KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 10 (2024) 851–856

www.elsevier.com/locate/icte

Secure and efficient communications with fine-grained access control in underwater wireless sensor networks

Donghyun Yu[a], Sinwoong Yun[b], Jemin Lee[a,*]

[a] School of Electrical & Electronic Engineering, Yonsei University, Seoul 03722, Republic of Korea
[b] Department of Electrical Engineering & Computer Science (EECS), Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu 42988, Republic of Korea

Received 2 January 2024; received in revised form 12 April 2024; accepted 24 April 2024
Available online 26 April 2024

Abstract

As UWSN have received attention, a need for an efficient and secure communication protocol has arisen to overcome the low device performance, node failure, and high propagation latency. However, existing works are either specialized for one-to-one communication or cannot satisfy low latency constraints. Therefore, this work proposes a secure communication protocol with fine-grained access control for UWSN that support secure and efficient one-to-many communication and considers potential internal attackers for high security level. Specifically, we adopt lightweight ABE to achieve fine-grained access control at low cost, and introduce outsourced decryption to further alleviate the computational load of underwater sensors.

© 2024 Published by Elsevier B.V. on behalf of The Korean Institute of Communications and Information Sciences. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Keywords: Underwater wireless sensor network; Underwater security; Access control; Attribute-based encryption

1. Introduction

As the ocean covers more than 70% of Earth's surface, underwater networks have received a lot of attention as well as terrestrial networks [1]. In particular, underwater wireless sensor networks (UWSN) are one of the major issues in the research field. In those networks, the underwater sensor nodes are deployed to the seabed for various applications such as environmental monitoring and military surveillance [2].

In order to support efficient and secure communication between underwater devices, not only the security but also the high reliability and low latency need to be satisfied. However, due to the characteristics of underwater environments, some challenges have appeared in UWSN for satisfying those requirements. Firstly, the underwater sensor nodes have low computational capacity, so it is hard to perform the expensive operations with low latency. Secondly, underwater sensors can move to another region to perform missions such as military surveillance. Moreover, their positions may change due to currents or turbulence.

To overcome the above challenges, some recent works designed protocols for secure communications in UWSN. Since these works aim to achieve low latency in one-to-one communication, these works propose a secure communication protocol and authentication method that only achieves basic security requirements such as confidentiality and integrity [3–7], and some work additionally achieves user anonymity [8]. However, in the large networks such as the UWSN, multiple sensors are distributed to collect data for various purposes. In those networks, the efficient and secure one-to-many communications need to be supported, while the above prior works only can support one-to-one communications.

Fine-grained access control, which allows or denies access to data based on multiple conditions, is a promising solution for supporting efficient and secure one-to-many communications. Specifically, it is used to prevent data from being exposed to malicious devices or legitimate but unauthorized devices, and the attribute-based encryption (ABE) is widely adopted to achieve this [9,10]. Recently, ABE is adopted to design secure communications for managing internet of underwater things (IoUT) environments [11]. By dealing with ciphertext-policy ABE (CP-ABE)-based protocol, they achieved the fine-grained access control in the underwater environments. Nevertheless, the proposed system is not suitable for

* Corresponding author.
E-mail addresses: xaos4715@gmail.com (D. Yu), lion4656@dgist.ac.kr (S. Yun), jemin.lee@yonsei.ac.kr (J. Lee).

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2024.04.009

2405-9595/© 2024 Published by Elsevier B.V. on behalf of The Korean Institute of Communications and Information Sciences. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

UWSN because it takes more than 20 s to encrypt messages due to the low computational capacity of the underwater device.

From the above limitations, this paper proposes the outsourcing-assisted secure underwater communication protocol with fine-grained access control (OA-SUC), which can support one-to-many communication and fine-grained access control within a reasonable latency in UWSN. The contributions of this paper are as follows:

- We adopt outsourcing-enabled and enhanced privacy-preserving ABE (OEEP-ABE) [12], a lightweight ABE, to simultaneously achieve fine-grained access control and low latency, and newly present outsourced decryption to further improve computational efficiency. In addition, we propose OA-SUC, which utilizes this to achieve basic security requirements as well as fine-grained access control, policy and attribute privacy. Additionally, considering the mobility of underwater units, OA-SUC includes an efficient handover authentication protocol.
- We demonstrate the security of our work through the security analysis of newly presented outsourced decryption and OA-SUC, and demonstrate the effectiveness of OA-SUC through performance evaluations.

