Security and Privacy in Localization for Underwater Sensor Networks

Hong Li, Yunhua He, Xiuzhen Cheng, Hongsong Zhu, and Limin Sun

ABSTRACT

Underwater sensor networks are envisioned to enable a wide range of underwater applications such as pollution monitoring, offshore exploration, and oil/gas spill monitoring. Such applications require precise location information as otherwise the sensed data might be meaningless. On the other hand, security and privacy are critical issues as underwater sensor networks are typically deployed in harsh environments. Nevertheless, most underwater localization schemes are vulnerable to many attacks and suffer from potential privacy violations as they are designed for benign environments. However, a localization scheme that does not consider security and privacy could lead to serious consequences, especially in critical applications such as military monitoring. In this article, we discuss the security and privacy issues in underwater localization, and investigate the techniques that can provide security and preserve node privacy in underwater sensor networks.

Hong Li is with Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS and George Washington University.

Yunhua He is with Xidian University and George Washington University.

Xiuzhen Cheng is with George Washington University.

Limin Sun and Hongsong Zhu are with Beijing Key Laboratory of IOT Information Security Technology, Institute of Information Engineering, CAS.

Hongsong Zhu is the corresponding author.

INTRODUCTION

Underwater sensor networks consist of a variable number of underwater sensors and vehicles (unmanned underwater vehicles, autonomous underwater vehicles, etc.) to perform collaborative monitoring tasks over a given underwater area. Such a networking technology is envisioned to enable many underwater applications such as pollution monitoring, offshore exploration, and oil/gas spill monitoring.

To support these applications, underwater sensors and vehicles should first configure their locations for various tasks such as data tagging, node tracking, and target detection. Location information is also needed to improve the performance of medium access and network protocols. A large number of underwater localization schemes have been proposed in past years. These schemes typically involve two phases, the *location-related information collection* phase and the *position estimation* phase. In the first phase, nodes measure location-related information such as distance, angle, and hop count to each other or to anchors. In the second phase, their locations are estimated by a centralized node or calculated by themselves locally.

As most of the proposed localization schemes were designed without taking security into consideration, the two phases are both vulnerable to many security threats such as replay attacks, Sybil attacks, and wormhole attacks. Attackers can exploit these security loopholes to interfere with the localization process, or make estimated location imprecise, which could lead to serious consequences in many critical applications such as military monitoring. Furthermore, most of the localization schemes suffer from potential privacy leakage (e.g., location privacy), since a node must reveal a lot of information in order to be localized. Privacy leakage may make the nodes easily captured by enemies. It may also lead to many other security issues such as location spoofing attacks. In this article, we first discuss the security and privacy issues in localization for underwater sensor networks. Then we survey a few secure and privacy-preserving localization schemes and discuss their suitability for underwater sensor networks.

The remainder of this article is structured as follows. First, we present an overview of the localization schemes proposed for underwater sensor networks. Then the security and privacy issues of underwater localization are investigated, respectively. Finally, open research issues and challenges are discussed, and the article is concluded.

THE LOCALIZATION SCHEMES IN UNDERWATER SENSOR NETWORKS

Generally speaking, there are two kinds of nodes in an underwater sensor network: *unknown* or *to-be-localized* nodes with locations that need to be determined, and *anchor*, *reference*, or *beacon* nodes the locations of which are known a priori. Anchor nodes define the coordinate system and provide beacon signals to assist in localizing the unknown nodes. Many localization algorithms have been proposed for underwater sensor networks. These schemes typically consist of a location-related information collection phase and a position estimation phase.

0163-6804/15/$25.00 © 2015 IEEE

Location-Related Information Collection Phase

In the location-related information collection phase, a node estimates its distances, angles, or hop counts to other nodes or to anchor nodes. Such information will be fed to the next phase for position estimation. The methods of information collection can be classified as either range-based or range-free.

