Low-cost Attacks against Packet Delivery, Localization and Time Synchronization Services in Under-Water Sensor Networks*

Jiejun Kong†, Zhengrong Ji†, Weichao Wang‡, Mario Gerla†, Rajive Bagrodia†, Bharat Bhargava*
†Dept. of Computer Science University of California Los Angeles, CA 90095
‡Dept. of EECS University of Kansas Lawrence, KS 66045
*CERIAS and Dept. of Computer Sciences Purdue University West Lafayette, IN 47907
{jkong,jizr,gerla,rajive}@cs.ucla.edu, wangwc@eecs.ku.edu, bb@cs.purdue.edu

ABSTRACT

Under-Water Sensor Networking (UWSN) is a novel network paradigm that is being proposed to explore, monitor and protect the oceans. The unique characteristics of the aquatic environment, namely huge propagation delay, absence of GPS signaling, floating node mobility, and limited (acoustic) link capacity, are very different from those of ground sensor networks. Since underwater networks are mostly autonomous and very difficult to directly monitor by humans, a very important requirement is the built-in protection from automated malicious attacks. In this paper we show that the aquatic environment is particularly vulnerable to attacks and security must be integrated into the UWSN architecture to protect its localization, synchronization and packet delivery services.

Categories and Subject Descriptors

C.2.0 [**Computer-Commmunication Networks**]: General—*Security and protection*

General Terms

Security, Measurement, Performance

Keywords

Underwater Sensor Network, Denial-of-service attack, Mobility, Wormhole length

1. 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. First, the Earth is a water planet and its viability as a base for life is dependent on waters ability to dissolve substances and its ability to significantly transport those substances by both diffusion and advection. To assess the aqueous environment and its role and function, it is therefore necessary to identify the multiple inputs and reservoirs that interact. This calls for the need of *large-scale long-term* and *distributed* data acquisition network for *periodic oceanographic monitoring*. Second, for the past several centuries, the ocean has played an increasingly important role in transportation and military activities. In emergent event investigations, e.g., for marine incidents (especially those involved with chemical pollution and oil spill) and military demands (for example submarine hunting), the state-of-the-art in communication technology has significantly surpassed the state-of-the-art of physical investigation in regard to effectiveness and efficiency. This calls for the need of building a *large-scale short-term* and *distributed* data acquisition network for *time-critical aquatic applications*.

The new UWSN paradigm, however, poses formidable new challenges with respect to existing ground sensor networks. First, UWSN relies on low-frequency acoustic communications because RF radio does not propagate well due to underwater energy absorption. The underwater acoustic link features extremely large latency and low bandwidth. Second, most of the nodes in ground sensor networks are stationary. For effective sensing, most of the underwater sensor nodes are constantly moving, except for some fixed fraction of nodes mounted on the sea floor. Even if the mission does not require motion and relocation, untethered underwater nodes will move due to water currents.

In addition, the UWSN challenge cannot be answered by any existing small-scale Underwater Acoustic Network (UAN) [29] [25] [37]. Here we use a military application to demonstrate the need and usefulness of UWSN rather than UAN. (1) Nowadays satellite technology is capable of scanning the entire Earth surface in hours. Hence the data processing center can identify any surfaced submarine at the granularity of hours on the timeline. However, given the typical mobility speed of a submarine (e.g., 10-15 knots), the submarine hunting task force has to locate the target in an area of hundreds of square nautical miles due to the coarse granularity. (2) Modern submarines (e.g., Russian KILO class) are protected by the newly developed low-probability detection (LPD) technology. To reduce a submarine's acoustic signature, the hull of the submarine is covered with rubber anti-sonar protection tiles to prevent acoustic detection. Its noise level is comparable to ocean's background noise, thus legible acoustic signature may only be collected within a very short distance from the submarine. (3) In addition, modern submarines (e.g., the same KILO class) are capable of launching anti-aircraft missiles from below the water surface. This poses severe threats to nearby manned platforms.

*Part of the work is funded by ONR MINUTEMAN grant N00014-01-C-0016 and NSF NRT grant ANI-0335302.

WiSE'05, September 2, 2005, Cologne, Germany.

An unmanned large scale UWSN is free of any of the troubles described above. A large amount of underwater sensor nodes can be air-dropped to the venue. An area of hundreds of square nautical miles may need thousands of sensor units. At real time, each ad hoc sensor unit monitors local underwater activities and reports sensed data via multi-hop acoustic routes to a distant command center. The probability that the target submarine can escape the large-scale coordinated detection is negligible. Afterward, the UWSN can also be used as a part of an underwater positioning and guide system to direct the anti-submarine torpedo to find and destroy the detected target. Clearly, the advantages of the new UWSN paradigm are: (1) *Localized and coordinated* sensing is far more precise than the existing *remote* telemetry technology, e.g., those relying on directional frequency and ranging (DIFAR) sonobuoys or magnetic anomaly detection (MAD) equipment. (2) *Scalability* of UWSN ensures that a large area can be covered for *time-critical* applications. (3) Casualty ratio is expected to be zero if *unmanned* platforms are used. (4) The *ad hoc* sensor deployment is *low-cost*. Each underwater sensor unit can be bound with an electronically controlled air bladder device. Once the network mission is accomplished, the command center issues commands to trigger all air-bladder devices and all sensors can float to surface to be recycled for next mission.

In order to realize the demanding UWSN paradigm, new models and protocols are required in most layers. One area which will definitely require revisiting (with respect to prior work in ad hoc and ground sensor networks) is vulnerability to security threats. This will be the main focus of our paper. Below, we give a brief revisit of these threats.

First, the threat source could be anywhere anytime in a deployed UWSN, where no clear line of defense exists. 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 localization, time-synchronization, multi-hop routing, and 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, protocols vulnerable to a few compromised nodes are not useful in UWSN. 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 certain pre-defined routing metrics (e.g., hop-count, latency). The quality of any collaborative network service is devastated if an adversary can falsely cheat the network by lying or tunneling, then reducing service quality to minimum.

In this paper, we study security attacks threatening collaborative underwater network services. We show that, no matter what kind of protocol stack we are building, any UWSN can be disabled by low-cost underwater denial-of-service attacks due to the unique characteristics of underwater acoustic channel. In particular, wormhole attack [15] and its variants impose great threat to underwater acoustic communication.