2. System and attack models

2.1. System model

As shown in Fig. 1, UWSN consist of underwater sensors, autonomous underwater vehicles (AUVs), surface stations (SSs), and a terrestrial base station (TBS).

- **Underwater sensor**: It collects a variety of information and transmits them to other sensors, AUVs, and SSs. Since it is resource-constrained, cannot perform complex tasks within low latency. In addition, it possesses mobility.
- **Autonomous underwater vehicle (AUV)**: The AUV can perform some cryptographic operations outsourced by sensors. The entity that plays this role is called a security agent (SA) [13].
- **Surface station (SS)**: This receives data from underwater sensors and AUVs and transmits it to the terrestrial area. Additionally, it installs an encryption material on each sensor before activation.
- **Terrestrial base station (TBS)**: This acts as a system administrator responsible for management of UWSN and system member registration.

We consider all communication channels for long-term key sharing to be secure. On the other hand, communication channels for data sharing and handover authentication can be vulnerable to various attacks.

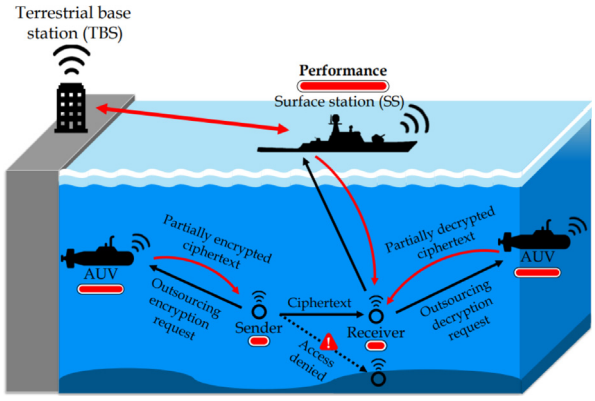

Fig. 1. Overview of system model.

2.2. Attack model and security requirements

In our system model, the SA (i.e., AUV) is the only entity that can learn the sensitive data of the sensor due to the outsourcing procedure. Therefore, we consider the SA as an honest but curious adversary who honestly follows the protocol but may try to expose any information. Additionally, every system member has its own assigned attributes and can encrypt messages according to specified policies and then send them to the desired receivers. All compromised entities are assumed to be malicious entities, and AUV and SS are assumed not to be colluding. In response to these system and attack models, the security requirements are as follows.

- **Confidentiality**: Messages broadcasted on UWSN must be hidden from all attackers.
- **Mutual authentication**: All legal entities in the system must be able to identify whether the other party exchanging messages is legitimate or not, and to verify the freshness of each message.
- **Fine-grained access control**: To prevent security breaches and data leaks, legal but unauthorized entities must be prevented from accessing sensitive data.
- **Policy and attribute privacy**: To prevent potential analysis or attacks, the policies of the ciphertext and the attributes of the receiver should not be exposed during encryption and decryption.

3. Outsourcing-Enabled and Enhanced Privacy-Preserving ABE (OEEP-ABE)

3.1. Intuition

The OEEP-ABE is an ABE proposed in [12] as a variant of PEAPOD [10] and EABEHP [14]. Compared with traditional ABE, the OEEP-ABE additionally supports outsourced encryption algorithms. Different from [12], in this work, not only the outsourced encryption, but also the outsourced decryption is used to improve the decryption efficiency.

3.2. Construction

The OEEP-ABE with decryption outsourcing consists of multiple algorithms. Among them, the same algorithms, used in [12], can be used here as well, including **Setup**, **KeyGen**, **Encrypt**, **Out.Encrypt1**, **Out.Encrypt2**, **Select.Policy**, and **Decrypt**. Here, we describe the newly introduced algorithms for outsourced decryption in the following.

