Borst, B. Preneel, and J. Vandewalle. Linear Cryptanalysis of RC5 and RC6. In *Fast Software Encryption*, pages 16–30, 1999.

[9] S. Brands and D. Chaum. Distance-Bounding Protocols (Extended Abstract). In T. Helleseth, editor, *EUROCRYPT'93, Lecture Notes in Computer Science 765*, pages 344–359, 1993.

[10] R. R. Choudhury, X. Yang, N. H. Vaidya, and R. Ramanathan. Using Directional Antennas for Medium Access Control in Ad Hoc Networks. In *ACM MOBICOM*, pages 59–70, 2002.

[11] S. Čapkun and J.-P. Hubaux. Secure Positioning in Sensor Networks. Technical Report IC/200444, EPFL, May 2004.

[12] S. Čapkun and J.-P. Hubaux. Securing Position and Distance Verification in Wireless Networks. Technical Report IC/200443, EPFL, May 2004.

[13] M. L. Davison. *Multi-Dimensional Scaling*. John Wiley and Sons, 1983.

[14] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. In *ACM CCS*, pages 42–51, 2003.

[15] L. Eschenauer and V. D. Gligor. A Key-Management Scheme for Distributed Sensor Networks. In *ACM CCS*, pages 41–47, 2002.

[16] H. Feistel. Cryptography and Computer Privacy. *Scientific American*, 228(5):15–23, 1973.

[17] O. Goldreich. *Foundations of Cryptography: Basic Tools*, volume 1. Cambridge University Press, 2001.

[18] H. M. Heys. Linearly Weak Keys of RC5. *IEE Electronics Letters*, 33(10):836–838, 1997.

[19] L. Hu and D. Evans. Using Directional Antennas to Prevent Wormhole Attacks. In *Network and Distributed System Security Symposium (NDSS)*, 2004.

[20] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In *IEEE INFOCOM*, 2003.

[21] J.-P. Hubaux, S. Čapkun, and J. Luo. The Security and Privacy of Smart Vehicles. *IEEE Security & Privacy*, pages 49–55, 2004.

[22] X. Ji and H. Zha. Sensor Positioning in Wireless Ad-hoc Sensor Networks with Multidimensional Scaling. In *IEEE INFOCOM*, 2004.

[23] B. Kaliski and Y. L. Yin. On Differential and Linear Crypt-analysis of the RC5 Encryption Algorithm. In D. Coppersmith, editor, *CRYPTO'95, Lecture Notes in Computer Science 0963*, pages 171–183, 1995.

[24] B. S. Kaliski and Y. L. Yin. On the Security of the RC5 Encryption Algorithm. Technical Report TR-602, RSA Data Security, Inc., September 1998.

[25] A. Kaya and S. Yauchi. An Acoustic Communication System for Subsea Robot. In *Oceans'89*, pages 765–770, 1989.

[26] D. B. Kilfoyle and A. B. Baggeroer. The State of the Art in Underwater Acoustic Telemetry. *IEEE Journal of Oceanic Engineering*, OE-25(1):4–27, January 2000.

[27] L. R. Knudsen and W. Meier. Improved Differential Attacks on RC5. In N. Koblitz, editor, *CRYPTO'96, Lecture Notes in Computer Science 1109*, pages 216–228, 1996.

[28] Y. Ko, V. Shankarkumar, and N. Vaidya. Medium access control protocols using directional antennas in ad hoc networks. In *IEEE INFOCOM*, pages 13–21, 2000.

[29] L. Lazos and R. Poovendran. SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks. In *ACM WiSe*, pages 21–30, 2004.

[30] M. Matsui. Linear Cryptanalysis Method of DES Cipher. In *Advances in Cryptology–EUROCRYPT'93*, pages 386–397. Spring-Verlag, 1994.

[31] National Institute of Standards and Technology. Federal Information. Data Encryption Standard, Processing Standards Publication 46-2. `http://www.itl.nist.gov/fipspubs/fip46-2.htm`, 1993.

[32] National Institute of Standards and Technology. Advanced Encryption Standard. `http://csrc.nist.gov/encryption/aes/`, 2001.

[33] C. E. Perkins, E. M. Royer, and S. Das. Ad-hoc On Demand Distance Vector (AODV) Routing. `http://www.ietf.org/rfc/rfc3561.txt`, July 2003.

[34] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar. SPINS: security protocols for sensor netowrks. In *ACM MOBICOM*, pages 189–199, 2001.

[35] J. G. Proakis, E. M. Sozer, J. A. Rice, and M. Stojanovic. Shallow Water Acoustic Networks. *IEEE Communications Magazine*, pages 114–119, November 2001.

[36] R. L. Rivest. The RC5 Encryption Algorithm. In *Fast Software Encryption: Second International Workshop*, pages 86–96, 1994.

[37] N. Sastry, U. Shankar, and D. Wagner. Secure Verification of Location Claims. *RSA CryptoBytes*, 6(1):16–28, 2004.

[38] Scalable Network Technologies (SNT). QualNet. http://www.qualnet.com/.
[39] Y. Shang, W. Ruml, Y. Zhang, and M. P. J. Fromherz. Localization from Mere Connectivity. In *ACM MOBIHOC*, pages 201–212, 2003.
[40] E. M. Sozer, M. Stojanovic, and J. G. Proakis. Undersea Acoustic Networks. *IEEE Journal of Oceanic Engineering*, OE-25(1):72–83, January 2000.
[41] W. Torgeson. Multidimensional Scaling of Similarity. *Psychometrika*, 30:379–393, 1965.
[42] S. Čapkun, L. Buttyán, and J.-P. Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, pages 21–32, 2003.
[43] W. Wang and B. Bhargava. Visualization of Wormholes in Sensor Networks. In *ACM WiSe*, pages 51–60, 2004.
[44] G. G. Xie and J. Gibson. A Networking Protocol for Underwater Acoustic Networks. Technical Report TR-CS-00-02, Department of Computer Science, Naval Postgraduate School, December 2000.
[45] Y. L. Yin. The RC5 Encryption Algorithm: Two Years On. *RSA CryptoBytes*, 2(3):14–15, 1997.