Wireless Pers Commun (2016) 89:479–499
DOI 10.1007/s11277-016-3283-z

CCM-UW Security Modes for Low-band Underwater Acoustic Sensor Networks

Mukhridinkhon Ibragimov[1] · Jae-Hoon Lee[1] · Muppalla Kalyani[1] · Jung-il Namgung[1] · Soo-Hyun Park[1] · Okyeon Yi[1] · Chang Hwa Kim[2] · Yong-Kon Lim[3]

Published online: 18 April 2016
© Springer Science+Business Media New York 2016

Abstract In this paper, we briefly describe an underwater media access control protocol based on the request to send/clear to send mechanism with security algorithms, which is proposed to provide data confidentiality, authenticity, and replay attack protection. The protocol includes the counter with cipher block chaining-message authentication code (CBC-MAC) for underwater (CCM-UW) mode that is the modified form of the counter with CBC-MAC (CCM*) mode for underwater acoustic communication, based on the advanced encryption standard/agency, research and institute, academy block cipher algorithm. CCM-UW security mechanism is suitable for underwater acoustic sensor networks (UWASNs) and offers six different security levels with different security strength, energy

✉ Soo-Hyun Park
shpark21@kookmin.ac.kr

Mukhridinkhon Ibragimov
mukhridin@kookmin.ac.kr

Jae-Hoon Lee
guderian88@kookmin.ac.kr

Muppalla Kalyani
mkalyani@kookmin.ac.kr

Jung-il Namgung
greenji@naver.com

Okyeon Yi
oyyi@kookmin.ac.kr

Chang Hwa Kim
kch@gwnu.ac.kr

Yong-Kon Lim
yklim@kiost.ac

[1] Kookmin University, Seoul, South Korea

[2] Gangneung-Wonju National University, Gangneung-si, South Korea

[3] Ocean Systems Engineering, KAIST, Daejeon, South Korea

consumption and transmission time. The results in the paper show that the protocol is not impracticable for UWASNs since it is energy efficient and saves transmission time.

Keywords CCM-UW (counter with CBC-MAC for underwater) · CCM* (counter with CBC-MAC) · Media access control (MAC) · RTS (request to send) · CTS (clear to send) · UWASNs (underwater acoustic sensor networks) · AES (advanced encryption standard) · ARIA (agency, research and institute, academy)

1 Introduction

To begin with, more than 70 % of our planet's surface is covered by water, and it is widely believed that the underwater world stores ideas and resources that will fuel much of the next generation of science and technology. However, underwater operations are fraught with difficulties due to the absence of easy methods to collect and monitor data [1]. Underwater Acoustic Sensor Networks (UWASNs) include underwater sensors and Autonomous Underwater Vehicles (AUVs) that are connected by wireless acoustic channels, then, the network is connected to the surface station that holds Internet connection through Radio Frequency (RF) communication. UWASNs can be used for many purposes, such as ocean sampling, environment monitoring, underwater resource exploration, distributed tactical surveillance, and disaster prevention [1].

Although underwater sensors exist, they are not still networked and their usage has many limitations:

- Deploying, retrieving, and using sensors are labor intensive;
- Collecting data is subject to extremely long delays;
- Manual aspects of using sensors can lead to error;
- Spatial scope for data collection with individual sensors is limited;
- Individual sensors cannot perform operations that require cooperation, such as tracking relative movement and indicating locations [2].

To continue, numerous obstacles on the underwater environment do not permit such networks to be secured. Herein, radio waves do not propagate well in underwater due to energy limitation, low bandwidth, slow data rates, long transmission delays, and the propagation speed of underwater is extremely high [3]. Although, we have many secured MAC protocols in traditional networks, those cannot be applied in underwater communication directly. Therefore, UWASNs require security mechanisms and algorithms to maintain data confidentiality and integrity. We intend to use CCM-UW security mechanism for our low-band UWASNs utilizing 70 kHz and whose data bit rate is 200 bps, LQI is very poor with 1 PDU size. CCM-UW is customized to this low-band network with energy limitation, low bandwidth, slow data rates, long transmission delays, and extremely high propagation speed as aforementioned. Hence, it is energy efficient and does not make transmission delays longer.

The US government adopted the AES published by the National Institute of Standards and Technology (NIST) in 2001, because the AES supports different types of modes such as ECB, CBC, CFB, OFB, and CTR. In this paper, we present the Counter with Cipher Block Chaining-Message Authentication Code (CBC-MAC) for Underwater (CCM-UW) mode of operation that is a modified form of the Counter with CBC-MAC (CCM*) in the AES standard algorithm. CCM (Counter with CBC-MAC) mode is a combination of the CBC-MAC mode with the CTR mode [4].

In this paper, we implemented the energy efficient and secured MAC for underwater networks, which succeed in saving energy and provides data integrity, confidentiality, data authentication, and replay attack prevention.

The rest of this paper is organized as follows: Sect. 2 provides the examples of the related works; Sect. 3 explains the architecture of UWASNs and main idea of our MAC protocol; the way of applying the CCM-UW security mechanism is described in Sect. 4; the performance analysis is shown in Sect. 5; and finally, the last section concludes our paper.

2 Related Works

The problem of secure underwater acoustic communication is quite a new research field [1]. Domingo presented a survey of security issues and possible countermeasures [5].

Similarly, [6] and [7] analyze the security and threats of underwater acoustic communication.

Dong et al. made taxonomy of attacks against underwater sensor networks [8]. They classified the attacks into three categories. The first includes physical attacks against nodes, the second includes attacks against protocols, while the third includes attacks against networks; however, Dong et al. did not provide any solutions.

Dini showed a secure communication suite for underwater sensor networks [3].

M. Zuba et al. studied the effects of denial of service "jam" attacks on underwater acoustic communication using real world field tests by building their own hardware jammer [9]. That kind of jammer achieved data integrity, but required more power.

In underwater communication, [10] explained attacks related to wireless sensor networks with respect to data authentication, integrity, and data availability [10] also explained two MAC layer attacks, which are traffic manipulation attacks and identity spoofing attacks.

For improving underwater communication security, we analyzed another wireless sensor communication system. In Zigbee wireless sensor network, they use the AES-CCM* for secure wireless communication to design network and upper layer. IEEE 802.15.4 wireless sensor network defines a secure MAC layer with AES-CCM* [4], so Zigbee use this layer for secure [4].

SBMAC [10] is an energy-efficient Smart Blocking MAC Mechanism for UWASNs, this mechanism uses multiple acknowledgement policies (such as No-Ack, Reduced-Whole-Ack, Multiple-Block-Ack, and Selective-Multiple-Ack), but it also consumes copious energy.

In [11], encrypted data communication is described. They use encryption method (RSA Algorithm for encryption and decryption) before encoding the data to improve security of ocean-observing and communication systems.