Range-Based Approaches: In range-based approaches, the distances between nodes are measured by time of arrival (ToA), time difference of arrival (TDoA), angle of arrival (AoA), or received signal strength indicator (RSSI). For example, the Underwater Positioning Scheme (UPS) [1] estimates the range differences between an unknown node and four anchor nodes based on TDoA. Given the locations of anchor nodes A, B, C, and D (as shown in Fig. 1), UPS calculates the range differences in two steps. In the first step, master node A, which is responsible for initiating a localization process, broadcasts a beacon signal. B replies to A with a beacon signal containing the time difference between receiving A's beacon and sending its own beacon. C replies to A with a beacon containing the time difference between receiving A's beacon and sending its own beacon after receiving beacon signals from both A and B. After receiving the beacons from A, B, and C, D performs the same process as B and C. Sensor S measures the arrival times of the beacon signals from anchor nodes A, B, C, and D locally. In the second step, these time differences are transformed into range differences from the unknown sensor to the anchor nodes, which are used in the trilateration equations to estimate the location of the sensor node.

Range-Free Approaches: In range-free approaches, nodes do not estimate distances or angles; instead, they measure hop count or network connectivity. For example, the Area Location Scheme (ALS) [2] estimates the area where an unknown node resides. In ALS, anchor nodes send out acoustic beacon signals at varying power levels. Each beacon packet contains the ID of the anchor node and the power level at which the signal is emitted. An unknown node passively listens to the beacon packets, keeps a list of IDs and their corresponding power levels, and sends this information to a sink node. The sink node processes the received information to estimate the area in which the unknown node is located based on the anchor nodes' locations and the signal propagation model. This process is illustrated in Fig. 2. Obviously, ALS can only provide a coarse location estimation for the unknown nodes within a certain area.

Position Estimation Phase

In this phase, the positions of unknown nodes are computed based on the information collected in the first phase. Position estimation can be either centralized or distributed.

Centralized Position Estimation: In centralized position estimation, the locations of the anchor nodes and the information collected in the first phase are sent to a centralized node.

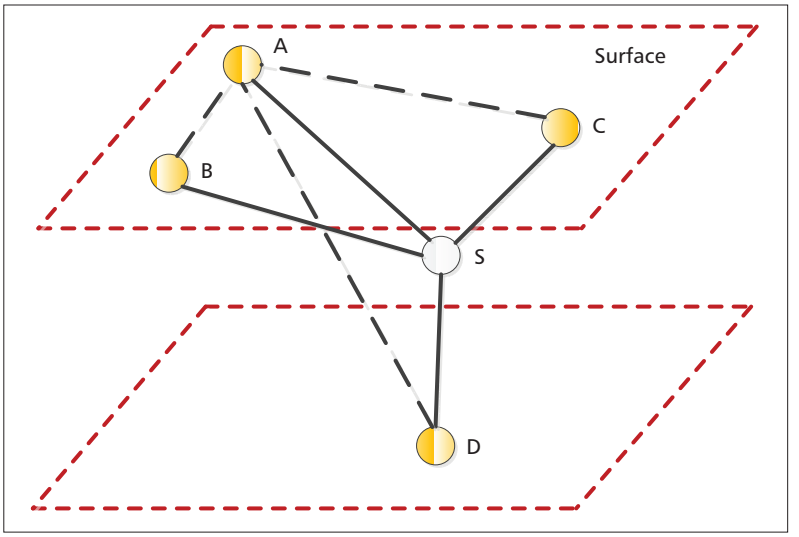

Figure 1. The Underwater Positioning Scheme (UPS).

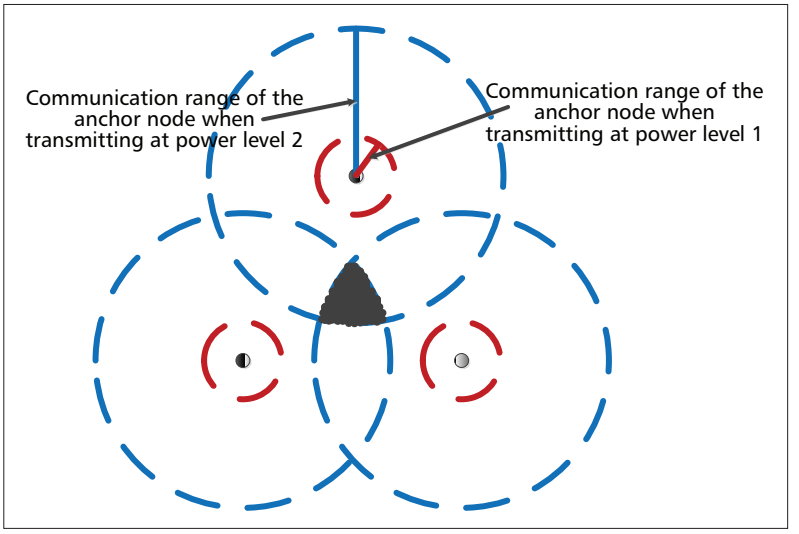

Figure 2. Three anchor nodes send out beacon messages at power levels 1 and 2. If an unknown node receives beacon messages from all three anchor nodes transmitting at power level 2, it resides in the shaded region

