

DISRUPTING PACKET DELIVERY, LOCALIZATION AND SYNCHRONIZATION SERVICES IN UNDER-WATER SENSOR NETWORKS

Jiejun Kong[†], Zhengrong Ji[†], Weichao Wang*, Mario Gerla[†], Rajive Bagrodia[†], Bharat Bhargava*

[†]Department of Computer Science
University of California, Los Angeles

*CERIAS and Department of Computer Sciences
Purdue University

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 in the design phase.

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. 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 scientific exploration, commercial exploitation and coastline protection using unmanned platforms. The ideal infrastructure for this type of extensive monitoring is an Under-Water Sensor Network (UWSN), which employs large amount of distributed, unmanned, and tetherless underwater sensor nodes to locally gather information in a timely manner. A self-organizing, self-reconfigurable network provides a more flexible and fault-tolerant support of sensing, monitoring and surveillance than a tethered system (for instance, a system of sensors tied to buoys).

The new UWSN paradigm, however, poses formidable new challenges with respect to existing ground sensor networks and ad hoc 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 patrolling, 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. 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.

UWSN is also very different from any existing small-scale Underwater Acoustic Network (UAN) [11] [9] [14]. The UWSN relies on *localized* sensing and coordinated networking amongst low-cost sensors and can scale to large populations. In contrast, existing UANs are small-scale networks relying on *remote* teleme-

try or sequential local sensing. Therefore, neither ground sensor networks nor UAN systems can serve as models for the implementation of a *localized, precise, and large-scale underwater sensing technology in a time-critical environment*.

In this work 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. Section 2 briefly illustrates the security attacks that can disrupt localization, synchronization, and data delivery services. Section 3 concludes the paper.

2. UNDERWATER SECURITY THREATS

As a sub-class of sensor network, UWSN is vulnerable to security attacks threatening all sensor networks. The target could be acoustic links, e.g., by passive eavesdropping and active link disruption, or unattended sensor nodes which can be captured, compromised, and re-inserted into the self-organizing UWSN. Moreover, the target could be the inherent requirement of collaborative networking. For example, sensor networks demand a set of cost-efficient means to achieve localization, time-synchronization, and multi-hop data diffusion amongst distributed nodes. 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.

More importantly, underwater adversary can exploit low bandwidth and huge propagation delay, two innate characteristics of underwater acoustic channel, to maximize its attacking strength.

- *Packet delivery disruption*: A wormhole attacker [7] 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 UWSN, the water medium is heavily contended at MAC layer amongst neighboring sensor nodes. Then the low-latency high-bandwidth wormhole link can be implemented in the form of wired links (Figure 1). Wormhole attack can be regarded as a meta-attack that disrupts the distance measurements amongst legitimate nodes. After the meta-attack succeeds, the attackers have abundant choices to selectively filter out critical traffic. Unfortunately, in all modern networks, control flows and data flows are separated due to obvious performance reasons. The wormhole link can selectively let control packets get through. Then the meta-attack succeeds if the wormhole link is 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.
- *Localization & synchronization disruption*: GPS is unavailable to any tetherless underwater node. This calls for GPS-

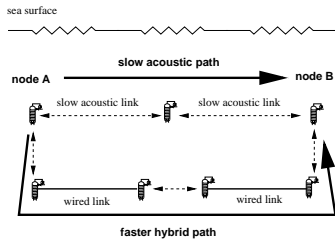


Fig. 1. Underwater wormhole (Low-cost underwater devices are connected by wire)

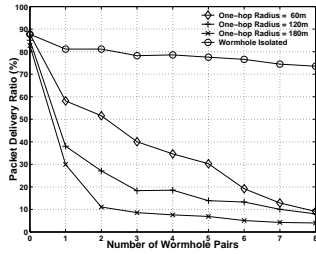


Fig. 2. Impact of wormhole attack on delivery ratio

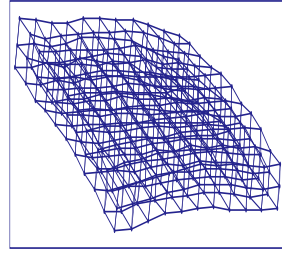


Fig. 3. Topological view (without wormhole)