1. We show that low-cost wormhole links of *any* length effectively disrupt communication services in UWSN. The adversary can implement wormholes longer than or shorter than the one-hop transmission range. Because many existing wormhole countermeasures proposed for radio networks [14][32] only ensure that a transmitter and its receiver are physically one-hop neighbors, they *cannot* be used to counter underwater wormholes shorter than one-hop distance. We analyze how the choice of wormhole length affects underwater communications, then use empirical simulation study to verify our analytic conclusions.
2. We show that *jam-and-replay attack* [34] [33] is a special case of wormhole attack where the wormhole length is shorter than one-hop distance. Since the bandwidth of the underwater acoustic channel is very narrow (e.g., tens of kHz), it is hard to resist narrow-band jamming unless we adopt a *jamming avoidance* strategy. That is, the communication protocol is re-executed in the hope that the jammer would miss a round and the communication gets through. As a result, compared to multi-round counterparts, single-round network protocols are appealing in UWSN because single-round protocol re-execution is more practical. We propose to use single-round protocols to measure pairwise neighbor distance for localization services in UWSN.
3. No signal, including those from the adversary, can propagate faster than the radio signals in ground ad hoc networks. Many existing wormhole countermeasures proposed for radio networks [15][32][35] exploit this fact to bound the distance between a sender and its receiver. Nevertheless, under the water such distance-bounding schemes [3] are ineffective against wormholes. We propose to leverage network-wise localization [36] to detect and isolate underwater wormholes. Nevertheless, our simulation study shows that network-wise localization incurs significant overhead. Therefore, currently it is an open challenge to devise an effectual and efficient means to stop underwater wormhole attacks.

The paper is organized as follows. Section 2 presents a new interpretation of related work in radio networks. Section 3 explains why underwater networks are more vulnerable to low-cost denial-of-service attacks. In Section 4 we at first present analytic study to quantify the effectiveness of underwater denial-of-service attacks, then use empirical simulation study to confirm our analytic results. Finally Section 5 concludes the paper.

2. DENIAL-OF-SERVICE IN GROUND SENSOR NETWORKS: A NEW VIEW

2.1 Notations

In the paper we will use the notations shown in Table 1.

Table 1: Notation

V_{max}	3×10^8m/s, radio signal propagation speed in air
V_a	1.5×10^3m/s, the acoustic signal propagation speed underwater
d_{v_1,v_2}	$\sqrt{(x_{v_1}-x_{v_2})^2+(y_{v_1}-y_{v_2})^2}$, physical distance between v_1 and v_2, where v_1 locates at (x_{v_1}, y_{v_1}) and node v_2 locates at (x_{v_2}, y_{v_2}) (3-D cases can be trivially deduced by adding the z-axis)
$f_K(\cdot)$	An encryption or decryption using symmetric K in a symmetric key scheme f (e.g., AES)

2.2 General sensor network security

To realize a scalable sensor network, sensor devices are low-cost and economically viable. They are limited in energy, computation, and communication capabilities. This makes many existing security mechanisms inadequate, and hence inspires new security research, such as efficient key management[10][7][21][4], authentication[24], data privacy and anonymity [22][6], that avoid expensive crypto operations. Cryptography is an essential building block of network security.

Nevertheless, in a self-organizing sensor network the power of cryptographic protection is limited. Many security attacks continue

to threaten sensor networks even if an ideal cryptosystem is efficiently protecting the network.

First, denial-of-service attacks, which could be in the form of (1) depleting sensor's on-device resource (e.g., draining battery by incurring extra computation and communication) and (2) disrupting network collaboration (e.g., routing, data aggregation, localization, clock synchronization), can disrupt or even disable sensor networks even though the network is protected by cryptography.

Second, a scalable sensor network is comprised of large amount of tetherless nodes scattered in a large region, where most sensor nodes are unmanned and unattended in a long time window. If not all nodes are with adequate physical protection, some tetherless and unattended nodes can be captured, compromised, and re-inserted back. Afterwards, cryptography is not an effective means to protect the network from the internal threats. Therefore, a security countermeasure vulnerable to a few compromised nodes is considered ineffective in sensor networks.

In this paper, we study how low-cost denial-of-service attacks, which can be launched by both outsiders and internal attackers, disrupt network services like routing, localization and time synchronization.

2.3 Single-hop wormhole: physical distance $=?=$ topological distance

Compared to active denial-of-service attacks like brute-force jamming, wormhole attack [15] is more "covert" in nature.

- The cost of brute-force jamming is relatively high. Besides, a brute-force jammer can be identified and located from its transmissions [38]. Then the legitimate side can employ physical means to destroy the jamming source. In contrast, as admitted in centralized wormhole detection schemes [36], identifying and locating wormholes in a *distributed* and *mobile* network is an open challenge.
- A wormhole attacker tunnels messages received in one location in the network over a low-latency high-bandwidth 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. For example, in wireless radio networks, the wireless medium is heavily contended at MAC layer amongst neighboring ad hoc nodes. Then the low-latency high-bandwidth wormhole link can be implemented in the form of directional antenna or even wired links.
- In all modern networks, control flows and data flows are separated due to performance concerns. Provided the attacking nodes can differentiate control packets from data packets, the wormhole link can selectively let control packets get through. Then the wormhole link has higher probability to be chosen as part of a route due to its excellent packet delivery capability. Once the wormhole link knows it is en route, it can disrupt network services by dropping data packets or introducing unexpected delay. Clearly, wormhole attack can be regarded as a meta-attack that disrupts the distance measurements or routing metrics amongst legitimate nodes. Then after the meta-attack succeeds, the attackers have abundant choices to selectively filter out critical traffic.

Fortunately, according to Einstein's theory of relativity, V_{max}, the signal propagation speed (not the group speed which could surpass the upperbound V_{max}, but could not be used to deliver information) of electromagnetic waves is an upper-bound, and signal always propagates in the shortest distance in the 4-dimensional time-space universe. Therefore, if a sender's radio signal is received

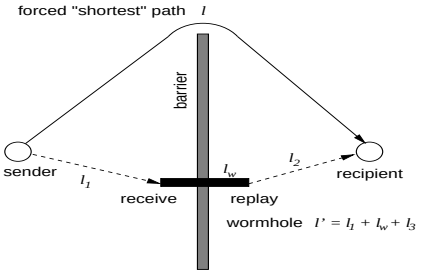

Figure 1: Single-hop wormhole attack

by a one-hop receiver, then the associated latency is more optimal than the one replayed by a wormhole, with an exception depicted in Figure 1:

- The wormhole attacker is a man-in-the-middle between the pair of one-hop sender and receiver. The signal propagation path length through the wormhole is $l' = l_1 + l_w + l_2$.
- The received signal is forced to propagate on a longer path with path length l. And the wormhole's receiving & replaying processing delay $\tau_w < \frac{l-l'}{V_{max}}$.