The centralized node then estimates locations for all the unknown nodes using techniques such as trilateration, multilateration, and triangulation. An example mechanism, the Hyperbola-Based Localization Scheme (HLS), was proposed in [3], which uses a hyperbola-based approach to localize unknown nodes. As shown in Fig. 3, an unknown node D sends a message to anchor nodes after detecting an event. Anchor nodes A, B, and C receive the message at times t_1, t_2, and t_3, respectively. Then these times and the locations of the anchor nodes are sent to a centralized node. As the difference between AD and BD is a constant that can be estimated by multiplying the speed of acoustic signals and the difference between t_1 and t_2, the unknown node is located on the hyperbola H_{AB}. Similarly, the unknown node is also located on the hyperbola H_{BC}. Then the centralized node can estimate the unknown node's location by computing the intersection of the two hyperbolas.

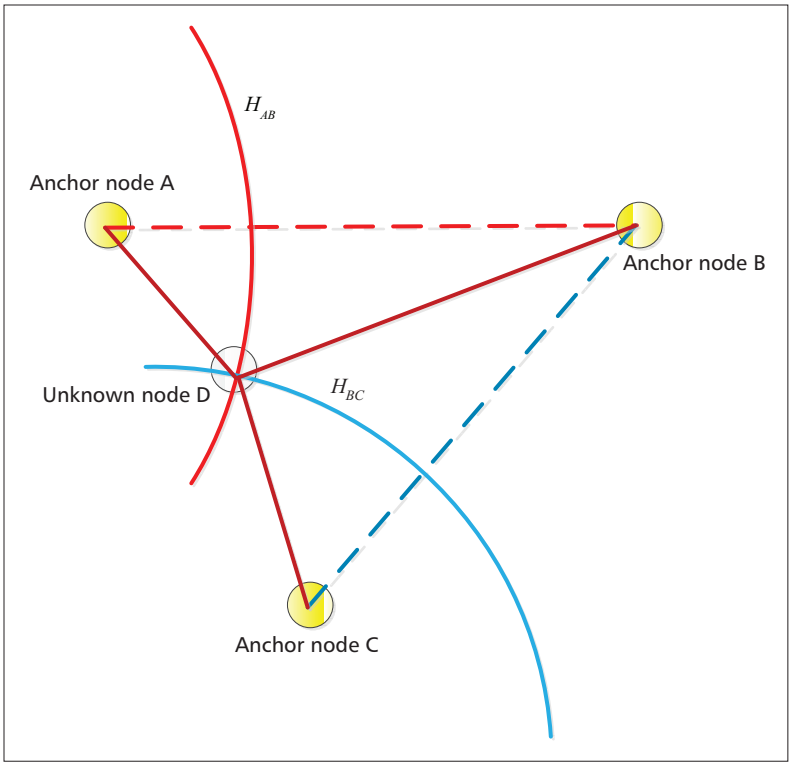

Figure 3. The Hyperbola-Based Localization Scheme.

Distributed Position Estimation: In distributed position estimation, each unknown node runs a localization algorithm locally after collecting location-related information. An example scheme was presented in [4], in which mobile anchor nodes first learn their coordinates via GPS before sinking and then broadcast beacons containing their positions as they are diving. Unknown nodes passively listen to the broadcast messages and use the ToAs of these messages to measure the ranges to the anchors. After hearing from several beacons, unknown nodes locally estimate their positions using triangulation.

Security Attacks on Underwater Localization and Countermeasures

The localization schemes described above perform well in secure environments. However, underwater sensor networks are usually deployed in harsh environments and operate unattended, making them extremely vulnerable to many security attacks. For instance, an attacker can disable the localization system or cause unknown nodes to have imprecise locations, which could lead to severe consequences in many critical applications. In this section, we investigate the security issues of underwater localization, and then discuss the techniques to secure underwater localization.