Yan et al. presented an efficient ECC implementation on a TMS320C6416 DSP board and took advantage of hardware features of DSP to accelerate the ECC operations [12].

In [13], they proposed security mechanism that can be used in underwater acoustic environment by choosing block cipher modes of operation, the OFB and CTR to increase efficiency in data transmission, and picked CMAC for message authentication. Initial vector for generating key stream, the counter management, and the proper length of MAC need to be worked on more.

In [14], they studied the threat, attack, and security issues of UWSN and argued that layered security schemes cannot protect UWSN against blended attacks and presented a novel preliminary conceive, which is a cross-layer, adaptive, selective security scheme. They pointed out that layered schemes are often inadequate and inefficient.

In [15], the SecFUN, a security framework for underwater acoustic sensor networks (UASNs), is introduced. The authors selected cryptographic primitives to build security framework (SecFUN). SecFUN provides data confidentiality, integrity, authentication and nonrepudiation by exploiting as building blocks AES in the Galois Counter Mode (GCM) and short digital signature algorithms. As a proof of concept of the proposed approach, they extend the implementation of the Channel-Aware Routing Protocol (CARP) to support the proposed cryptographic primitives.

In [16] Dini et al. presented SeFLOOD, a cryptographic suite providing protection against spoofing-based DoS and integrity attacks in Underwater.

In [17] Xu et al. proposed a secure MAC protocol for cluster-based UWSNs, called SC-MAC, which aims to ensure the security of data transmission. In SC-MAC, the clusters are formed and updated dynamically and securely.

In [18] Caiti et al. propose both a security suite, which is designed with the goal of reducing the communication overhead introduced by security in terms of number and size of messages between autonomous mobile underwater sensors, and a cooperative algorithm in which the mobile underwater sensors (installed on Autonomous Underwater Vehicles) respond to simple local rules based on the available information.

3 Underwater Acoustic Sensor Networks

In this section, we examine UWASN architecture and propose a secured MAC protocol.

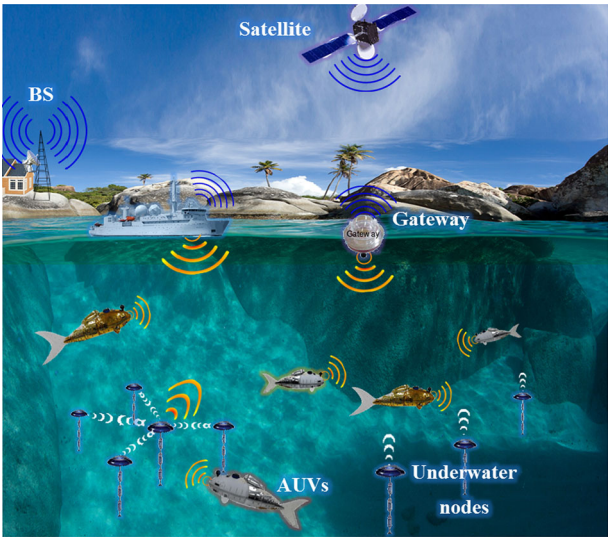

Fig. 1 UWASN architecture

3.1 UWASN Architecture

The architecture for underwater communication is depicted in Fig. 1. AUVs can collect underwater environment information, and then send it to the gateway.

In terrestrial networks, there are a multitude of channel-based and packet-based MAC protocols, which generally demonstrate poor performance when applied to UWASNs [20]. Furthermore, one of the handshaking-based protocols is Multiple with Collision Avoidance (MACA) that minimizes packet collisions.

We propose an underwater MAC protocol based on a flexible three-way handshaking mechanism [19] and we also prove that such protocol is reliable, scalable, and energy efficient. The usage of such mechanism enables MANETs to exchange mutual messages, such as RTS, CTS, DATA, and ACK. In some circumstances where there is no security, attackers can easily access MANETs and modify data. Coordination and information sharing among underwater nodes and AUVs require secure communication, however, acoustic channels are an open medium, so attackers conveniently equipped with acoustic modems can easily drop messages traversing the network. This could be extremely dangerous, for example, in distributed tactical surveillance applications where messages must be secret. Furthermore, attackers can also modify or inject false messages, as a result, we can lose data integrity, confidentiality, and authentication.

3.2 Basic Idea for Proposed MAC Protocol

We designed an underwater secured MAC protocol to efficiently manage an ad-hoc underwater environment monitoring system in the form of data reliability, energy efficiency, data confidentiality, authenticity, and anti-attacker prevention [21].

Figure 2 shows the attack of data exposure to an adversary. If Node A intends to send data to Node B, first of all, Node A sends a RTS_A for the occupying channel to Node B with a destination address. After receiving the RTS_A, Node B sends a CTS_B to Node A as an acknowledgement whether Node B is available. However, an adversary (Node C) can listen to the RTS_A signal and be ready to listen to the data from Node A. After Node A receives the CTS_B, Node A broadcasts the data for Node B. Node C can also receive this data, but the data that Node C receives is encrypted by shared security information

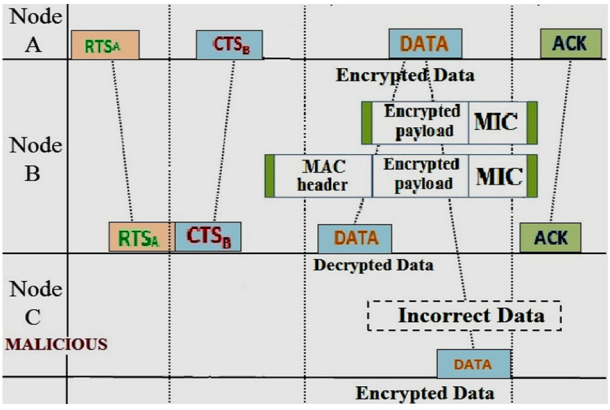

Fig. 2 Basic operation of secured MAC

between Node A and Node B. Although Node C receives the message from Node A, Node C cannot confirm the original message because it lacks the security information shared between Node A and Node B.

We manage threats similar to the example described in the previous paragraph using a cryptography algorithm. By applying the cryptography algorithm in a MAC protocol, we provide three security services: data confidentiality, data authenticity, and replay-attack protection.

3.2.1 Data Confidentiality

In underwater acoustic communication, adversaries equipped with acoustic modems can eavesdrop on messages. To prevent data exposure, we have to encrypt such data using cryptography algorithms, which are symmetric key ciphers or other types of ciphers.

Cryptography algorithms protect messages in transferred packets applied correctly. There are some cryptography algorithms that provide such security services. Symmetric key ciphers and public key ciphers are commonly used as cryptography algorithms. Public key ciphers that use public keys and private keys are not suitable for application in underwater acoustic communication because they require a significant amount of memory, computational power, and power consumption. Therefore, we use symmetric key ciphers for underwater acoustic communication in order to ensure data confidentiality.