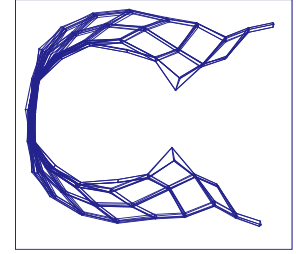


Fig. 4. Topological side view (with a wormhole)

free localization and synchronization designs. Unfortunately, all GPS-free localization designs, whether range-free [1][10] or range-dependent [6][5], 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 [3] and handshake [4] to do local synchronization. Then various approaches are used to expand local synchronization to multi-hop scenarios (e.g., TPSN [4] uses a post facto expanding method [2], LTS [13] uses an on-demand route) as well as to network-wide scale (e.g., AD [8] uses proactive broadcast. TDP [12] clusters the network according to master node election, and then nodes synchronize with the master nodes). All such 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 packet loss and re-transmission (e.g., via wormholes), disseminating false alarms and reports, and depriving sleeping cycles of sensor nodes. Countermeasures against these attacks are extremely important in long-term sensor networks.

2.1. Evaluation

An l meters long wired link can always gain l/v ms delay advantage (where $v=1500$ m/s is acoustic signal propagation speed). This makes the wormhole links favored by best-effort routing schemes. We use pairwise CBR traffic flows to evaluate the impact of wormhole attack in a revised QualNet simulation environment that is enhanced to simulate underwater acoustic channel. 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 wired devices into the network.

Wormhole also disrupts any distance measurement schemes relying on measuring the acoustic propagation latency. As shown in Figure 3 and 4, a pairwise wormhole shortens the topological distance between the two neighborhoods where its ends locate. This effectively “bends” the network topology. To attack the network more effectively, the adversary can throw in more wormholes into the network. In a nutshell, incorrect distance measurement will disrupt GPS-free localization and synchronization services in underwater networks.

3. CONCLUSION

We seek to illustrate that security and resilience components must be unified into underwater sensor networks prior to deployment. Otherwise, if these components are grafted on as afterthoughts to the architecture, then any deployed UWSN can be easily disabled, and we have to pay much higher price to insert the security supports as after-the-fact intrusions. Various low-cost service disruption attacks exploit innate characteristics of the underwater acoustic channel, thus threaten all UWSNs with any protocol stack implementation. Many critical network services, such as multi-hop data delivery, localization and synchronization, are vulnerable to the attacks. We conclude that it is an open challenge to devise an effective and efficient countermeasure against the underwater attacks.

4. 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] 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.
- [3] 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.
- [4] S. Ganeriwal, R. Kumar, and M. B. Srivastava. Timing-sync Protocol for Sensor Networks. In *ACM SenSys*, pages 138–149, 2003.
- [5] 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.
- [6] L. Hu and D. Evans. Localization for Mobile Sensor Networks. In *ACM MOBICOM*, pages 45–57, 2004.
- [7] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In *IEEE INFOCOM*, 2003.
- [8] Q. Li and D. Rus. Global Clock Synchronization in Sensor Networks. In *IEEE INFOCOM*, 2004.
- [9] J. G. Proakis, E. M. Sozer, J. A. Rice, and M. Stojanovic. Shallow Water Acoustic Networks. *IEEE Communications Magazine*, pages 114–119, November 2001.
- [10] 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.
- [11] E. M. Sozer, M. Stojanovic, and J. G. Proakis. Undersea Acoustic Networks. *IEEE Journal of Oceanic Engineering*, OE-25(1):72–83, January 2000.
- [12] W. Su and I. F. Akyildiz. Time-Diffusion Synchronization Protocol for Sensor Networks. *IEEE/ACM Transactions on Networking*, 13(1), 2005.
- [13] J. van Greunen and J. Rabaey. Lightweight Time Synchronization for Sensor Networks. In *ACM WSNA*, pages 11–19, 2003.
- [14] 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.