Attacks on Underwater Localization

DoS Attacks: Underwater localization can be affected by denial of service (DoS) attacks of the following kinds:

- Jamming attack: This is a common attack in wireless networks and has been well studied, especially for terrestrial sensor networks. Underwater links are mainly based on acoustic channels with narrow frequency bands; thus, an attacker can easily interfere with a physical channel to disable the localization process through narrowband jamming.
- Attacking critical nodes: In underwater localization systems, the failure of critical nodes such as anchors could directly affect the localization process. For example, if the master node in UPS [1] is compromised or destroyed by an attacker, the localization process may not be started.

Attacks on Range-Based Measurement: These attacks mainly target range-based localization schemes that first measure the distances between nodes. An attacker can make a node appear closer to or farther away from another node. Such attacks can be launched with many different ways:

- Replay attack: In a replay attack, an attacker first intercepts the message while jamming the legitimate communication channel, and then replays the same message. As with a jamming attack, a replay attack is not specifically designed for underwater localization, but it can also make unknown nodes get imprecise locations. When replay attacks are launched during the location-related information collection phase, an unknown node could get an imprecise propagation time and signal strength, causing imprecise distance estimation based on ToA/TDoA or signal strength.
- Delay/advanced response: In ToA/TDoA-based localization schemes, a node is supposed to reply immediately after receiving other nodes' beacon messages during the location-related information collection phase. A compromised node can delay the reply to appear farther away from the sender, or send the response before receiving other nodes' beacon messages to appear closer.
- Changing transmission power: In some range-based localization schemes, the distance between two nodes is estimated by the signal strength. A malicious node can change its transmission power to make it appear closer to or farther away from other nodes.

Attacks on Range-Free Measurement: In range-free localization, a malicious node can simply adjust its transmission power to change the network topology, which could result in imprecise estimation of hop count and proximity. This phase can also be affected by wormhole attacks. An attacker connects two or more nodes through low-latency direct links (called wormhole links) that can be established by a variety of means such as a cable in underwater. Then one node records a packet at a location in the network and forwards the message to its colluding partners in other parts of the network by wormhole links. After receiving the message, the colluding partners replay it. In this way the wormhole attack changes the network topology and deteriorates the positioning accuracy of range-free localization by either enlarging the neighborhood to affect proximity measurement (e.g., ALS [2]) or shortening the shortest routing

path between two nodes to impact the hop count measurement (e.g., DV-Hop [5]).

Advertising False Information: Since most localization algorithms take locations of the anchor nodes as input, a malicious node can attack the location estimation process by providing false information:

- Providing false locations of the anchor nodes: A compromised anchor can send a false position to unknown nodes or centralized nodes. An advertised false position of an anchor node can lead to erroneous position computation even when the distances are precisely estimated. In [6], the authors showed that a receiver can easily be spoofed to an arbitrary location in GPS localization, which is also possible in underwater localization.
- Providing false range-based/range-free information: In centralized localization, all information collected in the first phase should be sent to a centralized node. Thus, an attacker can forge many identities and advertise erroneous information by a Sybil attack. The erroneous information can largely decrease the accuracy of localization even though other legitimate nodes measure the range-based/range-free information precisely in the first phase.

Non-Cooperation: Most of the localization algorithms require a minimal number of anchor nodes for location estimation. For example, HLS [3] needs at least three anchor nodes. If some of the anchor nodes are compromised or destroyed by an attacker, and the number of anchors falls below a threshold, location estimation can fail. In many distributed localization schemes, unknown nodes should cooperate to estimate their locations, as demonstrated in CLS [7] and UPS [1]. If an attacker compromises some of the nodes and launches DoS attacks, the localization estimation process may not function correctly. In centralized localization, an attacker can disrupt the location estimation process by compromising the centralized node that estimates the locations for the unknown nodes.

Techniques for Securing Underwater Localization

Compared to the traditional security attacks in terrestrial sensor networks, the attacks against underwater localization are more difficult to defend due to the unique characteristics of acoustic channels characterized by high bit error rate, large and variable propagation delay, and low bandwidth. Encryption is a straightforward way to address security attacks, but it consumes a lot of energy, and it also cannot defend against most of the attacks described above. Securing underwater localization is still an unexplored research area. Several secure localization schemes have been proposed in the last few years to provide secure positioning of the nodes in terrestrial sensor networks. Generally speaking, secure localization schemes can be classified into the following categories.