ATTACK 1. ***(Jam-and-replay attack)*** *In [34][33], a man-in-the-middle can attack sensor localization protocols by jamming a legitimate transmission then replaying the* same *transmission before the expected re-transmissions. It was shown that* malicious distance enlargement attack *[33], a variant of jam-and-replay attack, can disrupt distance bounding protocols [3] by increasing any pairwise distance measurement in a GPS-free localization scheme.*

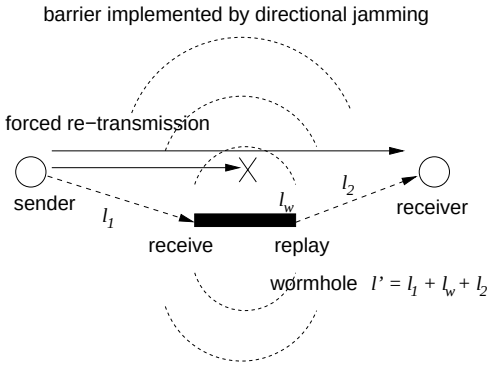

Figure 2: One-hop jam-and-replay attack

In this paper we give the jam-and-replay attack a new interpretation. We illustrate the connection between wormhole attack and jam-and-replay attack.

Unlike a brute-force jammer, this time the attacker is "smarter" and must satisfy many timing constraints. The jam-and-replay attack requires the adversary to intercept the entire legitimate transmission before the real receiver does. Therefore, (1) the adversary's physical presence is between the pair of one-hop sender and recipient. Moreover, (2) the propagation delay is very short, so the adversary must have extra hardware support to launch the attack. For example, the attacker can use directional antenna, which allows the attacker to receive the sender's signal on one direction, and meanwhile jam the signal on other directions. A jam-and-replay attacker is essentially a one-hop wormhole attacker depicted

in Figure 1. In this case the barrier is implemented by directional signal jamming. The attacker succeeds if the wormhole's receiving & replaying delay $\tau_w < \frac{l-l'}{V_{max}} + \tau_{timeout}$*, where* l *is the shortest distance between the sender/receiver pair and* $\tau_{timeout}$ *is the sender's timeout delay for re-tranmission.* ■

Fortunately, in Figure 1, the length of the barrier is proportional to an attacking device's processing latency τ_w. A 1 μs increment in τ_w requires an increment of about $300m$ in the barrier length. As to Figure 2, physical layer mechanisms like spread spectrum have been extensively studied as means of improving resistance to partial-band jamming in wireless radio networks. In a nutshell, a single-hop wormhole in radio networks functions only as a man-in-the-middle, and any anti-jamming support like spread spectrum can largely reduce the effectiveness of its attack. In the extreme case, the network can enforce the *jamming avoidance* policy, which states that a protocol execution must be restarted after jamming interference is detected, until no jamming interference is detected during the entire execution time.

2.4 Multi-hop wormhole: physical distance $\neq$ topological distance

Wormhole attack is a severe threat against any multi-hop wireless ad hoc network, where a source or a forwarder must rely on its ad hoc neighbors in network service provisioning, for example, to deliver packets to the intended recipient or to acquire sensor node positions using a GPS-free localization service. In order to disrupt network services, the wormhole attackers must be able to differentiate control flows from data flows, so that the control flows that pass through the wormholes give the network an incorrect routing or localization metric. Unfortunately, modern computer networks differentiate their control flows and data flows due to performance reasons. No scalable network deployed in practice has ever used uniform packet flows. Control packets are normally short packets that disseminate directives across the network, and data packets are longer in size to serve the need of network applications.

In the Internet, control packets like ICMP, IGMP are all differentiable from data packets in length and traffic pattern. This remark is also true for mobile ad hoc networks and wireless sensor networks, where various routing or diffusion schemes must use short control packets to find packet delivery paths at first. In addition, in networks with node mobility (e.g., UWSN), on-demand discovery is preferred over proactive discovery. Due to the nature of on-demand design, a packet flow initiated after a long idle period is likely a control flow. All of these offer wormhole attackers abundant chances to differentiate packet flows:

Low-cost pairwise wormhole implementation
Prerequisite: Estimated control packet length threshold is l_c. Estimated on-demand idle time threshold is τ_c.
01 IF {an intercepted packet's header is not encrypted}
02 IF {it is a control packet}
03 Let the packet get through the wormhole.
04 ENDIF
05 ELSE
06 IF {(packet is shorter than l_c) OR
(it is the first packet transmitted after τ_c idle time)}
07 Let the packet get through the wormhole.
08 ENDIF
09 ENDIF
10 Otherwise, drop the packet.

Clearly, due to non-cryptographic attacking methods (e.g., line 06 and other feasible implementations), a wormhole attacker is resistant to cryptographic countermeasures. Even if (1) the network is protected by an ideal cryptosystem that is not vulnerable to any cryptanalysis and (2) the wormhole nodes are non-member outsiders, the wormhole attacker can successfully attack the network as long as it can differentiate control packets from data packets. A possible countermeasure in radio networks is to use a uniform length for all packets. But unfortunately this is infeasible in modern networks due to obvious performance reasons. Therefore, wormhole attack requires network-based countermeasures. However, *it is invalid to devise a network-based countermeasure that uses delay-tolerant control flows to counterbalance a wormhole's timing advantage* (e.g., selecting best forwarding path from delayed route discovery flows), because this makes the network protocol further vulnerable to remote wormholes. In radio networks, a typical countermeasure is to ensure that *routing topological neighbors are indeed physical neighbors within bounded distance*:

- 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 legitimate neighbor nodes. This design effectively makes packet transmissions unobservable to the outside wormhole attackers, but is vulnerable to a single point of compromise which reveals the pattern to the adversary.
- Packet leash [15] adopts a wormhole prevention and wormhole detection approach. 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.
- An approach to detect wormholes without clock synchronization is proposed in [32][34][33][35]. Every node is assumed to be equipped with a nano-second hardware that can use various distance bounding protocols [3] to securely bound the transmission distance of communicating parties.
- Another approach is based on the use of directional antennas. In [14], 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 [19] 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 are identified according to system anomalies detected by sector-based location and distance estimation in the one-hop neighborhoods of the locators.