- **TransformKey**(SK_{U_r})[1]: This algorithm takes SK_{U_r} as an input. It randomly selects $t \in \mathbb{Z}_q$ and produces transformed secret key TK_{U_r} as

$$TK_{U_r,1} = SK_{U_r,1} + t,\ TK_{U_r,2} = SK_{U_r,2} + t. \tag{1}$$

- **Out.Decrypt1**(C, TK_{U_r})[2]: This algorithm takes C and TK_{U_r} as inputs, and produces sC as

$$sC = A^{TK_{U_r,1}} \times D^{TK_{U_r,2}}. \tag{2}$$

- **Out.Decrypt2**(sC, t, I_r)[3]: This algorithm takes sC, t, and I_r as inputs, and produces M as

$$M = \prod_{i \in I_r} B_i \times sC/(A \cdot D)^t. \tag{3}$$

4. Outsourcing-Assisted Secure Underwater Communications with fine-grained access control (OA-SUC)

The OA-SUC consists of two phases, which are explained in the following subsections.[4]

4.1. System initialization and key management

This section describes how TBS generates and distributes system parameters and keys for each entity. It also explains how SS generates and distributes encryption material to each sensor. TBS generates (MPK, MSK) through **OEEP-ABE.Setup**, publishes the master public key MPK, and keeps the master secret key MSK. User secret key SK_U is generated by **OEEP-ABE.KeyGen** and securely distributed for each member of the system. Additionally, long-term symmetric keys $K_{\mathrm{AU,S}}$ and $K_{\mathrm{SS,S}}$ between AUV and sensor and between SS and sensor, respectively, are generated and securely distributed. Finally, TBS generates and securely distributes the private key sk_{AU} and public key pk_{AU} of each AUV. In addition, long-term symmetric keys $K_{\mathrm{TBS,SS}}$, $K_{\mathrm{TBS,AU}}$, and $K_{\mathrm{TBS,S}}$ are distributed between TBS and each SS, AUV, and sensor, respectively.

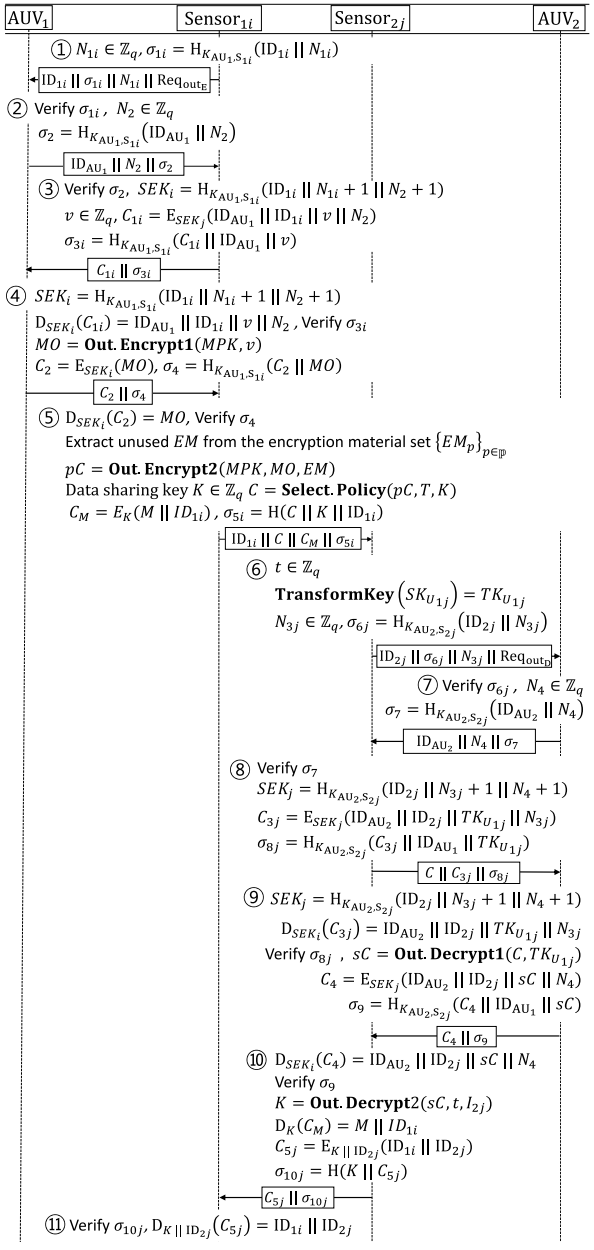

Fig. 2. Attribute-based data sharing (ABDS) protocol between underwater sensors.