Misbehavior Detection: Such schemes were proposed to detect compromised nodes or location anomalies. In [8], the authors detected malicious anchor nodes by comparing the distance measured from the beacon signal of an anchor node and the distance calculated using the location information provided by the anchor node. If the difference between them is larger than the maximum distance error, the detecting node can infer that the received beacon signal is malicious, as depicted in Fig. 4. In [9], the authors identified location anomalies by verifying whether the derived locations were consistent with the deployment knowledge. In underwater sensor networks, nodes may drift with water current and oceanographic animals, rendering the proposed schemes mentioned above inapplicable underwater.

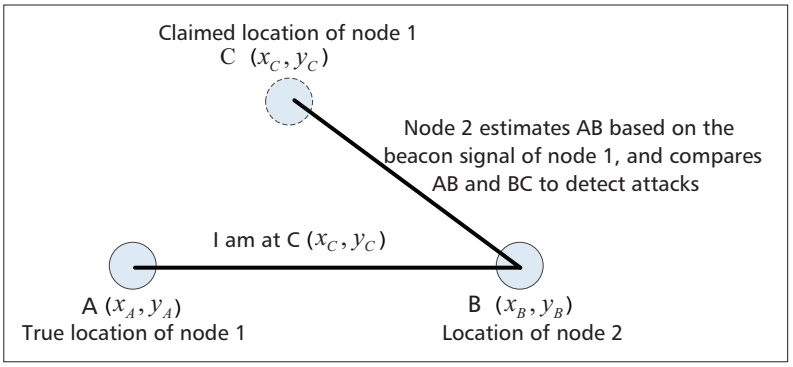

Figure 4. If malicious node 1 advertises a false location C, the difference between AB and BC should be larger than the measurement error.

Robust Location Computation: Robust location computation aims to precisely estimate unknown nodes' locations in an untrusted environment. In [10], the authors developed two attack-resistant location estimation techniques to tolerate the malicious attacks against range-based location discovery in wireless sensor networks. The proposed scheme first identifies malicious location references by examining the inconsistency among them (indicated by the mean square error of the estimation), and defeats malicious attacks by removing malicious data. Then each anchor node votes on the cell in which the node may reside. In [10], the authors proposed a range-independent localization scheme called SeRLoc, which is robust against wormhole attacks, Sybil attacks, and the compromising of network entities. SeRLoc first detects attacks based on properties such as sector uniqueness and communication range violation using directional antennas and then filters out the attacked locators. Finally, unknown nodes determine their locations based on the beacon information transmitted by the locators, which are equipped with omnidirectional antennas.

Location Verification: Location verification schemes try to validate the reliability of location computation. In [12], the authors proposed a distance bounding protocol that can be used to verify the proximity of two devices connected by a wired link. In [13], the authors presented an Echo protocol to verify whether a node is inside a particular region. In Echo, a verifier sends a packet containing a nonce to the prover using RF; then the prover immediately echoes the packet back to the verifier using ultrasound; finally, the verifier checks whether the prover node is in the claimed region by estimating the round-trip time. This process is depicted in Fig. 5.

In many critical applications, the positions of the sensor nodes are very sensitive. Location privacy leakage could bring many problems. For example, enemies can easily destroy the anchor nodes to disable the whole network if they harvest the locations of the anchors in a military reconnaissance application.

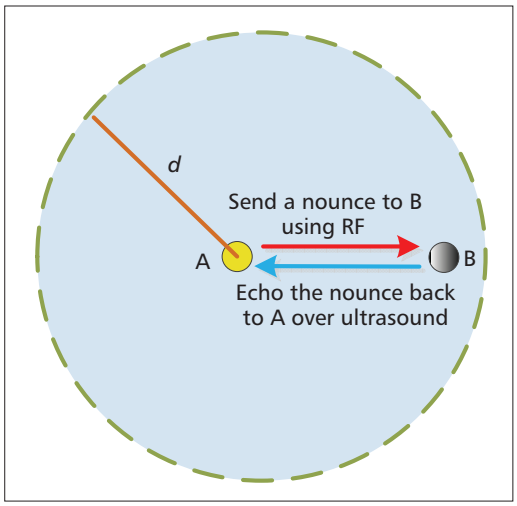

Figure 5. If node B claims that it is located within the circle with a radius d centered at node A, the round-trip time should be less than $d/c + d/s$, where c is the speed of light and s is the speed of ultrasound.