In summary, in radio networks single-hop wormholes are less menacing than their multi-hop counterparts. Thus most existing countermeasures require certain capabilities (e.g., watermarked radio interface, GPS, precise timing device, or directional antenna) to detect wormholes longer than one-hop. This effectively limits a wormhole's length, thus reduces the attacker's threat to single-hop wormhole attack, which in turn is relatively unrealistic in radio networks with anti-jamming or jamming avoidance supports.

3. THE VULNERABLE UWSN

3.1 UWSN characteristics

Underwater acoustic (UW-A) channel Communications in the UnderWater Acoustic (UW-A) channel are with following innate characteristics.

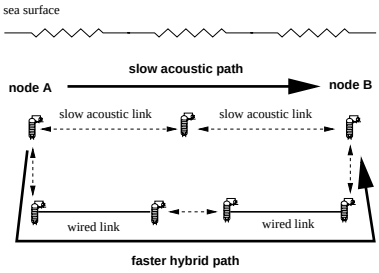

Figure 3: Underwater wormhole (Low-cost underwater devices are connected by wire)

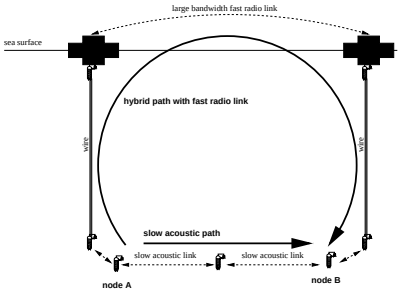

Figure 4: Surface-level wormhole (Low-cost surface-level devices are connected by RF radio)

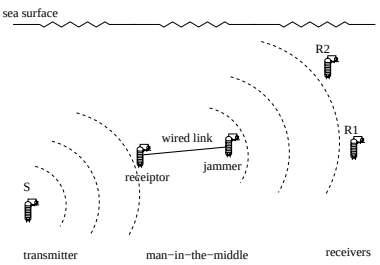

Figure 5: Underwater jam-and-replay attack

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 and most acoustic systems operate below 30kHz [18]. 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 spectrum at the range of 60m radius [17]. The entire width of useful acoustic bands is only a small fraction of useful RF bandwidth. Therefore, compared to radio networks, where narrow-band jamming (partial-band jamming) can be ameliorated by spread spectrum technology[1], which has no analogous counterpart in underwater communications.

Second, as surveyed in [18], 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. This implies a larger transmission latency, which leads to heavier channel contention.

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.

Node assumption Each UWSN node should be a low-cost embedded system equipped with necessary sensing devices. Due to water current and other underwater activities, underwater sensor nodes, except those nodes closely mounted on the sea floor, are with random mobility. From empirical observations, underwater objects may move at the speed of 2–3 knots (or 1.0–1.5 m/s) in a typical underwater condition. Besides, every underwater node may be capable of moving autonomously according to deployment and mission requirements.

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 tetherless and self-organizing.

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 regard to 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.

3.2 Low-cost Underwater Security Threats

As a sub-class of sensor network, UWSN is vulnerable to security attacks threatening all sensor networks. And the cost paid by the attacker is lower than their colleagues in ground networks. The underwater adversary can exploit low bandwidth and huge propagation delay, two innate characteristics of underwater acoustic channel, to strengthen the effectiveness of its attacks.

- *Packet delivery disruption*: As depicted in Figure 3 and 4, in underwater environment attackers can explore fast radio or wired links to significantly decrease propagation delay. *Whether the wormhole length is longer than the legitimate one-hop transmission range or not*, an l_w meters long wired/-wireless link can always gain $\approx \frac{l_w}{V_a}$ms timing advantage. Thus a "hybrid path" features smaller propagation latency as long as it is not more than l_w meters longer than the "slow acoustic path". This makes the wormhole links favored by best-effort routing schemes.

  Besides these physically connected wormholes, jam-and-replay attackers can use another means to implement single-hop wormholes. The underwater acoustic channel also offers jam-and-replay attackers a paradise. As depicted in Figure 5, the attacker can use two low-cost nodes to implement the attack, and *no expensive hardware (such as directional sound ray) is needed on the two low-cost nodes.* Right after the receiptor node receives the last bit, it notifies the jammer node to start jamming (then replaying). As an l_w-meter wired transmis-

[1] 802.11b/g divides the spectrum into 14 overlapping channels of 22MHz each. 802.11a uses three 100 MHz bands for operation in the US.

sion can gain $\approx \frac{l_w}{V_a}$ seconds advantage to acoustic transmissions, there are still $\approx \frac{w \cdot l_w}{V_a}$ legitimate bits in the progress of propagation in an acoustic channel with bandwidth w. These bits are successfully jammed.

- *Localization & synchronization disruption*: Wormhole existence also disrupts any distance measurement schemes relying on measuring the acoustic propagation latency, signal strength and angle-of-arrival. Because GPS is unavailable to tetherless underwater nodes, UWSN has to rely more on GPS-free localization and synchronization designs. Unfortunately, all existing GPS-free localization designs, whether range-free [1] [26] or range-dependent [13] [12], can be easily disabled by security attacks that can disrupt one-hop and/or multi-hop distance measurement (e.g., range, hop-count, etc.). Moreover, GPS-free time-sync protocols rely on broadcast [9] and handshake [11] to do local synchronization. Then various approaches are used to expand local synchronization to multi-hop scenarios (e.g., TPSN [11] uses a post facto expanding method [8], LTS [31] uses an on-demand route) as well as to network-wide scale (e.g., AD [20] uses proactive broadcast. TDP [30] clusters the network according to master node election, and then nodes synchronize with the master nodes). In all such GPS-free time synchronization schemes, disruption in distance measurement is translated into disruption in time measurement. In a nutshell, all these GPS-free localization schemes and time synchronization schemes are vulnerable to wormhole attack and similar distance disruption methods.
- *Resource depletion*: The attackers may choose to invoke energy-hungry operations on sensor nodes. Once critical resources, like battery power, are drained, the gullible sensor nodes are disabled. Feasible attacks may be in the form of incurring excessive data packet losses and re-transmissions (e.g., due to wormhole attack), disseminating false alarms and reports, and depriving sleeping cycles of sensor nodes. Countermeasures against these attacks are extremely important in long-term sensor networks. In this paper we will focus on the impact of wormhole attack which incurs more energy expense on legitimate nodes due to packet losses and retransmissions caused by service disruption.

