Challenges in Secure Underwater Wireless Sensor Network with Fine-grained Access Control

Donghyun Yu† and Jemin Lee*
†Daegu Gyeongbuk Institute of Science and Technology (DGIST), South Korea
*Sungkyunkwan University (SKKU), South Korea
Email: xaos4715@dgist.ac.kr, jemin.lee@skku.edu

***Abstract*—Underwater wireless sensor networks (UWSN) are increasingly critical for various maritime activities, including military applications and underwater resource exploration. However, UWSN encounters significant challenges in ensuring secure, accurate, and low-latency communication. The differences between UWSN and terrestrial wireless sensor networks (WSN), such as lower device performance, higher communication cost and latency, and mobility, create obstacles in directly applying WSN security solutions to UWSN. This paper discusses these challenges and security solutions to meet the unique requirements of UWSNs.**

***Index Terms*—Underwater communcation, access control, attribute-based encryption, lightweight cryptosystem, lightweight authentication and key agreement**

I. Introduction

Expanding human activities beyond terrestrial domains into the underwater domains has led to a steady increase in underwater endeavors, involving underwater drones, submarines, and marine resource exploration. Consequently, this trend poses significant challenges for underwater wireless sensor networks (UWSN) communication, particularly concerning security, accuracy, and low-latency requirements. Despite the critical importance of addressing these challenges, research in this area remains relatively limited, necessitating more robust investigations, especially in the domain of security.

There are several differences between UWSN and terrestrial wireless sensor networks (WSN), and these differences significantly influence the security of UWSNs. For instance, UWSN sensor nodes have inferior device performance compared to WSN sensor nodes, are more prone to failures, and generally exhibit mobility. Additionally, UWSNs incur considerably higher communication costs and experience greater latency compared to WSNs [1].

Although we are familiar with various research endeavors aiming to address security issues in WSNs, applying these solutions directly to UWSNs becomes challenging due to the inherent differences between the two. Specifically, UWSN sensor nodes have inferior device performance compared to WSN sensor nodes, making it difficult to implement computationally demanding cryptographic techniques such as public key-based cryptography that require high computational power and large memory capacity. Additionally, traditional authentication and key agreement mechanisms require a large number of communication and can have a significant impact in UWSN with high communication cost.

This work was supported by Korea Research Institute for defense Technology planning and advancement(KRIT) - grant funded by the Defense Acquisition Program Administration(DAPA) (KRIT-CT-22-078).

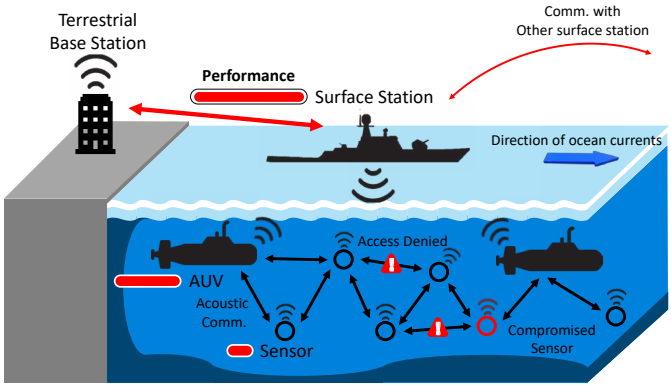

Fig. 1: An environment of underwater wireless sensor networks (UWSN)

Based on these challenges, some works [2]–[4] have introduced the anticipated security threats, challenges, and security requirements in UWSN. These include basic security requirements such as confidentiality, authentication, and integrity that should be achieved in UWSN. However, the increasing underwater activities demand UWSN to achieve the same level of security as WSN. To achieve this, the system should be designed to support advanced cryptographic techniques even on UWSN's low-performance devices.

Fine-grained access control is granting or denying data access based on multiple conditions to prevent unauthorized access and data exposure. It is necessary for efficient and secure data sharing among devices in WSN [5], and it may also be crucial for achieving a high level of security in UWSN. In particular, since underwater devices handle sensitive data and possess mobility, fine-grained access control can be considered an essential security requirement. Therefore, this paper discusses the constraints and distinctive features of UWSN and describes the methods to achieve fine-grained access control and lightweight authentication and key agreement mechanisms in UWSN. Subsequently, it introduces future research directions for UWSN security solutions.

II. Constraints and Distinctive Features of UWSN

In this section, we provide a brief overview of the constraints and distinctive features in UWSN.