Privacy Issues in Underwater Localization and Countermeasures

Besides the security attacks mentioned above, underwater localization also suffers from privacy vulnerabilities since a node must reveal certain information in order to be localized.

Identity Privacy of Underwater Localization

In most underwater localization schemes, different types of nodes may have different traffic patterns. For example, anchor nodes may periodically broadcast beacon messages while the node in charge of position estimation in a centralized localization mechanism may send the computed location information back to all the unknown nodes. Therefore, an attacker can thus simply sniff the traffic and then infer the identities of the nodes based on the traffic patterns. If a critical node is identified, it might be disabled by the attacker, causing the whole localization system to fail. Such an identity privacy disclosure may also result in other security vulnerabilities.

Location Privacy of Underwater Localization

In many critical applications, the positions of the sensor nodes are very sensitive. Location privacy leakage could bring many problems. For example, enemies can easily destroy the anchor nodes to disable the whole network if they harvest the locations of the anchors in a military reconnaissance application. Location privacy leakage may also lead to other security attacks such as the location spoofing attack. In the following, we discuss the location privacy issues in the location-related information collection phase and the location estimation phase.

Location Privacy in Location-Related Information Collection: In this phase, anchor nodes or unknown nodes broadcast beacon messages to measure the range, hop count, or network connectivity information. Attackers can passively sniff the beacon messages and estimate the distance to the sender based on the signal propagation model at different locations. Then the sender's location can be estimated using trilateration, as depicted in Fig. 6a. An attacker can also pretend to be an anchor node or unknown node and calculate its distances to authentic unknown/anchor nodes using TDoA, ToA, or RSSI at different locations; then it utilizes the computed range information to estimate the anchor's location by trilateration.

Location Privacy in Position Estimation: In both centralized and distributed localization, the positions of the anchor nodes are fed into the localization algorithms; thus, the anchors need to reveal their locations to the centralized node or all the unknown nodes, rendering such information potentially learnable by other nodes, as depicted in Fig. 6b. On the other hand, in centralized localization, the positions of all the unknown nodes are estimated by the centralized node, which implies that knowledge of the unknown nodes' locations is not limited to the unknown nodes themselves. If the centralized node is compromised, the unknown nodes' location privacy is violated.

Techniques to Preserve Privacy in Underwater Localization

Several schemes have been proposed in the past year to address the privacy issues in localization. The authors in [14] proposed a multi-lateral privacy-preserving localization mechanism in pervasive environments based on secure least squared error (LSE) estimation. In this scheme, privacy is protected as the position of an unknown node is calculated without the need to reveal anchors' locations, and the knowledge of the localization outcome is strictly limited to the unknown node itself. The authors in [15] developed a Privacy-Preserving WiFi Fingerprint Localization scheme (PriWFL), which utilizes homomorphic encryption to hide an unknown node's location during the localization process while preserving the location accuracy. These two schemes either involve a high communication overhead or require large computation capacity due to the use of computationally intensive cryptographic algorithms. Therefore, they cannot be used in underwater localization since the bandwidth of the acoustic links and the energy of underwater sensors are limited.

Open Research Issues and Challenges

Although many schemes have been proposed to secure the localization process and preserve the node privacy in terrestrial wireless sensor networks, they are not applicable underwater due to the unique characteristics of acoustic channels. In terrestrial wireless sensor networks, nodes use RF to establish the communication infrastructure. However, radio waves propagate at