Before the sensor performs underwater activities, SS uses $K_{\mathrm{SS,S}}$ to securely install the encryption material EM, which is used for attribute-based data sharing, into the sensor. Here, the number of encryption materials can be properly determined considering the sensor's storage space and update period.

4.2. Attribute-based data sharing (ABDS)

The ABDS protocol is a protocol used to share data between system members in UWSN. Resource-constrained devices (e.g., sensors) should use outsourced encryption and decryption, while high-performance devices can use normal

[1] SK_{U_r} is the user secret key output from **KeyGen** algorithm with MSK, ID_r, and I_r as input, where MSK is master secret key generated by **Setup** algorithm, ID_r is identity of user r, and I_r is set of attributes indices of user r.

[2] C is the ciphertext output from **Encrypt** or **Select.Policy** algorithm with MPK, T, and M as input, where MPK is master public key generated by **Setup** algorithm, T is policy set, and M is message. In addition, A and D are g^r and g^{dr} generated with $r \in \mathbb{Z}_q$ randomly selected by encryptor and MPK, respectively.

[3] B_i is $p_i(g^{a_i})^r$ generated with r randomly selected by encryptor, g^{a_i}, elements of MPK, and p_i, where p_i is message tuple.

[4] In the underwater environment, the network coverage is quite wide, as the message is delivered through acoustic communication, and thus, key distribution and data sharing can be performed without any issue.

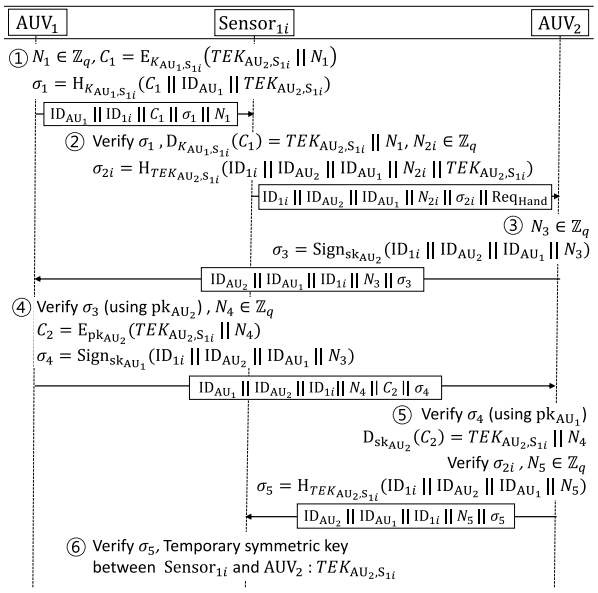

Fig. 3. Handover authentication protocol.

encryption and decryption. To emphasize the purpose of our work, in the proposed protocol, both the message sender and receiver are sensors, and the AUV plays the role of SA. The ABDS protocol consists of 11 steps, as shown in Fig. 2. Due to page limit, we omit the description of the ABDS protocol and the handover authentication protocol, and we only provide a summary of these protocols.

The ABDS protocol can be summarized as follows. Note that the step number in the following is referring to the number in Fig. 2. The Sensor_{1i} and AUV_1 perform the mutual authentication process (steps 1 to 3); the AUV_1 generates a partial ciphertext MO through **Out.Encrypt1** (step 4); the Sensor_{1i} generates a preliminary ciphertext pC and final ciphertext C through **Out.Encrypt2** and **Select.Policy**, respectively (step 5); the Sensor_{2j} transforms its secret key through **TransformKey** (step 6); the Sensor_{2j} and AUV_2 perform the mutual authentication (steps 6 to 8); the AUV_2 generates a partially decrypted ciphertext sC through **Out.Decrypt1** (step 9); and the Sensor_{2j} decrypts a partially decrypted ciphertext sC to obtain key K through **Out.Decrypt2** and sends ack message to Sensor_{1i} (steps 10 and 11).

4.3. Handover authentication

The handover authentication protocol is executed when a sensor moves from the coverage of a source AUV to that of another target AUV. The sensor can securely exchange temporary symmetric keys with the target AUV with the help of the source AUV. The resource-constrained sensor can securely perform handover authentication with low computational cost. The handover authentication protocol consists of 6 steps, as shown in Fig. 3. As the ABDS protocol, the description of the handover authentication protocol is omitted.