3.2.2 Data Authenticity

Adversaries equipped with acoustic modems can inject false messages in underwater acoustic communication. To maintain the stability of communication states, we need to convince that transferred data is not changed and derived from correct origin. That is why, we generate Message Authenticate Codes (MAC) of transferred data similarly to CRCs; however, there are differences between MAC and CRC, because MAC needs the key to generate the MAC value, while CRC doesn't. In order to generate MAC, secure parameters are required to be known, such as Initial Vectors (IVs), Keys, and other additional secrete information. MAC is generated by compressing of data with key and additional secrete information, so that compressed process provides the data integrity. If at least one bit of the original messages concluding data and additional secrete information is changed, MAC values will totally change. Thereby, additional secrete information shared between entities provide the data authenticity.

3.2.3 Replay-Attack Protection

Because underwater acoustic communication is wireless, there is a possibility that adversaries can perform sniffing and spoofing. Adversaries capture messages that are forwarded by senders to receivers, and keep them. Then, they resend the message to the receivers after transmission is done. Thereafter, the receivers cannot distinguish previous messages from current messages. In order to prevent such attacks, we use frame counters in generating MAC. If frame counter is contained in only header not in MAC, like sequence number in IP header, attacker can find the frame counter and fix it, and receiver cannot suspect the attack. Because of this, frame counter is also contained in MAC. If the same data is sent to receiver with different frame counter, each MAC in received data is totally different due to different frame counter. Ultimately, to implement replay attack is

impossible. This is why, we use frame counters instead of sequence numbers to generate MAC.

4 CCM-UW Security Mechanism

We design secure underwater communication with cryptography technology, since using cryptography algorithm can protect data and improve the communication environment. There are typically two types of cryptography algorithm. First one, the Public key algorithm uses a key pair with public key and private key. Public key algorithm is quite comfortable and dynamically stable, because only one key pair, including public key and private key, can communicate the other with same public key infrastructure, and non-repudiation is guaranteed by using public key signature. However, Public Key Infrastructure (PKI) is hard to implement and requires much memory and computing power than symmetric algorithm.

On the other hand, the symmetric key algorithm is designated to use keys shared between entities on communication, where the number of keys is as many as the number of entities. For this reason, symmetric key algorithm is not as comfortable as public key algorithm. However, the overload of key management is not a critical problem in limited entities like underwater, because of a small number of entities. Also, symmetric key algorithm does not require as many resources for operational purposes as the public key algorithm does, and there is no need for an infrastructure like PKI. Therefore, we decided to use the symmetric key algorithm for designing secure underwater communication.

NIST (National Institute for Standard and Technology) provides the cryptography algorithm strength [FIPS 800-57] including symmetric key algorithm. This means how cryptography algorithm can be endurable against burst-force attack. Following table shows the period of the strength of each cryptographic algorithm (Table 1).

In this table, we use two symmetric cryptography algorithms of 128-bit security strength. The first is the typical 128-bit symmetric key algorithm AES in 2000, while the second one is the Korea standard cryptography algorithm ARIA published in 2004. Both algorithms are not fast and cost-efficient, but they are still having scale of applying the cryptography algorithm in underwater communication. Later in Sect. 5, we analyzed the performance results and energy consumption of operating cryptography algorithm.

There are numerous methods of operating cryptography algorithm. Principally, 128-bit symmetric cryptography algorithm (e.g. AES, DES, etc.) transforms 16-byte plaintext to 16-byte cipher-text with 128-bit symmetric key. In case if you have more than 16-byte

Table 1 Security strength

Security Strength		2011 through 2013	2014 through 2030	2031 and beyond
80	Applying	Deprecated	Disallowed	
	Processing		Legacy use	
112	Applying	Acceptable	Acceptable	Disallowed
	Processing			Legacy use
128	Applying/processing	Acceptable	Acceptable	Acceptable
192		Acceptable	Acceptable	Acceptable
256		Acceptable	Acceptable	Acceptable

data, you need a method of encrypting large data, which is called modes of operation. In previous Sect. 3, we have provided 3 security services including data confidentiality, data authenticity and replay attack protection, so we should use modes of operation with authenticity to provide these services. Typically, modes of operation with authenticity are of two types, namely CCM (Counter with CBC-MAC) and GCM (Galois Counter Mode). Figure 3 shows both CCM mode and GCM mode respectively.

Both modes use counter mode to encrypt scheme, because of the advantage of the counter mode to preserve data's length before and after encrypting. And encrypt scheme does not enquire padding process, and it is faster than other modes that require padding process. The difference of two modes is the way of generating MAC scheme, as CCM mode use the CBC-MAC based on symmetric algorithm, while GCM mode use the Galois HASH function based on 128-bit finite field GF(2^{128}) operation. While generating MAC scheme, the difference of the modes of operation's performance is shown in the way how block cipher (e.g. AES or ARIA, etc.) and Galois HASH function implement. To add, with limited resources, the gap of performance of CCM and GCM is critical. Figure 4 shows the result of CCM and GCM operation time with 128-bit MAC for each data size of 16, 32, 64, and 96 bytes.

In general, CCM mode is widely used at IEEE 802.11 (WLAN), IEEE 802.15.3 (UWB), and IEEE 802.15.4 (ZigBee) to support security services over wireless intervals [22]. For example, IEEE 802.15.4 (UWB) system uses the CCM* mode, which is modified from the CCM mode. They limit the size of MAC value and define the input parameter such as additional authentication data. As a result, we use the CCM-UW mode which is modified from the CCM mode like CCM* mode. Figure 3 shows how the CCM-UW mode of operation with AES block ciphers works.