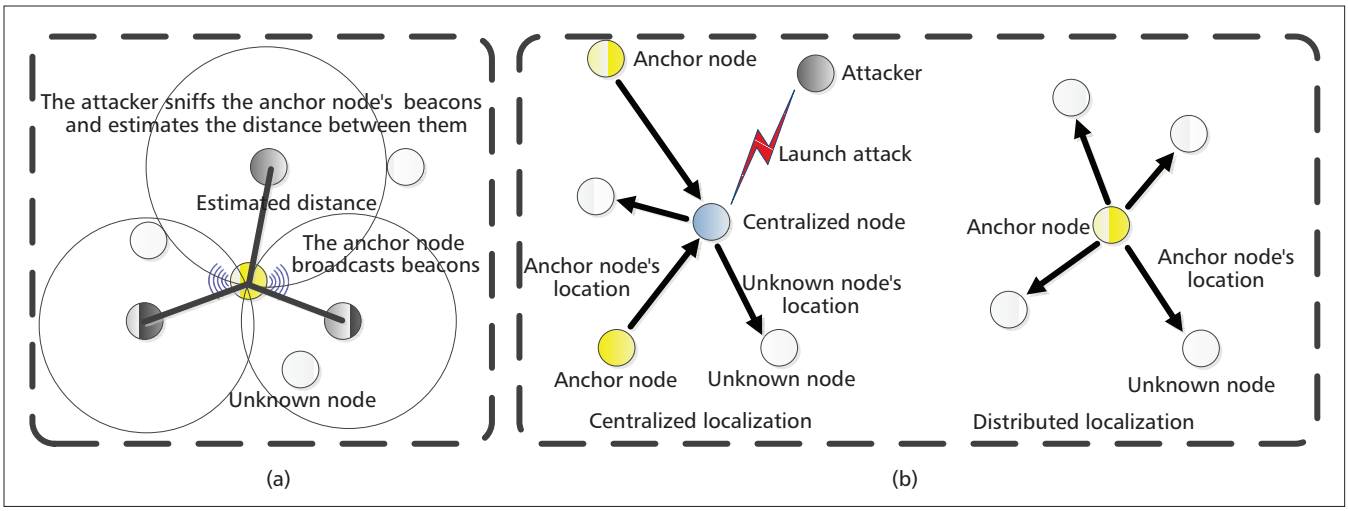

Figure 6. Location privacy leakages in underwater localization: a) location privacy leakage in the location-related information collection phase; b) location privacy leakages in the location estimation phase.

long distances through conductive sea water only at low frequencies (30–300 Hz), which requires large antennae and high transmission power. Therefore, underwater links are mainly based on acoustic wireless communication, which is characterized by high bit error rate, large and variable propagation delay, and low bandwidth. Securing underwater localization and preserving privacy are thus full of challenges. In the following, we summarize the major open research issues for securing localization and preserving privacy in underwater localization:

- Attack detection and location verification in a dynamic underwater environment. Under water, nodes can move with the water current and oceanographic animals, which complicates attack detection and location verification.
- Robust location computation in a noisy environment. The high bit error rate induced by fading, multipath, and refractive properties of the sound signal can cause transmission errors of critical security packets, which may lead to failure of secure localization schemes.
- Lightly weighted privacy-preserving schemes in resource-constrained underwater environments. Since acoustic channels are narrowband, and underwater nodes are energy-limited, the main challenge of designing a privacy-preserving scheme is how to make it lightly weighted without sacrificing location accuracy.

Conclusion

In this article, we discuss the security and privacy issues in underwater localization. We first review the major localization algorithms proposed for underwater sensor networks. Then we introduce the attacks against underwater localization and summarize a few secure localization schemes. We also analyze the privacy issues in underwater localization and discuss techniques for privacy preservation during the localization process. Finally, we outline the open research challenges of secure and privacy-preserving underwater localization.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Grant No. 61472418), National High Technology Research and Development Program of China (Grant No. 2013AA011102), and the "Strategic Priority Research Program" of the Chinese Academy of Sciences (Grant No. XDA06040100).

References

[1] X. Cheng *et al.*, "Silent Positioning in Underwater Acoustic Sensor Networks," *IEEE Trans. Vehic. Tech.*, vol. 57, no. 3, 2008, pp. 1756–66.

[2] V. Chandrasekhar and W. Seah, "An Area Localization Scheme for Underwater Sensor Networks," *IEEE OCEANS 2006-Asia Pacific*, 2007, pp. 1–8.

[3] T. Bian, R. Venkatesan, and C. Li, "Design and Evaluation of a New Localization Scheme for Underwater Acoustic Sensor Networks," *IEEE GLOBECOM 2009*, pp. 1–5.

[4] M. Erol, L. F. Vieira, and M. Gerla, "Localization with *Dive'n'Rise* (DNR) Beacons for Underwater Acoustic Sensor Networks," *Proc. 2nd Wksp. Underwater Networks*, ACM, 2007, pp. 97–100.