The handover authentication protocol can be summarized as follows. Note that the step number in the following is referring to the number in Fig. 3. The AUV_1 generates temporary symmetric key between Sensor_{1i} and AUV_2 $TEK_{\text{AU}_2,\text{S}_{1i}}$ (step 1); the Sensor_{1i} requests a handover from AUV_2 (step 2); the AUV_2 and AUV_1 perform the mutual authentication process with public key cryptography (steps 3 to 5); the AUV_1 sends $TEK_{\text{AU}_2,\text{S}_{1i}}$ to the AUV_2 (step 4); and the AUV_2 and Sensor_{1i} perform the mutual authentication process using $TEK_{\text{AU}_2,\text{S}_{1i}}$ (steps 5 and 6).

5. Security analysis

In this section, we prove the security of OEEP-ABE and OA-SUC. Since the security of OEEP-ABE was already proven in [12], it is sufficient that we prove the security of the newly introduced outsourced decryption procedure. Finally, we compare the security features with related works [4,7,8,11].

5.1. Security analysis of outsourced decryption introduced in OEEP-ABE

We prove the security of the outsourced decryption procedures, **TransformKey**, **Out.Decrypt1**, and **Out.Decrypt2**, which are not introduced in OEEP-ABE. For outsourced decryption, the user selects a random value t, and adds it to their private key SK_U to generate a transformed user key TK_U. Afterwards, it is transmitted to the SA. The only information that SA can obtain through TK_U is $SK_{U_1} - SK_{U_2}$, and there is no knowledge that SA can obtain through this information. Additionally, SA can generate sC through **Out.Decrypt1**, and since sC includes g^{rt} and g^{drt} due to t randomly selected by the user, SA cannot infer the message M and attributes of the user through sC. Therefore, SA does not know the user's secret key SK_U and the user's attribute set I, so the outsourced decryption with OEEP-ABE achieves attribute privacy.

5.2. Security analysis of OA-SUC

This subsection shows that the proposed OA-SUC achieves all the security features proposed in Section 2.2.

- **Confidentiality:** The OA-SUC guarantees confidentiality using OEEP-ABE and symmetric key encryption. In the ABDS protocol, AUV and sensor generate a session key SEK using the long-term symmetric key $K_{\text{AU,S}}$. The two devices share data using this SEK as a symmetric key. Attackers cannot obtain these SEKs because only AUVs and sensors that hold long-term symmetric keys can generate them. Additionally, the sensor uses OEEP-ABE to encrypt the symmetric key K that will be used when encrypting the message, and uses K to encrypt the data to be transmitted. Since OEEP-ABE's security has been proven in [12] and Section 5.1, only devices satisfying the policy assigned to the ciphertext can obtain the correct data.
- **Mutual authentication:** As with confidentiality, the AUV and sensor authenticate each other by generating a signature σ through HMAC using the long-term symmetric key $K_{\text{AU,S}}$. Therefore, other devices and attackers cannot

Table 1
Security comparison with related works.

	[4]	[7]	[8]	[11]	OA-SUC
Confidentiality	√	√	√	√	√
Mutual authentication	√	√	√	√	√
Efficient one-to-many communication	×	×	×	√	√
Replay attack	×	√	√	×	√
Fine-grained access control	×	×	×	√	√
Policy and attribute privacy	–	–	–	×	√

generate σ, that is, they cannot impersonate AUVs and sensors. Additionally, the HMAC generated by each device during this process includes a nonce N, preventing the reuse of previous signatures.

- **Fine-grained access control:** In OA-SUC, sensors use ABE to encrypt and share data. The ciphertext of ABE is assigned to a policy, and only devices with a set of attributes that satisfy this policy can decrypt the ciphertext and obtain the correct data. Therefore, devices that are legitimate but do not satisfy the policy cannot obtain the correct data.
- **Policy and attribute privacy:** OA-SUC uses OEEP-ABE, which is a cryptosystem in which a policy is assigned to the ciphertext and a set of attributes is assigned to the secret key. Exposure of policies and attributes enables potential analysis and attacks. The policy privacy of OEEP-ABE is proven in [12], and the attribute privacy is proven to be achieved in Section 5.1. Therefore, OA-SUC achieves policy and attribute privacy.