4. THREAT EVALUATION

In this section we evaluate the impact of underwater security attacks by analytic study and empirical simulation study.

4.1 Analytic study

4.1.1 Aggravated channel contention

It is trivial to remark that UW-A channel is vulnerable to partial-band jamming due to its extremely narrow bandwidth. Moreover, here we also show that the huge propagation delay aggravates channel contention, which is another form of jamming caused by friendly network members.

UWSN is a network with node mobility and thus dynamic neighborhood. This makes deterministic channel access protocols (such as TDMA) unattractive because of the large overhead of maintaining reservation slots in every changing neighborhood. However, random access protocols, even with carrier sensing capabilities, are also aggravated by the unique characteristics of UW-A channel. As Figure 6 shows, nodes B senses the idle channel and starts transmission before the signal from node A arrives. When either node finishes its current transmission and the signal from the other one arrives, it will detect the collision and schedule the next round of

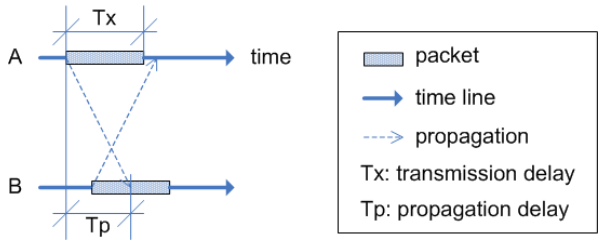

Figure 6: Collision detection in a random access protocol

transmission. It is easy to derive conceptually from Figure 6 that the time of collision detection (T_c) to ensure a collision-free transmission must be

$$T_c = max(T_x, 2T_p)$$

where T_x and T_p are transmission and propagation delays, respectively. In radio networks, T_p is negligible, so $T_c = T_x$. But in underwater networks, the term $2T_p$ can be the decisive factor, so $T_c = 2T_p$ means many new cases of "friendly" jamming. This implies that in UWSN it is much harder to differentiate the real jamming signals from a jam-and-replay attacker and the "friendly" jamming signals from a legitimate member. Clearly, in Figure 2 this helps single-hop wormhole attackers. In addition, any distance evaluation protocol relying on measuring timing difference is disrupted due to potential distance enlargement whenever such (whether malicious or "friendly") jamming signal interferes [33]. Thus the protocol must be re-executed until a round during which there is no interfering signal. Due to this reason, *single-round* distance measurement protocols are preferred over their multi-round counterparts.

4.1.2 Underwater wormhole of any length

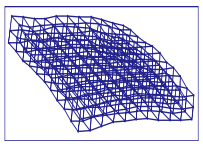

Figure 7: Topological view (without wormhole)

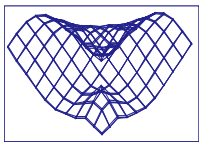

Figure 8: Topological front view (with a wormhole)

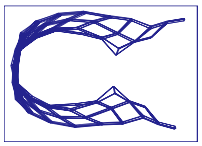

Figure 9: Topological side view (with a wormhole)

Any multi-end wormhole can be treated as a composition of multiple pairwise wormholes. A pairwise wormhole has two ends. Let a (with 2-D coordinates x_a, y_a. 3-D cases can be easily deduced by adding z-axis) denote one wormhole end, and b (with 2-D coordinates x_b, y_b) denote the other end. The wormhole length $l_w = \sqrt{(x_a - x_b)^2 + (y_a - y_b)^2}$. As depicted in the figures, the wormhole shortens the topological distance between the two neighborhoods where its ends locate. This effectively "bends " the network topology (Figure 7, 8 and 9).

For any communication pair v_1 and v_2, the wormhole successfully attacks underwater acoustic communication between v_1 and v_2 when

$$d_{v_1,v_2} > min((d_{v_1,a} + d_{v_2,b}), (d_{v_1,b} + d_{v_2,a})) + \tau_w \cdot V_a, \quad (1)$$

i.e., when the propagation delay of the legitimate transmission is always slower than the one of the wormhole-replayed transmission (even if v_1 sends a acoustic signal directly to v_2). If v_1 and v_2 must communicate via multi-hop forwarding, then Inequation 1 can be relaxed by considering forwarding delay (e.g., queuing delay, transmission delay, processing delay, and delay caused by contention

and jam-and-replay attack). Let τ_h denote the average per-hop delay, and k denotes the number of hops between v_1 and v_2. The extra delay incurred by multi-hop forwarding is $k \cdot \tau_h$. The wormhole successfully attacks the communication between v_1 and v_2 when

$$d_{v_1,v_2} + k \cdot \tau_h \cdot V_a \; > \\ min((d_{v_1,a} + d_{v_2,b}), (d_{v_1,b} + d_{v_2,a})) + \tau_w \cdot V_a \qquad (2)$$

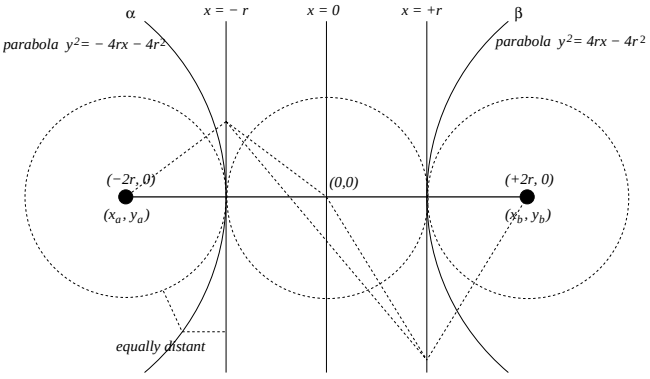

Figure 10: Geometric analysis of wormhole's impact

Figure 10 explains Inequation 1 in details. Without loss of generality, we can define $r = l_w/4$ and a Cartesian coordinate system with one wormhole end at $(x_a = -2r, y_a = 0)$ and the other wormhole end at $(x_b = 2r, y_b = 0)$. We can construct two parabolas: α is defined as the curve $\sqrt{(x+2r)^2 + y^2} = x$ which is equally distant to the y-axis and the point $(-2r, 0)$; and β is defined as the curve $\sqrt{(x-2r)^2 + y^2} = x$ which is equally distant to the y-axis and the point $(2r, 0)$.