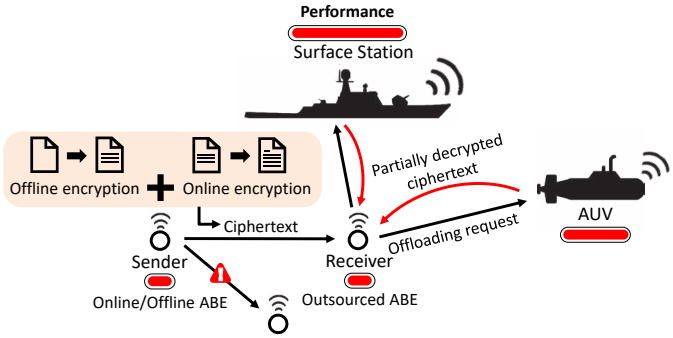

Fig. 2: Overview of outsourced ABE and online/offline ABE in UWSN

A. Low Device Performance

As shown in Fig. 1, UWSN sensor nodes often have an extremely constrained power supply compared to WSN, necessitating energy-efficient and low-power data processing. These drive the adoption of lightweight cryptosystems for encryption and authentication purposes [3], [4].

B. Expensive Communication Cost and High Latency

Unlike WSN which uses RF communication, UWSN utilizes specialized underwater communication technologies like acoustic communication. This can lead to relatively shorter communication distances and higher signal attenuation, resulting in expensive communication costs and long latency. Thus, the authentication and key agreement mechanisms in UWSN should minimize the number of communications.

C. Prone to Failures

Due to the unique nature of UWSN, sensor nodes are exposed to more physical constraints such as water temperature, pressure, and ocean currents, which can lead to more frequent device failures. Such failures can expose security vulnerabilities and make UWSNs susceptible to various attacks like device intrusion and control. Therefore, the addition and revocation of devices and secret keys should be flexible in UWSN [3], [4].

D. Device Mobility

Unlike WSN, where device mobility is generally limited, devices in UWSN have relatively greater mobility, given their unique roles in tasks like data collection. As a result, this mobility demands reliable authentication and access control mechanisms for devices whenever they move. Additionally, tracking and ensuring privacy protection for mobile devices are required [1], [3], [4].

III. Lightweight Cryptosystem for Fine-grained Access Control

This section describes a technique that allows attribute-based encryption (ABE) [6], the most well-known cryptosystem to achieve fine-grained access control, to be efficiently utilized in low-performance devices in UWSN.

A. Attribute-based Encryption (ABE)

It is public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes. In the ABE, successful decryption of a ciphertext is possible only when the attributes in the user key match attributes in the ciphertext. It generally involves computationally expensive operations such as exponential operations and pairing operations, which cause long computation times on low-performance devices.

B. Outsourced Attribute-based Encryption [7]

In support of data users with restricted computational resources, resource-intensive operations can be outsourced to high-performance devices (e.g., autonomous underwater vehicle (AUV)). Specifically, underwater devices can outsource the majority of the decryption operations to high-performance devices and perform final decryption at a low cost using their attribute secret key to the partially decrypted ciphertext generated by the high-performance device.

C. Online/Offline Attribute-based Encryption [8]

To alleviate the computational burden on data owners, the majority of the encryption operations can be done offline, where access policies and messages are undetermined. Specifically, underwater devices can efficiently perform encryption of ABE with low latency by pre-computing resource-intensive operations in idle states.

D. Application Scenario

In order to achieve fine-grained access control with low latency for underwater devices with limited computational resources in UWSN, it is essential to minimize the online computational overhead by leveraging both the online/offline ABE and outsourced ABE as mentioned above. It should be noted that online/offline ABE requires performing offline encryption for each message prior to online encryption for ensuring security. That is, performing offline encryption as much as possible during idle states allows multiple messages to be securely transmitted online. Therefore, scheduling is necessary to determine when and how many times offline encryption should be performed. Furthermore, outsourced ABE incurs communication overhead during the process of outsourcing decryption. To minimize this overhead, it is crucial to reduce the length of the transmitted message as much as possible.

By appropriately utilizing the already proposed online/offline ABE and outsourced ABE, an ABE suitable for underwater communication can be implemented. However, the robust environmental factors of underwater communication may demand a more stringent ABE approach.

IV. Lightweight Authentication and Key Agreement Mechanism

This section describes the authentication and key agreement mechanisms among underwater devices in UWSNs, considering the features of UWSN in Sec. II. For each of the four features in UWSN, the authentication and key agreement mechanisms must support four requirements as follows.

A. Low Computational Overhead

In the authentication and key agreement processes, it is crucial to avoid imposing high computational overhead on underwater devices. Therefore, symmetric key cryptography using pre-shared long-term keys and public-key cryptography with low computational overhead of underwater devices, such as ABE [7], [8] mentioned in Sec. III, should be used appropriately.