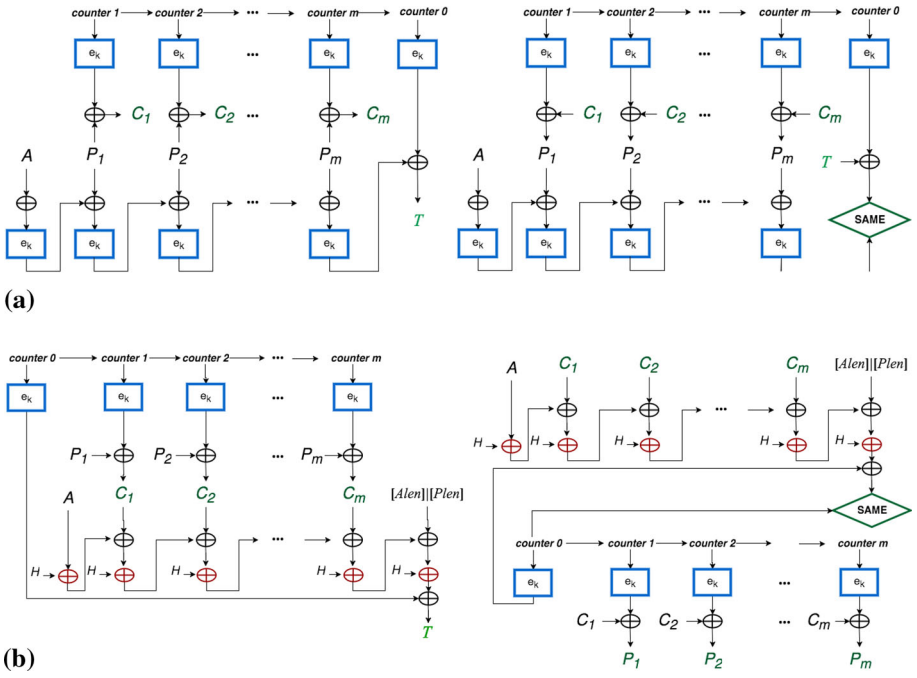

Fig. 3 Core mechanisms of CCM and GCM mode of operations. **a** Counter with CBC-MAC (CCM) mode of operation. **b** Galois counter mode (GCM) mode of operation

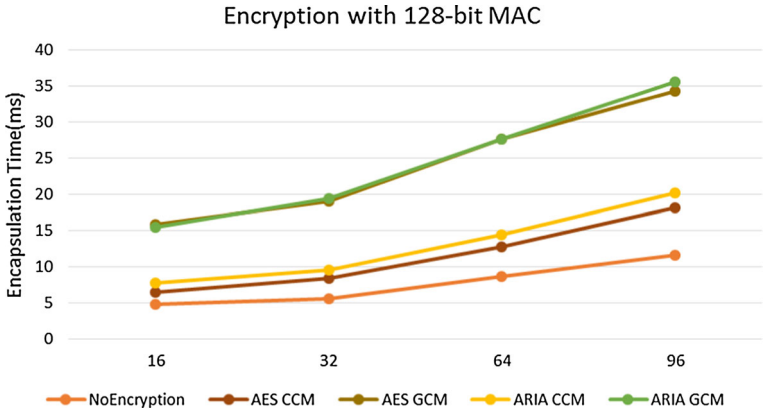

Fig. 4 Comparison between CCM and GCM

There are two parts of the CCM-UW mode. The first part is a generated MAC scheme. As Fig. 5 shows, plaintext used to generate MAC is a total packet that includes the header and payload according to MAC value roles. There are three roles of MAC. The first role confirms where the packet is originated that is called data authenticity. MAC is generated using pre-shared data integrity keys. If there are no pre-shared keys or the keys are incorrect, MAC values also become incorrect. Plaintext that is one of the key materials for generating MAC includes the source address in the header. If the header's source address is changed or incorrect, the corresponding MAC value is also incorrect. Thus, the information such as integrity key and source address in header confirms where the packet originated. The second role of MAC is the protection from replay attack. The frame counter needs to generate MAC. If frame counter's orders are mixed or forged, MAC value becomes incorrect. Attacker can change frame counter, however, attacker does not know the integrity key, he/she cannot generate correct MAC of the changed frame counter. Hence,

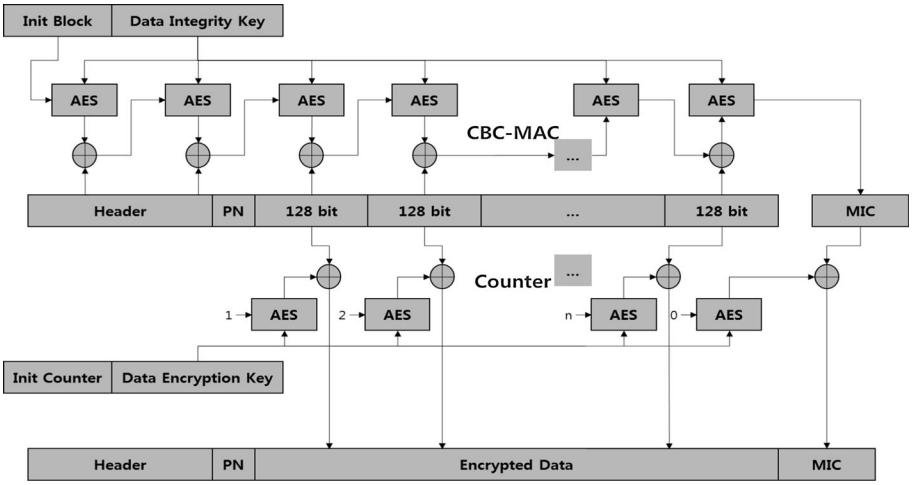

Fig. 5 CCM-UW mode of operation-based symmetric key cipher

we can successfully protect the system from replay attack. The third MAC role confirms whether data is changed or not. In order to generate MAC, we use the CBC-MAC mode that provides data integrity, which enables us to confirm data authenticity by checking MAC. Consequently, we can gain three types of information at once by checking MAC.

The second part of the CCM-UW mode is data scheme using the counter mode with encryption key. The counter mode has some advantages, as it has no decryption scheme and both the encryption and decryption operate just XOR operation with encrypted counter. Since XOR operation is bit-wise addition, encryption and decryption are same. Thus, counter mode preserves the data length before encryption and after decryption, and there is no another data length field to notify the changed data length after encrypt scheme.

These two parts use different keys, as generate MAC scheme uses the integrity key and encrypt scheme uses the encryption key. The reason for using two keys is the exposure of key information, because the more secure key managements are used by separated keys depending on their role, therefore more secure underwater communication system can be designed.

To operate this CCM-UW mode, an auxiliary security header that includes security parameters is essential. The CCM* defined in the IEEE 802.15.4 standard has an auxiliary security header with the size varied from 5 to 14 bytes. The auxiliary security header contains three fields: security control, frame counter, and key identity. The size of the auxiliary security header is not suitable for underwater acoustic communication due to limited communication environment, thus, to reduce the size of such header, we customize the fields of the auxiliary security header of CCM* (IEEE 802.15.4 standard). As a result, the auxiliary security header size is reduced by 4-byte: security control—one byte (contained 1-bit security enable and 3-bit cipher suite, 3-bit security level), key identifier—one byte, and frame counter—two bytes. In underwater single-hop communication, we suppose that there are no more than 255 devices around each device and CCM-UW concern single-hop in operation MAC layer (Media Access Control layer). Because of this assumption, Key identifier, which is distinguished around devices, is enough for covering the around single-hop. We also design the cipher suite field. There are many symmetric key algorithms with different security strength, requirement and performance. We design a flexible CCM-UW by using cipher suite, so that the developer defines another block cipher, and can use it. Unlike CCM* mode, CCM-UW uses only 6 security levels. MAC provides several secure services, but still 128-bit MAC is a disadvantage for underwater communication to transfer rather than providing security service. Thus, we designed six security levels to operate CCM-UW, except for security levels 3 and 7 of the CCM* mode, as described in Table 2.