The entire network area has following important areas: (1) the area to the left of the parabola α; (2) the area to the right of the parabola β; and (3) the three regions partitioned by the two lines $x = -r$ and $x = r$.

- *Vulnerability*: For any v_1 and v_2, if one of them is in area (1) and the other is in area (2), then the wormhole's attack success ratio is 1.
- *Safety*: For any v_1 and v_2, if both of them are in one of the regions defined in (3) and in the same region at same time, then the wormhole's attack success ratio is 0.
- *Variable cases*: Except the above two extreme cases, the wormhole's attack success ratio depends on v_1 and v_2's exact locations.

To prove "vulnerability", we can choose any node v_1 to the left of parabola α and v_2 to the right of parabola β. Suppose v_1's coordinates is $(-x_1, y_1)$ and v_2's coordinates is (x_2, y_2). The distance via wormhole is less than $x_2 + x_1$ (which is the distance value if v_1 and v_2 are on parabolas), while the direct distance is $\sqrt{(x_2 + x_1)^2 + (y_2 - y_1)^2}$. The latter one is obviously greater than the former one.

To prove "safety" in the middle region, we can connect v_1 and the origin, also v_2 and the origin. The newly connected lines and the line between v_1 and v_2 construct a triangle. The distance between v_1 and v_2 via the wormhole is greater than or equal to the sum of the length of these two newly connected lines, which is longer than the third edge in the triangle. For the left or right region, the triangle property continues to hold, and the distance between one of v_1, v_2 and the opposite wormhole is longer than the distance between this node and the origin. Thus it is trivially true that the distance via wormhole is longer than the direct distance.

Clearly, the "safety" zone is the single wormhole's dead angle, while the "vulnerability" zone is the wormhole's bull's-eye. To attack the network more effectively, the adversary can throw in more wormholes, so that more network areas are "vulnerable" to at least one wormhole.

So far we have ignored the indefinite $k \cdot \tau_h \cdot V_a$ and $\tau_w \cdot V_a$ for the ease of presenting the idea. When the multi-hop delay is considered, the left parabola α and the left partition line $x = -r$ is shifted to the right by $\frac{(k \cdot \tau_h - \tau_w) \cdot V_a}{2}$ distance, and the right parabola β and the right partition line $x = r$ is shifted to the left by the same distance. This effectively enlarges the "vulnerability" zone. This enlargement also shows the difference between underwater networks and radio networks:

- In underwater networks, the two ends of a pairwise wormhole can be treated as a single topological point (as radio signal propagation latency is negligible compared to acoustic delay). This is the reason why wormholes shorter than one-hop range also threaten the network.
- But in radio networks, the above remark is not true. It is the multi-hop delay $k \cdot \tau_h$ that realizes the Inequation 2 and the "vulnerability" zone.

Finally, from Figure 11 we can see the trade-off in selecting wormhole length l_w. A longer wormhole defines a pair of farther but flatter parabolas α_1 and β_1. Compared to the parabolas α_2 and β_2 (defined by a shorter wormhole), the "vulnerability" zone is larger in long range, but smaller in short range. Therefore, *a viable strategy for wormhole attackers is to deploy wormholes of various lengths to strengthen their attacks*.

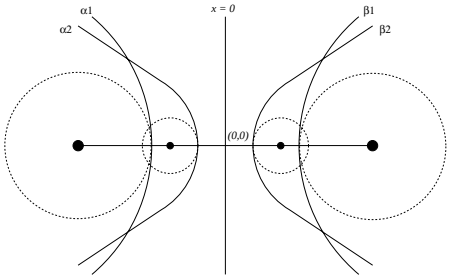

Figure 11: Impact of underwater wormhole length

4.2 Simulation study

4.2.1 Wormhole attack against packet delivery

We use pairwise CBR traffic flows to evaluate the impact of wormhole attack in a revised QualNet simulation environment [27] that is enhanced to simulate underwater acoustic channel. 350 sensor nodes are deployed in a $500 \times 500 \times 100 m^3$ 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 [23] with enlarged timeout values to cope with large propagation delay. The length of each pairwise wormhole is 80m, and the one-hop transmission range R varies from 60m to 180m. As depicted in Figure 12, 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 pairwise wormholes. This means data reports

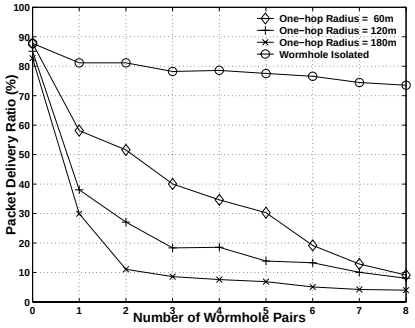

Figure 12: Impact of wormhole attack on delivery ratio

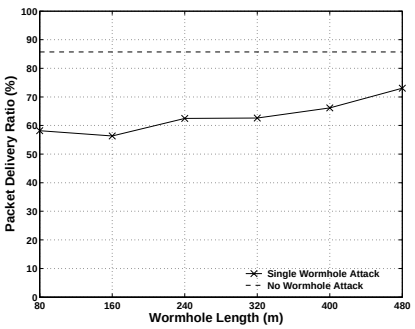

Figure 13: Impact of wormhole length on delivery ratio

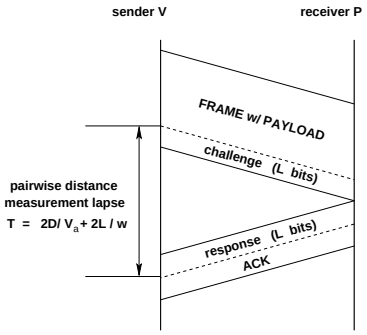

Figure 14: Pairwise distance measurement in 1-round handshake

are more likely to be lost than to be delivered when the enemy throws a few low-cost tiny devices into the network. Finally, we assume an ideal wormhole detection countermeasure can identify all wormholes, and excludes the wormholes in acoustic communication. 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.