B. Minimum Number of Communications and Low Communication Overhead

In the authentication and key agreement processes, an increase in the number of communications may occur due to message retransmissions caused by bit errors. While such occurrences may only lead to low latency in conventional communication (i.e., terrestrial communication), it poses a significant challenge in underwater communication. To minimize the retransmissions caused by bit errors, one potential solution is to encrypt the same message with multiple keys. By decrypting each ciphertext and comparing the resulting messages, it is possible to verify if the number of identical messages exceeds a specific threshold, effectively avoiding retransmissions caused by bit errors.

To reduce communication overhead, it is crucial to minimize the message length. Strategies such as removal of unnecessary header information and redundant data, and data compression, can be considered for this purpose. Additionally, in scenarios where multiple keys need to be sent to achieve a reduced number of communications, a key derivation function can be employed to derive multiple keys from a single key.

C. User and Key Revocation Mechanisms

Due to the frequent device failures and intentional compromise, sensitive values, including keys, within the devices may be exposed. Therefore, system administrators must swiftly identify compromised devices and take measures to prevent the devices or their keys unusable within the system. To achieve this, the system needs to maintain user and key revocation lists and perform periodic key update procedures. The ABE supporting user or attribute revocation can be employed to minimize additional computational and communication overhead imposed on underwater devices. Specifically, the system administrator should add the long-term secret key of the compromised device to the user revocation list. The system should utilize ABE with direct revocation, ensuring secure key revocation and updates whenever a device compromise event occurs without any additional overhead on the user.

D. Handover Authentication and Key Agreement Mechanisms

When a device moves to a different cluster, it needs to perform authentication with the access point of that cluster and carry out key agreement among the devices within the new cluster. Ensuring service continuity during mobility requires a fast and secure authentication and key agreement process. Thus, lightweight handover authentication and key agreement mechanisms are essential. To reduce the computational overhead in the authentication and key agreement process within the new cluster, it is possible to use the results of the authentication and key agreement with the previous cluster without compromising security. Additionally, minimizing communication overhead by actively leveraging terrestrial communication between the old and new access points and reducing message length can also be considered.

V. Future Challenge in Security of UWSN

Some works proposed for UWSN security are still in the theoretical stage [2]–[4], and there are few empirical works that have proposed lightweight cryptosystems or lightweight authentication and key agreement mechanisms for UWSN. Additionally, beyond the aforementioned challenges, the advancement of UWSN will necessitate new security features, such as privacy-preserving for underwater devices. In conclusion, the successful implementation of suitable cryptosystems and authentication and key agreement mechanisms, specifically designed for constraints and distinctive features of UWSN, stands as a prominent future challenge.

VI. Conclusions

In this paper, we explore cryptosystems and authentication and key agreement mechanisms that are well-suited to the constraints and distinctive features of underwater wireless sensor networks (UWSN). Specifically, we adopt fine-grained access control as an essential security requirement for UWSN and describe a lightweight approach of attribute-based encryption (ABE) to achieve it. Additionally, we present four security requirements for authentication and key agreement mechanisms, carefully considering the constraints of UWSN. In conclusion, this paper goes beyond exploring the basic security requirements in UWSN, providing criteria for cryptographic systems and mechanisms that are well-suited for UWSN, thus aiming to expedite the implementation of a secure UWSN.

References

[1] A. P. Das and S. M. Thampi, "Secure communication in mobile underwater wireless sensor networks," in *Proc. Int. Conf. Adv. Comput. Commun. Inform. (ICACCI)*, Aug. 2015, pp. 2164–2173.

[2] Y. Cong, G. Yang, Z. Wei, and W. Zhou, "Security in underwater sensor network," in *Proc. International Conference on Communications and Mobile Computing (CMC)*, vol. 1, Apr. 2010, pp. 162–168.

[3] G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," *Sensors*, vol. 18, no. 11, p. 3907, Nov. 2018.

[4] G. Yang, L. Dai, G. Si, S. Wang, and S. Wang, "Challenges and security issues in underwater wireless sensor networks," *Procedia Comput. Sci.*, vol. 147, pp. 210–216, Feb. 2019.

[5] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," *IEEE Trans. Parallel. Distrib. Syst.*, vol. 22, no. 4, pp. 673–686, Jun. 2010.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. Symp. Secur. Priv (S&P)*, May 2007, pp. 321–334.

[7] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

[8] S. Hohenberger and B. Waters, "Online/offline attribute-based encryption," in *Proc. International Conference on Theory and Practice of Public Key Cryptography (PKC)*, Mar. 2014, pp. 293–310.