Table 2 Six security levels in CCM-UW mode

Security level	Integrity (MAC) (bits)	Encryption
CCM-UW		
0	0	×
1	32	×
2	64	×
3	0	✔
4	32	✔
5	64	✔

As a result, we reduce power consumption by decreasing sending data and maintaining security strength. This modification is the result of a compromising plan between underwater acoustic communication and security strength. If we further reduce the size of the security parameter or MAC, the guarantee of security provided by the cryptography algorithm decreases.

We analyzed energy consumption in six different security levels. The corresponding results of these levels in terms of energy consumption are described in Sect. 5.

5 Performance Analysis

In this section, we show our test bed environment for implementing the CCM-UW security mechanism, and evaluate the energy consumption of each level.

The test bed is illustrated in Fig. 6. Since it is designed to explore the studies related to underwater communication, all the hardware resources are carefully selected to offer a real underwater environment and the freedom to customize environmental parameters with affordable budgets. The water tank with dimensions of 250, 80, and 70 in length, width, and height, respectively, is used to represent the underwater environment. Underwater transducers and modems are utilized to provide acoustic communication channels in the water tank [23].

As for the CCM-UW mode test, there are two nodes (Node A and Node B in Fig. 6) that communicate with each other; one node is the sender and the other one is the receiver. In the figure, Node C does not have a security mechanism and each node has a transducer, a modem, and a MAC board. We developed new protocols for the MAC board because the MAC layer protocols and the CCM-UW security mechanism were also developed for the MAC board using the C programming language. After developing the CCM-UW security mechanism for the MAC protocol, we tested the existing MAC protocol and the new protocol in six security levels in order to compare their energy consumption because we intend to show that there are no significant differences between the existing MAC protocol and the secured MAC protocol. Moreover, we aim to offer the secured MAC protocol with six different security levels by comparing their consumed energies for transmissions.

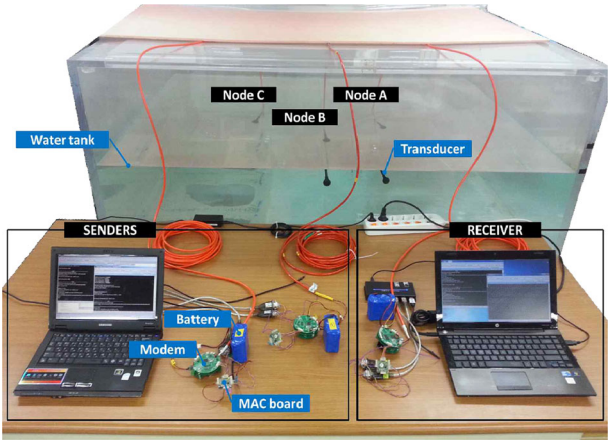

Fig. 6 Test bed setup

Furthermore, after obtaining positive results in our test bed, we implemented the protocol in a real environment with a fish robot in Han River, South Korea [23].

In order to verify the functionality and performance of the secured MAC protocol, an indoor experiment was conducted in the test bed. The parameters for the test are listed in Table 3.

In the test bed, two nodes have CCM-UW security mechanisms, and the security levels are defined by checking the data sent by the sender. Node C fails to understand the received data because its MAC board does not have both encryption and decryption algorithms. For example, in Fig. 7, the information in the sender part is 13 bytes with different functions, namely, the first byte contains the security level, the second byte contains the security key identifier, the third byte contains the destination node ID, the fourth byte contains the payload length, and remaining nine bytes represent the data. Here in, by changing the first byte, we can use different security levels without modifying the source code.

A battery supplies power for the modem and transducer in our test. Each node has a battery, and the battery's nominal voltage is 14.8 V. In fact, the battery starts with higher voltage, and then slowly drifts to 15 V, and finally even lower to 12 V. However, this depends on battery capacity; therefore the results can be different for various batteries. We used the same capacity batteries to measure the differences of the voltages defined before and after each transmission. It is possible to gain the consequences of the protocol comparison through assistance of the following method. Using a multi-meter as the voltmeter, we can easily measure battery voltage before and after transmission, and can define the differences of the voltages:

$$\Delta V = V^{before} - V^{after} \tag{1}$$

Here V^{before} is the voltage of the battery before transmission, and V^{after} is the voltage of the battery after transmission.

In fact, each sender and receiver node consumes energy to send and receive data, we calculate all consumed voltages. This is equal to the sum of the sender's consumed voltage and the receiver's consumed voltage:

$$\Delta V = \left(V^{before}_{sender} - V^{after}_{sender}\right) + \left(V^{before}_{receiver} - V^{after}_{receiver}\right) \tag{2}$$

Herein V^{before} is the voltage of the sender/receiver before transmission, and V^{after} is the voltage of the sender/receiver after transmission.

We measure the Direct Current (DC) voltage of both the sender and receiver batteries using the multi-meter for each transmission, and collect all voltage values. Those all calculations are done for one security level, accordingly, we use the same method for six CCM-UW levels of the AES and ARIA algorithms.

Table 3 Test environment parameters

Parameters	Values
Data rate	1 kbps
Data transmit duration	200 ms
Acoustic speed	1500 m/s
Number of nodes	3
Transmit power	<100 W

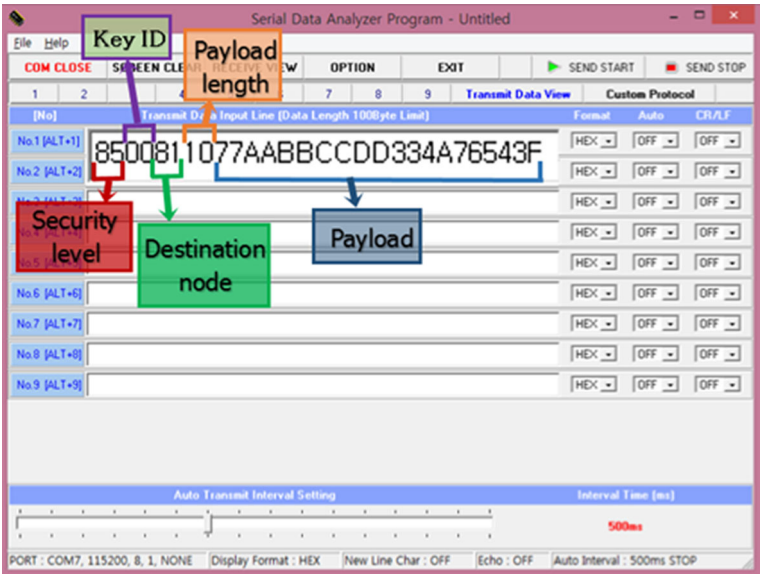

Fig. 7 Transmission emulator

In order to compare the energy consumption of each level, we require the sum of the consumed voltages of all transmissions; the total consumption formula can be defined as follows:

$$\Delta V_T = \sum_{n=1}^{N} \Delta V_n \tag{3}$$

In this formula, ΔV_T is the total voltage consumption for all transmissions, N is the total number of transmissions, and ΔV_n is the consumed voltage of each transmission.