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 80m to 480m. The length extension drops data delivery ratio lower initially, but then the attack's impact is ameliorated. This effect is justified by our analytic study: Given a bounded network area, when wormhole's length is too long and both ends reach network boundaries, the "vulnerability" zone decreases in size and this helps mitigating wormhole attacks for random network traffic.

4.2.2 Wormhole attack against localization & synchronization

The high-frequency radio wave used by Global Positioning System (GPS) is quickly absorbed by water, hence cannot propagate under the water surface. Currently it is feasible to use GPS to precisely identify the coordinates of nodes *above* the water surface, or to employ high-end high-cost underwater positioning systems to identify the coordinates of a few underwater nodes within a small area. Neither method has fully addressed positioning and time-synchronization problem for a scalable UWSN. So far to our best knowledge, a scalable, low-cost and secure positioning and synchronization system like GPS is not yet available to underwater nodes. Due to these reasons, we use a GPS-free localization scheme [28] in our evaluation.

Single-round acoustic distance measurement In pairwise distance measurement, a pair of one-hop 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 extra hardware cost. Therefore, a Time-of-Arrival (ToA) approach is a better choice for low-cost underwater networks. Other than off-the-shelf acoustic modems, measuring ToA does not rely on any special hardware.

As depicted in Figure 14, a pair of nodes can estimate their pairwise distance by 1-round handshake. Because the adversary can use *jamming-and-replay attack* to increase the measured distance value between P and V, the 1-round handshake must be restarted whenever any jamming interference is detected during the handshake, until a round during which no interference is detected. This jamming avoidance method is required since anti-jamming spread spectrum is not available under the water.

Protocol A: Pairwise distance measurement in 1-round handshake

Prerequisite: Two underwater neighbors P and V use an acoustic channel with bandwidth w. They share an L-bit long symmetric key K. $f_K(\cdot)$ denotes an encryption or decryption using K in the symmetric key scheme f (e.g., AES).

1 V chooses an L-bit random nonce x, and piggybacks encrypted nonce $f_K(x)$ at the *end* of a unicast packet to P;
2 V's measurement timer starts at the moment when the first bit of x is transmitted;
3 P piggybacks the decrypted x at the *beginning* of its ACK packet;
4 V's measurement timer stops at the moment when the last bit of x is received;
5 The timer returns value T. V computes the distance

$$d = \frac{(T - 2L/w) \cdot V_a}{2}$$

In radio networks, signal propagation delay T_p is negligible compared to transmission delay T_x. Due to this reason, distance bounding protocols used in radio networks [3] [32] [35] must measure time-of-arrival (ToA) using very efficient processings (e.g., bitwise-XOR only). Then after the ToA measurement round(s), a cryptographic round is used to verify whether the ToA measurement rounds are actually executed between the key sharers P and V. This means the distance measurement protocol must be multi-rounds in radio networks.

However, in underwater networks the situation is different. Now T_p dominates T_x. Processing delays that are less than or comparable to T_x are allowed in ToA measurements. In our simulation study, Protocol A is implemented at the link layer, and the processing latency of P (including cross-layer latency the between the physical layer and the link layer and the decryption latency of nonce) is randomly selected between 1ms to 5ms. The deviation in latency measurement only causes slight errors in distance measurement, which is depicted in Figure 7 to show that the reconstructed topology is not a strict grid like what is deployed. Because the processing latency is small compared to propagation latency T_p, the slight deviation does not disrupt the 1-round distance measurement procedure.

Unfortunately, introducing underwater wormholes into the network significantly disrupts the distance measurement.

- *Distance decrement*: This disruption can be caused by worm-

holes implemented by either internal sensor member nodes or merely external outsiders. In both cases, a pair of wormhole nodes P' and P'' in the middle of two uncompromised nodes P and V can shorten the measured distance between P and V.

- *Distance increment*: If 1-round Protocol A is used and distance measurement is collected only when there is no jamming interference detected, then jam-and-replay attackers and external wormholes (implemented by outsiders) cannot increase distance measurement. Thus the distance increment disruption can only be caused by an internal attacker P, who intentionally inserts a chosen period of latency before it sends back the response. Then V will measure an enlarged pairwise distance.

In a nutshell, since distance measurement can be easily disrupted by wormhole attackers. The wormholes must be identified and eliminated to implement GPS-free localization and time-synchronization (as disrupted distance measurement is translated into disrupted time measurement) in underwater environments.

Wormhole detection via network-wise localization We have seen that wormholes shorter than one-hop range is effective, thus countermeasures based on neighbor relation verification [14][32] are ineffective. In addition, as shown above, countermeasures based on distance bounding [15][32][35] are also ineffective due to wormhole's "distance decrement" effect. Instead, we propose to leverage network-wise localization to identify and isolate underwater wormholes.

We do not assume trivial localization solutions like wiring a large number of underwater nodes with surface GPS, or using a precise but expensive system to sequentially locate each underwater sensor. These solutions not only increase per-unit deployment cost, but also impede network's scalability and mobility. In our evaluation, pairwise distance measurements, though disrupted by wormholes, are used as distance vectors in a low-cost localization service based on multi-dimensional scaling (MDS) [5]. In MDS-MAP [28] and other recent efforts [16][2], MDS can rebuild the network topology and generate a virtual position for every active sensor.

As we analyzed early in this section, the attackers will distribute many wormholes with variable lengths into the network. Identifying all of them requires a distributed mechanism to detect a wormhole of any length. Clearly, we can use MDS to reconstruct the transmogrified topology. Figure 7, 8 and 9 illustrate the results of using MDS-VoW [36] to detect and isolate a wormhole link. The figures show that a "curvature" of topology caused by a wormhole of approximately k-hop length must be identified in the k-hop neighborhood (which is called k-sphere in this paper).

Nevertheless, centralized designs [28][2][36] do not fit in a scalable network. A *distributed* solution like [16] is needed in a scalable UWSN. More importantly, none of the above GPS-free localization schemes address node mobility. Due to mobility, all k-spheres must be reconstructed constantly. In our distributed MDS-VoW, we adopt a proactive approach and use constrained flooding to disseminate a pairwise distance measurement up to k hops away. Every MDS-capable sensor node periodically reconstructs its own k-sphere to identify any wormhole inside. This method fails to identify a wormhole if either end of the wormhole is outside of the k-sphere. Thus for long-range wormholes, a larger k must be used. Because the distance vectors disseminated in a larger k-sphere become less fresh and less accurate (ever since the moment when the vectors are measured), this wormhole detection approach is less effective when k increases. It also incurs more communication and MDS-computation overhead when k increases.