Finally, the overall security comparison between OA-SUC and related works [4,7,8,11] is shown in Table 1. As can be seen in Table 1, the proposed protocol can guarantee more security features than related works.

6. Performance evaluations

In this section, we compare the computational cost and execution time of the OA-SUC with related works. Our experimental testbed consists of a desktop and a microcomputer. The desktop is with an Intel® Core™ i5-11500 @ 2.7 GHz 6 cores processor and 16 GB RAM. The microcomputer utilizes a Raspberry Pi 3 B+ with a 1.4 GHz 64-bit quad-core ARM Cortex-A53 CPU and 1 GB RAM. We use the desktop as the AUV, acting as the SA, and the microcomputer as the sensor.

In the "OEEP-ABE supporting outsourced decryption" used in this work and the OEEP-ABE proposed in [12], the decryption costs allocated to the receiver are $T_{\text{EXP}} + (N_r + 2)T_{\text{M}}$ and $2T_{\text{EXP}} + (N_r + 1)T_{\text{M}}$, respectively. Thus, the computational burden on the receiver is reduced by about 50%. In addition, Table 2 is a comparison table of computational cost and time for OA-SUC and related works [4,7,8,11]. Here, we set $I_E = N_s = 16$, $I_D = N_r = 8$.

As shown in Table 2, [4,7], and [8] have significantly lower computation times compared to [11] and OA-SUC. Since they are designed with a focus on one-to-one communication, and as shown in Table 1, they do not support efficient one-to-many communication, achieve only basic security requirements, and thus only consist of operations with low complexity. In particular, they do not guarantee fine-grained access control, resulting in low computation time but a relatively low security level and efficiency.

In contrast, [11] and OA-SUC support efficient one-to-many communication and achieve fine-grained access control, as shown in Table 1. However, this inevitably results in high computational cost, and therefore [11] has high computational cost and time. On the other hand, the proposed OA-SUC can significantly reduce the cost and time by using "OEEP-ABE supporting outsourced decryption" to outsource resource-intensive operations such as exponential operation and pairing operation to the high-performance devices.

In conclusion, the OA-SUC is expected to be a suitable security solution for UWSN as it can execute one-to-many communication and fine-grained access control within reasonable latency compared to related works.

7. Conclusions

In this work, we propose an outsourcing-assisted secure underwater communication (OA-SUC) with fine-grained access control. We adopt the OEEP-ABE [12], an ABE that supports outsourced encryption for achieving fine-grained access control and solving resource issues. Additionally, we introduce an outsourced decryption for further improved computational efficiency. Moreover, considering the mobility of underwater units, OA-SUC includes an efficient handover authentication protocol. From the security analysis and performance evaluation, we show that the proposed OA-SUC can achieve a high

Table 2
Performance comparison with related works.

	[4]	[7]	[8]	[11]	OA-SUC
Computation cost (Sensor)	$4T_H + 4T_{Bp} + 4T_{SE}$	$8T_H$	$16T_H + 4T_{Cp} + 2T_{SE}$	$(2I_E + I_D + 6)T_{Exp} + (2I_D + 1)T_P + 2T_M$	$T_{Exp} + (N_s + N_r + 3)T_M + 12T_H + 8T_{SE}$
Computation cost (AUV)	–	$5T_H$	$11T_H + 3T_{Cp} + 2T_{SE}$	–	$(N_s + 4)T_{Exp} + T_M + 9T_H + 3T_{SE}$
Computation time	0.42 ms	0.08 ms	0.48 ms	467.54 ms	11.18 ms

T_H : hash function cost, T_{SE} : symmetric encryption cost, T_{Cp} : Chebyshev polynomial cost, T_{Bp} : bivariate polynomials cost, T_{Exp} : exponential operation cost, T_P: pairing operation cost, T_M : multiplication operation cost, I_E : number of attributes used in encryption, I_D : number of attributes used in decryption, N_s : size of the attribute universe, N_r : number of the user's attributes.

security level within a reasonable latency even in underwater communication between resource-constrained underwater sensors. Moreover, cryptosystems and security protocols can still be effective not only in underwater environments but also in other settings (IoT networks, vehicular networks). In future work, we will derive more practical results, including propagation latency and computation time based on real device performance rather than a campus environment.