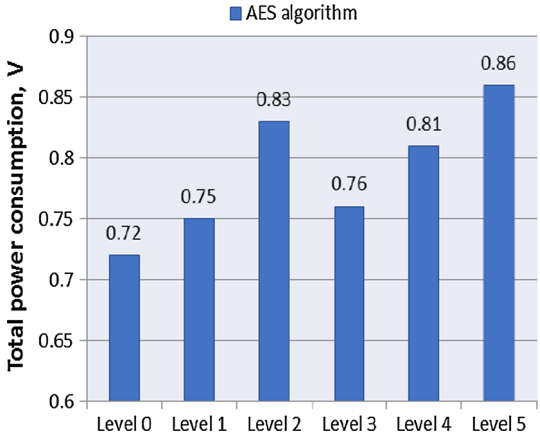

Fig. 8 Energy consumption comparison of six CCM-UW levels in AES algorithm

Data size fluctuates from four to 26 bytes for every transmission, and we repeat every transmission 80 times in order to obtain clearer results.

Figure 8 shows the results of six security levels of the AES algorithm. As expected, the nodes with higher security levels and more integrity values waste more energy. Conversely, sometimes amount of energy consumed is not as important as provision of higher security.

In these cases, the algorithms with higher security levels are sustainable for usage. According to the results in Fig. 8, although levels 3 and 0 have the same MAC values, level 3 consumes more power than level 0 because there is no encryption in level 0.

Figure 9 shows the results of six security levels of the ARIA algorithm. Power consumption of the CCM-UW security levels of the ARIA algorithm increase as their MAC values grow. This algorithm is widely used in Korea. In Fig. 9, the CCM-UW mode security level 5 with encryption and 64-bit MAC consumes more energy compared to the other levels. However, for cases where security strength is more important than power consumption, such algorithm can be quite useful.

Figure 10 shows the energy consumption differences between the AES and ARIA algorithms. We compare the levels with zero-bit MAC, which are levels 0 and 3. By comparing the same levels in both algorithms, based on the results the ARIA algorithm consumes more energy than the AES algorithm.

Figure 11 also shows the energy consumption differences between the AES and ARIA algorithms. However, we compare the levels with 32-bit MAC, which are levels 1 and 4. In addition, in this figure, ARIA consumes more energy than AES. It is not easy to detect the distinctions of the diagrams in Fig. 11 because the results are found from real measurements.

Similarly to Figs. 10 and 11. Figure 12 also illustrates the energy consumption differences between the AES and ARIA algorithms. We compare the CCM-UW mode levels 2 and 5, which have 64-bit MAC values. This figure also demonstrates that AES is more energy efficient than the ARIA algorithm.

We compared the security levels of each algorithm and demonstrated the results. As we predicted earlier, the security levels have different energy consumptions, and such difference depends on whether there is encryption and MAC values. Moreover, larger MAC

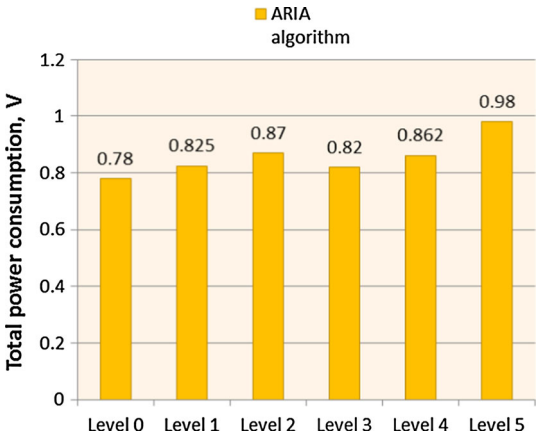

Fig. 9 Energy consumption comparison of six CCM-UW levels in ARIA algorithm

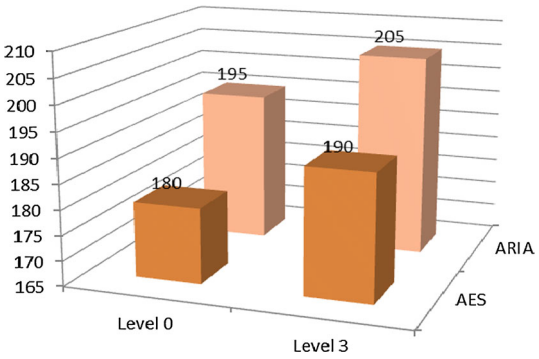

Fig. 10 Comparison between CCM-AES and CCM-ARIA with 0 bit Integrity

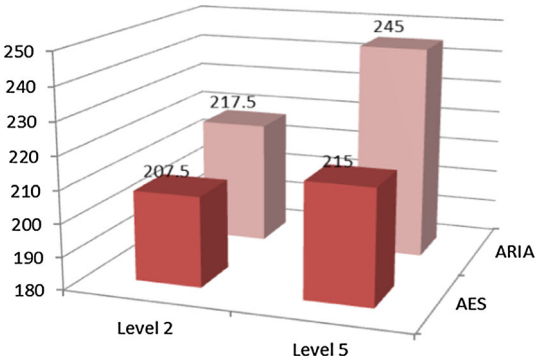

Fig. 11 Comparison between AES and ARIA algorithms with 32-bit MIC

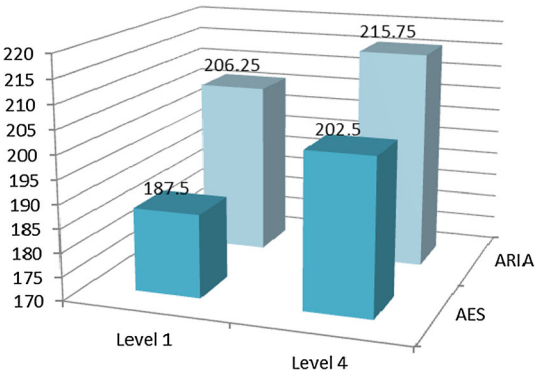

Fig. 12 Comparison between AES and ARIA algorithms with 64-bit MIC

values have stronger security strengths. In fact, some communication systems do not require encryptions, thus, all security levels are suitable and valid.

The comparison of power consumption of two protocols is demonstrated in Fig. 13: the existing protocol (the last in the figure, from bottom to top), and the new secured protocol with 12 levels (each algorithm has six levels).