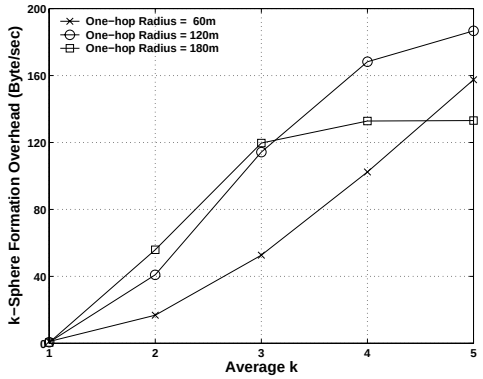

Figure 15: Overhead of reconstructing k-spheres using MDS-MAP

Figure 15 shows the incurred communication overhead for k-sphere reconstruction. 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, the associated communication overhead for k-sphere reconstruction increases from 16 Byte/sec to 149 Byte/sec—a roughly quadratic increment with respect to k. This is because pairwise distance vectors are disseminated in a k-sphere whose size increases roughly quadratically[2]. We also run simulation using larger one-hop transmission range. The results show similar patterns, except the curves are flattened at top (as k-sphere approaches the entire network). In a nutshell, in our current evaluation the legitimate side can pay quadratic cost (to wormhole length) to detect wormholes with high probability using distributed and proactive MDS-VoW. However, obviously we are looking forward to seeing more efficient countermeasures to replace the inefficient quadratic solution.

5. CONCLUSION

In this paper, we seek to illustrate that security must be unified into underwater sensor networking in the design phase. We show various low-cost denial-of-service attacks in the form of wormhole tunneling and jam-and-replay. These attacks exploit innate characteristics of the underwater acoustic channel, thus threaten all UWSNs with any protocol stack implementation. More importantly, in contrast to radio networks, we point out that the attacks are now equally applicable to multi-hop and single-hop scenarios. Therefore, existing countermeasures proposed to protect radio networks, for example by neighborhood verification and distance bounding, cannot be used to protect the vulnerable UWSNs. Many critical network services, such as multi-hop data packet delivery, localization and time-synchronization, are vulnerable to the attacks. We use analytic study and empirical simulation study to verify the fact that the low-cost attacks can disrupt and even disable a deployed UWSN. We propose to leverage network-wise localization to identify and isolate underwater wormholes. We conclude that it is an open challenge to devise an effective and efficient countermeasure against the practical low-cost attacks.

Acknowledgement We thank Guang Yang for discussions on acoustic multiple access control. We also thank all anonymous reviewers who made a number of constructive suggestions.

[2]The size increment should be cubic in a cubic space, but recall that ocean's depth is much smaller than its length and width. Thus we simulate a somehow "flat" underwater network (2000x2000x200m^3) to approximate the real world scenario.

6. REFERENCES

[1] P. Bahl and V. N. Padmanabhan. RADAR: An In-Building RF-Based User Location and Tracking System. In *IEEE INFOCOM*, pages 775–784, 2000.

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

[3] 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.

[4] H. Chan, A. Perrig, and D. Song. Random Key Predistribution Schemes for Sensor Networks. In *IEEE Symposium on Security and Privacy*, pages 197–215, 2003.

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

[6] J. Deng, R. Han, and S. Mishra. Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks. In *IEEE International Conference on Dependable Systems and Networks (DSN)*, pages 594–603, 2004.

[7] 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.

[8] J. Elson and D. Estrin. Time Synchronization for Wireless Sensor Networks. In *International Parallel and Distributed Processing Symposium (IPDPS), Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing*, 2001.

[9] J. Elson, L. Girod, and D. Estrin. Fine-grained Network Time Synchronization using Reference Broadcasts. In *USENIX Operating systems design and implementation (OSDI)*, pages 147–163, 2002.

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

[11] S. Ganeriwal, R. Kumar, and M. B. Srivastava. Timing-sync Protocol for Sensor Networks. In *ACM SenSys*, pages 138–149, 2003.

[12] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher. Range-Free Localization Schemes for Large Scale Sensor Networks. In *ACM MOBICOM*, pages 81–95, 2003.

[13] L. Hu and D. Evans. Localization for Mobile Sensor Networks. In *ACM MOBICOM*, pages 45–57, 2004.

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

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

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

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

[18] 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.

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

[20] Q. Li and D. Rus. Global Clock Synchronization in Sensor Networks. In *IEEE INFOCOM*, 2004.

[21] D. Liu and P. Ning. Establishing Pairwise Keys in Distributed Sensor Networks. In *ACM CCS*, pages 52–61, 2003.

[22] C. Ozturk, Y. Zhang, and W. Trappe. Source-Location Privacy in Energy-Constrained Sensor Network Routing. In *ACM SASN*, pages 88–93, 2004.

[23] 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.

[24] 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.

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

[26] A. Savvides, C.-C. Han, and M. B. Srivastava. Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors. In *ACM MOBICOM*, pages 166–179, 2001.

[27] Scalable Network Technologies (SNT). QualNet. `http://www.qualnet.com/`.

[28] Y. Shang, W. Ruml, Y. Zhang, and M. P. J. Fromherz. Localization from Mere Connectivity. In *ACM MOBIHOC*, pages 201–212, 2003.

[29] E. M. Sozer, M. Stojanovic, and J. G. Proakis. Undersea Acoustic Networks. *IEEE Journal of Oceanic Engineering*, OE-25(1):72–83, January 2000.

[30] W. Su and I. F. Akyildiz. Time-Diffusion Synchronization Protocol for Sensor Networks. *IEEE/ACM Transactions on Networking*, 13(1), 2005.

[31] J. van Greunen and J. Rabaey. Lightweight Time Synchronization for Sensor Networks. In *ACM WSNA*, pages 11–19, 2003.

[32] 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.

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

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

[35] S. Čapkun and J.-P. Hubaux. Secure Positioning of Wireless Devices with Application to Sensor Networks. In *IEEE INFOCOM*, 2005.

[36] W. Wang and B. Bhargava. Visualization of Wormholes in Sensor Networks. In *ACM WiSe*, pages 51–60, 2004.

[37] 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.

[38] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. In *ACM MOBIHOC*, pages 46–57, 2005.