Data Encryption and Authentication Mechanism based on Block Cipher Mode for Underwater Acoustic Sensor Networks

Yung-Pyo Kim¹, Jung-Woo An², Soo-Hyun Park¹, Okyeon Yi², JuHum Kwon³, Chang-Hwa Kim⁴

¹ Ubiquitous System Lab., Graduate School of Business IT, Kookmin University, Korea
{kuniv003, shpark21}@kookmin.ac.kr
² Cryptography & Information Security Inst., Graduate School, Kookmin University, Korea
{anjungwoo, oyyi}@kookmin.ac.kr
³ Korea Air Force Central Computer Center, Korea
jkweon@gmail.com
⁴ Ocean Sensor Network System Technology Research Center, Gangneung-Wonju National University, Korea
kch@gwnu.ac.kr

Abstract. In recent years, due to a variety of potential applied areas and unlimited possibilities, the underwater acoustic sensor networks and related researches have been focused and conducted continually. However, the underwater acoustic sensor networks have lots of constraints in applying the technique because the underwater communication uses different electrical signal compared with the ground communication environment. Due to the differences, applying the ground security mechanism intact is almost impossible in the way that is used in ground. This paper introduces the characteristics of underwater acoustic environment and related security mechanism that is used in terrestrial wireless sensor networks. And, based on those considerations, propose security mechanism that can be used in underwater acoustic environment. The proposed security mechanism guarantees the integrity and confidentiality of data. Further, this paper gives emphasis on the minimization of the size of data frame that is also an important data factor in the underwater acoustic sensor networks. In the future, simulation for the proposed mechanism will be implemented in order to verify the applicability to the real underwater acoustic environment.

1 Introduction

The underwater acoustic communication can be applied in various areas. Examples include the monitoring of marine environment, the development and search of deep underwater, the collection of ocean data, tactical use of the military purpose, etc. In recent years, the necessity of using underwater acoustic sensor networks is being escalated due to the rising interest for both public and academic. However, the difference from that of the ground communication and the underwater environment which cannot use the Radio Frequency (RF) signal is constrained to a limited communica-
tion using the acoustic signal. The efficiency of the underwater communication using acoustic is significantly low because of the long transmission delay and the packet collision. Furthermore, exchanging battery in a node is not relatively easy in the underwater environment. Therefore, reducing consumption of electric power and thereby maximizing energy efficiency is another issue to be resolved. Because of these environmental limitations, applying security in the underwater acoustic communication is rather difficult. The security in underwater acoustic sensor network should not only guarantee the requirement of secure data communication but also meet the need of efficiency of node to node communications. Furthermore, in order to construct secure communication environment from the diverse cyber-attacks, proper countermeasures should be accompanied together with the analysis of the network characteristics and the corresponding threat. This paper diagnoses the considerations as to apply security mechanism that is suitable for the underwater acoustic sensor networks; furthermore, proposes the data encryption and the authentication technique based on the corresponding block encryption algorithm.

2 Security Mechanism on UWASN

All things considered above, this paper suggests the appropriate security mechanism on UWASN: the OFB or CTR mode using block cipher for data encryption and decryption, and CMAC for message authentication. The OFB and CTR mode, which can be used as stream cipher, require no further costs and only need small bits of length for data authentication. Also, it is possible to control the CMAC depending on the situation of underwater network, which could maximize the efficiency. Figure 2 shows the security mechanism to provide encryption and data authentication. Figure 3 displays how to create key stream for encryption.

![Figure 1. Adaptive encryption and data authentication mechanism for underwater communication environment](image-url)
A lot of block cipher such as AES, T-DES, etc. can be applied to the n-bit block cipher algorithm. For sure, you just can follow the block cipher system that each nation's security policies insist. Also, the cipher key and Integrity key has to be derived from the secret key that is previously shared. The receiver can decrypt the cipher to get plain text and is able to create MAC and authenticate the message by matching the MAC created with the MAC transmitted.

3 Conclusion and Future Work
As the interests in underwater environment, which has numerous application fields and unlimited possibility, keep increasing, a number of researches are being done pertaining to this issue. However, the research on underwater acoustic sensor network applying security seems to stand still. This paper has introduced security mechanisms which is used on the ground and suggested the suitable security mechanism for acoustic sensor network, considering the limitations of underwater environment. In the underwater network, in order to achieve the efficiency of transmission, the length of data frame has to be minimized regardless of whether the security is applied or not. Simultaneously, it is required to satisfy the security requirement on wireless communication and should consider the limitations of underwater environment. Therefore, we have chosen block cipher modes of operation, the OFB and CTR to increase efficiency in data transmission, and picked CMAC for message authentication.

However, when it comes to availability, one of the key requirements as well as integrity and confidentiality, it still requires to be simulated to prove this point. Not only that, initial vector for generating key stream, the counter management, and the proper length of MAC need to be worked on more.
In the future, the researches on the problems such as DoS, replay attack by collision and error, black hole, synchronization from the security perspective by each level of protocol should proceed, and this should also prove the feasibility to realize in the real world.

Acknowledgment
This work was supported by the IT R&D program of MKE/KEIT. [10039140], Development of Crypto Algorithms (ARIA, SEED, KCDSA, etc.) for Smart Devices(ARM7/9/11, UICC).