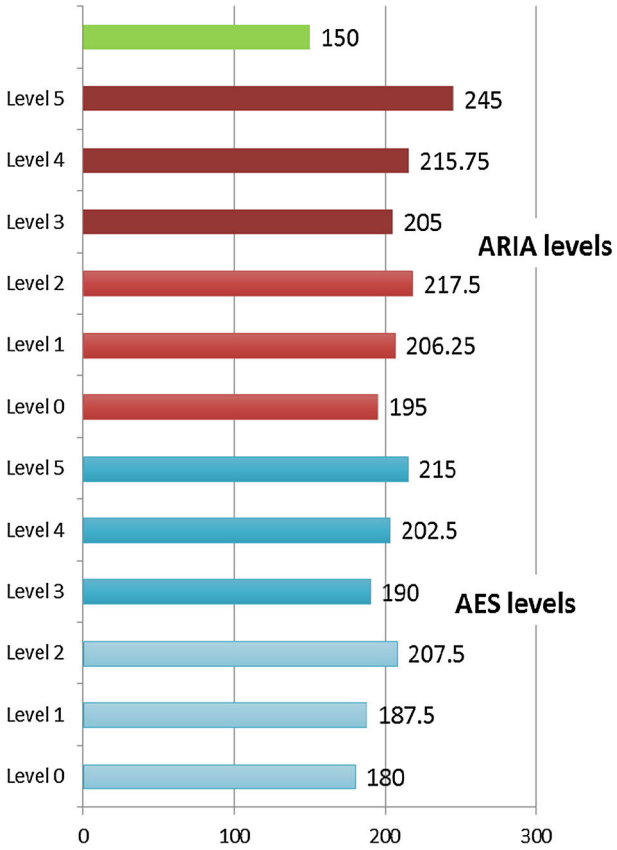

Fig. 13 Consumed energy comparisons between all security levels of AES and ARIA algorithms with the MACA protocol

It is not an exaggeration to conclude from the experience that a security mechanism requires more data packets and energy consumption. Therefore, such security mechanism is difficult to apply for UWASNs. However, in accordance with Fig. 13, the protocols with security mechanisms consume almost as much energy as the protocol without a security mechanism. The outcome indicates that a security mechanism is not substantial for underwater communication. In order to provide higher security strength, the CCM-UW mechanism does not demand a significant amount of MAC values or more energy because it is modified for UWASNs by reducing data size.

Lastly, Fig. 14 shows comparisons among CCM-AES and CCM-ARIA security levels and MACA protocol without security in terms of latency. CCM-AES levels spend more time than CCM-ARIA security levels in the result and there is no big difference with MACA protocol. The result shows the system with CCM-UW modes does not need extra energy and time.

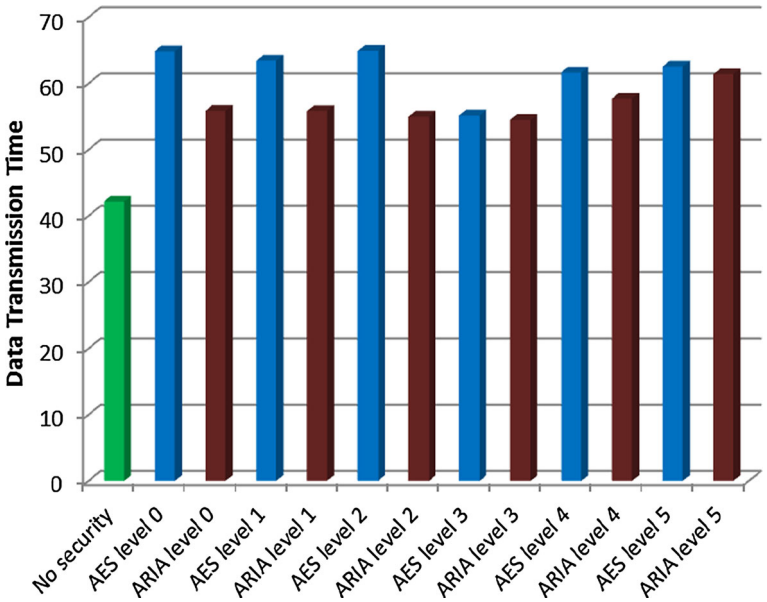

Fig. 14 Transmission time comparison between all security levels of AES and ARIA algorithms with the MACA protocol

6 Conclusions

In this paper, upon making use of the CCM-UW mode altered from the CCM* mode based on the AES and ARIA algorithms, we demonstrated an energy efficient secured MAC protocol, and made comparisons regarding each security level and algorithm. We examined the proposed secured MAC protocol with the existing MAC protocol with the help of empirical experiment consequences, and supplied the energy consumption of each security level of the CCM-UW; we also suggested a reference for applying security in underwater acoustic communication to developers or vendors. This result is not optimized, but provides sufficient data to research and deploy network security in underwater communication. We also showed the possibility of applying modern cryptographic technology. The technology for underwater security can work along another network system, such as IEEE 802.11 (WLAN), IEEE 802.15.3 (UWB), or IEEE 802.15.4 (ZigBee).

Acknowledgments This work is part of the results for the research "Development of the wide-band underwater mobile communication systems" supported by the Ministry of Oceans and Fisheries, Korea.

References

1. Akyildiz, I. F., Pompili, D., & Melodia, T. (2005). Underwater acoustic sensor networks: Research challenges. *Ad hoc Networks, 3*(3), 257–279.
2. Detweiller, C., Vasilescu, I., & Rus, D. (2007). An underwater sensor network with dual communications, sensing, and mobility. *Proceedings of OCEANS* 2007-Europe, pp. 1–6.
3. Dini, G., & Lo Duca, A. (2012). A secure communication suite for underwater acoustic sensor networks. *Sensors, 12*(11), 15133–15158.