CRediT authorship contribution statement

Donghyun Yu: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Resources, Software, Validation, Visualization, Writing – original draft, Writing – review & editing. **Sinwoong Yun:** Conceptualization, Writing – original draft, Writing – review & editing, Validation. **Jemin Lee:** Supervision, Conceptualization, Funding acquisition, Investigation, Methodology, Project administration.

Declaration of competing interest

The authors declare that there is no conflict of interest in this paper.

Acknowledgments

This work was supported in part by Korea Research Institute for defense Technology planning and advancement (KRIT) - grant funded by the Defense Acquisition Program Administration (DAPA) (KRIT-CT-22-078); and in part by the Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.2021-0-01277, Development of attack response and intelligent RSU technology for vehicle security threat prevention)

References

[1] M. Ayaz, I. Baig, A. Abdullah, I. Faye, A survey on routing techniques in underwater wireless sensor networks, J. Netw. Comput. App. 34 (6) (2011) 1908–1927.

[2] J. Luo, Y. Chen, M. Wu, Y. Yang, A survey of routing protocols for underwater wireless sensor networks, IEEE Commun. Surv. Tut. 23 (1) (2021) 137–160.

[3] A. Al Guqhaiman, O. Akanbi, A. Aljaedi, C.E. Chow, Lightweight multi-factor authentication for underwater wireless sensor networks, in: IEEE Int. Conf. Comput. Sci. Comput. Int., CSCI, Las Vegas, NV, 2020, pp. 188–194.

[4] X. Yu, H. Chen, L. Xie, A secure communication protocol between sensor nodes and sink node in underwater acoustic sensor networks, in: IEEE Int. Conf. Artif. Intell. Comput. App., ICAICA, Dalian, China, 2021, pp. 279–283.

[5] K.A. Taher, et al., A novel authentication mechanism for securing underwater wireless sensors from sybil attack, in: IEEE Int. Conf. Electr. Eng. Inf. Commun. Tech., ICEEICT, Dhaka, Bangladesh, 2021, pp. 1–6.

[6] U. Jain, M. Hussain, Security mechanism for maritime territory and frontier surveillance in naval operations using wireless sensor networks, Concurr. Comput.: Pract. Exper. 33 (17) (2021) e6300.

[7] C.M. Kumar, R. Amin, M. Brindha, SafeCom: Robust mutual authentication and session key sharing protocol for underwater wireless sensor networks, J. Sys. Arch. 130 (2022) 102650.

[8] S. Zhang, X. Du, X. Liu, A secure remote mutual authentication scheme based on chaotic map for underwater acoustic networks, IEEE Access 8 (2020) 48285–48298.

[9] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: IEEE Symp. Secur. Priv., SP'07, Oakland, CA, 2007, pp. 321–334.

[10] A. Kapadia, P.P. Tsang, S.W. Smith, Attribute-based publishing with hidden credentials and hidden policies., in: Netw. Distrib. Syst. Secur. Symp., NDSS, vol. 7, San Diego, CA, 2007, pp. 179–192.

[11] M. Gopinath, G. Tamizharasi, L. Kavisankar, R. Sathyaraj, S. Karthi, S. Aarthy, B. Balamurugan, A secure cloud-based solution for real-time monitoring and management of internet of underwater things (IOUT), Neural Comput. App. 31 (2019) 293–308.

[12] D. Yu, S. Lee, R.-H. Hsu, J. Lee, Ensuring end-to-end security with fine-grained access control for connected and autonomous vehicles, 2023, arXiv preprint arXiv:2312.07898.

[13] R.-H. Hsu, J. Lee, T.Q. Quek, J.-C. Chen, Reconfigurable security: Edge-computing-based framework for IoT, IEEE Netw. 32 (5) (2018) 92–99.

[14] D. Yu, R.-H. Hsu, J. Lee, S. Lee, EC-SVC: Secure can bus in-vehicle communications with fine-grained access control based on edge computing, IEEE Trans. Inf. Forensics Secur. 17 (2022) 1388–1403.