[5] D. Niculescu and B. Nath, "Dv Based Positioning in Ad Hoc Networks," *Telecommun. Sys.*, vol. 22, no. 1–4, 2003, pp. 267–80.

[6] N. O. Tippenhauer *et al.*, "On the Requirements for Successful GPS Spoofing Attacks," *Proc. 18th ACM Conf. Comp. and Commun. Security*, ACM, 2011, pp. 75–86.

[7] D. Mirza and C. Schurgers, "Collaborative Localization for Fleets of Underwater Drifters," *IEEE OCEANS 2007*, 2007, pp. 1–6.

[8] D. Liu, P. Ning, and W. Du, "Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks," *Proc. 25th IEEE Int'l. Conf. Distrib, Comp, Sys,*, 2005, pp. 609–19.

[9] W. Du, L. Fang, and P. Ning, "Lad: Localization Anomaly Detection Forwireless Sensor Networks," *Proc. 19th IEEE Int'l. Parallel and Distrib, Processing Symp.*, 2005, pp. 41a–41a.

[10] D. Liu, P. Ning, and W. K. Du, "Attack-Resistant Location Estimation in Sensor Networks," *Proc. 4th Int'l. Symp. Info. Processing in Sensor Networks*, IEEE Press, 2005, p. 13.

[11] L. Lazos and R. Poovendran, "Serloc: Robust Localization for Wireless Sensor Networks," *ACM Trans. Sensor Networks*, vol. 1, no. 1, 2005, pp. 73–100.

[12] S. Brands and D. Chaum, "Distance-Bounding Protocols," *Advances in CryptologyłEUROCRYPT'93*, 1994, Springer, pp. 344–59.

[13] N. Sastry, U. Shankar, and D. Wagner, "Secure Verification of Location Claims," *Proc. 2nd ACM Wksp. Wireless Security*, 2003, pp. 1–10.
[14] T. Shu *et al.*, "Multi-Lateral Privacy Preserving Localization in Pervasive Environments," *2014 Proc. IEEE INFOCOM*, Apr. 2014, pp. 2319–27.
[15] H. Li *et al.*, "Achieving Privacy Preservation in WiFi Fingerprint-based Localization," *2014 Proc. IEEE INFOCOM*, 2014, pp. 2337–45.

Biographies

HONG LI is a Ph.D. student at the University of the Chinese Academy of Sciences. He received his B.A. from Xi'an Jiaotong University. He currently works under Prof. Limin Sun in the Institute of Information Engineering, Chinese Academy of Sciences. His primary research interests include security and privacy in wireless networks, and localization.

YUNHUA HE is a Ph.D. student at Xidian University. He received his B.A. from Wuhan insititute of Technology. He currently works under Prof. Limin Sun at the Beijing Internet of Things Security Center. His primary research interests include location privacy for vehicular ad hoc network, and incentive mechanisms for mobile social networks.

LIMIN SUN [M] received his B.S., M.S., and Ph.D. degrees from the College of Computers, National University of Defense Technology in 1988, 1995, and 1998, respectively. Currently, he is a professor in the Institute of Information Engineering, Chinese Academy of Sciences. His research interests include security and privacy in wireless networks, wireless sensor networks, and the Internet of Things. He is a Senior Member of the China Computer Federation (CCF).

XIUZHEN CHENG [F] received her M.S. and Ph.D. degrees in computer science from the University of Minnesota — Twin Cities in 2000 and 2002, respectively. She is a professor in the Department of Computer Science, The George Washington University, Washington, DC. Her current research interests include cyber physical systems, wireless and mobile computing, sensor networking, wireless and mobile security, and algorithm design and analysis. She worked as a program director for the U.S. National Science Foundation (NSF) for six months in 2006 and joined the NSF again as a part-time program director in April 2008. She received the NSF CAREER Award in 2004.

HONGSONG ZHU [M] (zhuhongsong@iie.ac.cn) received his Ph.D. degree from the Institute of Computing, Chinese Academy of Sciences. He is an associate professor in the Institute of Information Engineering, Chinese Academy of Sciences. His research interests include security and privacy in wireless networks, indoor localization, wireless sensor networks, and the Internet of Things. He is a Senior Member of CCF.