4. Yi, O., et al. (2014). Implementation of ARIA Cryptographic Modules based on ARM9 Devices. *International Journal of Security and Its Applications, 8*(2), 243–250.
5. Domingo, M. C. (2011). Securing underwater wireless communication networks. *Wireless Communications IEEE, 18*(1), 22–28.
6. Jiang, H. F., & Xu, Y. (2011). Research advances on security problems of underwater sensor networks. *Advanced Materials Research, 317*, 1002–1006.
7. Yang, G., Wei, Z., Cong, Y., & Jia, D. (2012). Analysis of security and threat of underwater wireless sensor network topology. *Fourth International Conference on Digital Image Processing* (ICDIP 2012). International Society for Optics and Photonics.
8. Dong, Y., & Liu, P. (2010). Security considerations of underwater acoustic networks. *Proceedings of the International Congress on Acoustics* (ICA'10), Sydney, Australia.
9. Zuba, M. et al. (2015). Vulnerabilities of underwater acoustic networks to denial of service jamming attacks. *Security and Communication Networks, 8*(16), 2635–2645.
10. Singh, Y., Barak, D. D., Siwach, V., & Rani, P. (2012). Attacks on wireless sensor network: A survey. *International Journal of Computer Science and Management Studies, 12*(3), 2231–5268.
11. Katariya, A., Arya, A., & Minda, K. (2010). Coded under water acoustic communication (UWA) with cryptography. In *Computational Intelligence and Communication Networks (CICN), 2010 International Conference on* (pp. 493–497). IEEE.
12. Yan, H., Shi, Z. J., & Fei, Y. (2009). Efficient implementation of elliptic curve cryptography on DSP for underwater sensor networks. In *7th Workshop on Optimizations for DSP and Embedded Systems (ODES-7)* (pp. 7–15).
13. Kim, Y.-P., An, J.-W., Park, S.-H., et al. (2012). Data encryption and authentication mechanism based on block cipher mode for underwater acoustic sensor networks. *Proceeding of the 2012 International Conference on Information Science and Technology, Part 1,* April 28–30, pp. 374–376, Shanghai, China.
14. Cong, Y., Yang, G., Wei, Z., & Zhou, W. (2010). Security in underwater sensor network. In *Communications and Mobile Computing (CMC), 2010 International Conference on* (Vol. 1, pp. 162–168). IEEE.
15. Ateniese, G., Capossele, A., Gjanci, P., Petrioli, C., & Spaccini, D. (2015). SecFUN: Security Framework for Underwater acoustic sensor Networks. In *Proceedings of OCEANS-Genova*, 1–9.
16. Dini, G., & Duca, A. L. (2011). SeFLOOD: A secure network discovery protocol for Underwater Acoustic Networks. In *Computers and Communications (ISCC), 2011 IEEE Symposium on* (pp. 636–638). IEEE.
17. Xu, M., Liu, G., & Guan, J. (2015). Towards a secure medium access control protocol for cluster-based underwater wireless sensor networks. *International Journal of Distributed Sensor Networks, 2015*, 40.
18. Caiti, A., Calabro, V., Dini, G., Lo Duca, A., & Munafo, A. (2012). Secure cooperation of autonomous mobile sensors using an underwater acoustic network. *Sensors, 12*(2), 1967–1989.
19. Shin, S. Y., Namgung, J. I., & Park, S. H. (2010). SBMAC: Smart blocking MAC mechanism for variable UW-ASN underwater acoustic sensor network environment. *Sensors, 10*(1), 501–525.
20. Melodia, T., Kulhandjian, H., Kuo, L. C., Demirors, E. (2013). Advances in underwater acoustic networking. In: *Mobile Ad Hoc Networking: Cutting Edge Directions* (p. 852).
21. Lee, J.-Y., et al. (2013). A MAC protocol based on flexible RWT for underwater mobile ad-hoc networks. *OCEANS-Bergen, 2013 MTS/IEEE*. IEEE.
22. Yi, O., Yun, S., Park, M., & Song, H. (2014). Implementation of ARIA cryptographic modules based on ARM9 devices. *International Journal of Security and Its Applications, 8*(2), 243–250.
23. Jeon, J.-H., Yun, N.-Y., Park, S.-H., et al. (2012). A moving underwater communication system with bio-inspired fish robots. In *Proceedings of the Seventh ACM International Conference on Underwater Networks and Systems*, WUWNet '12, No. 15.

Mukhridinkhon Ibragimov has received his B.S. degree in Information Technologies department at Tashkent University of Information Technologies, Tashkent, Uzbekistan in 2013. He is studying for a master's degree in Financial Information Security, Kookmin University. His fields of interest are Underwater Delay/Disruption Tolerant Networks (UWDTNs), Security algorithms and mechanisms, Internet of Underwater Things (IoUT), M2M and smart devices, embedded software and systems.

JaeHoon Lee has received his B.S. in mathematics from Kookmin University in 2013. Now, he is unified master and doctor degrees course in the Department of Financial Information Security, Kookmin University, Korea. His current research interests the Network Security.

Muppalla Kalyani has received her Bachelor degree in 2009 from Sri Venkateswara University, India and received Master's degree in 2012 from JNTU Anantapur University, India. Currently she is Ph.D. student in Graduate School of Business IT, Kookmin University, Korea. Her current research interests include Underwater IoT (Internet of Things), Underwater Delay and Disruption Tolerant Network and Implementing RTOS embedded software systems.

Jung-il Namgung has received his B.S. degree in mechanical engineering from Incheon University in 1995, M.S. and Ph. D degrees in Business IT from Kookmin University in 2005, 2011, respectively. Now, he is a BK21+ research professor in the department of Financial Information Security, Kookmin University. His current research interests include IoT (Internet of Things) / M2M (Machine to Machine communication) and Context Awareness / Service Composition / Artificial Intelligence.

Soo-Hyun Park has received his B.S., M.S. and Ph.D. degrees in computer science & engineering from Korea University in 1988, 1990 and 1998, respectively. Now, he is a professor in the Department of Information System, Kookmin University, Korea. His current research interests include Underwater IoT (Internet of Things), M2M system and Ubiquitous Network.

Okyeon Yi has received his M.S degree in Department of Mathematics from Korea University in 1990. He graduated his Ph.D. degree in Department of Mathematics from University of Kentucky in 1996. He was team leader at ETRI, Korea from 1999 to 2001. He is a professor in Department of Mathematics and Department of Financial Information Security, Kookmin University since 2001. His current research topics are: CMVP, Wireless Security, Mobile Security and IoT Security.

Changhwa Kim is a professor of the Department of Computer Science and Engineering at Gangneung-Wonju National University where he leads as a director Underwater Sensor Network Research Center located in that university. He graduated with Bachelor's degree in 1895 from Korea University located in Seoul, Korea, and he has also received his M.Sc. and Ph.D. in 1987 and 1990, respectively, from the same university.

His research interests are in Underwater Acoustic Communication and networks, Internet of Things (IoT), Distributed Systems, and Intelligent Systems. Her work has explored the development of protocol stacks, system components, and their integration for the implementation of underwater acoustic communication and network system. His current research focuses on an underwater IoT as an integration of underwater acoustic communication and the current IoT concepts.

Yong-Kon Lim has received his the M.S. degrees in power and electrical engineering from Chung-Nam University in 1984 and Ph. D degrees in electronic engineering from A-Jou University in 1994, respectively. He has been working at Korea Research Institute of Ships and Ocean Engineering (KRISO) since 1980. Presently, he is a principal researcher and a professor in the department of ship and ocean engineering at University of Science and Technology (UST). His main interests are underwater acoustic telecommunication, underwater acoustic network, integrated logistic system for Ocean, and integrated communication system for ships.