Journal of Korea Multimedia Society Vol. 20, No. 12, December 2017(pp. 1940-1950)
https://doi.org/10.9717/kmms.2017.20.12.1940

수중 음파 센서네트워크에 기존 네트워크 보안을 적용하기 위한 고려사항과 논쟁점

신동현[†], 이승준[††], 김창화[†††]

Considerations and Issues for Applying the Existing Network Security to Underwater Acoustic Sensor Networks

DongHyun Shin[†], Seung-Jun Lee[††], Changhwa Kim[†††]

ABSTRACT

The security threat types in underwater communication networks environment are almost the same as the terrestrial, but the security of mechanisms the terrestrial RF-based networks environment can not be directly applied due to not only the limited resources of each node but also unsafe channel such as low propagation delay, high bit error rate etc. Nevertheless there has not been much research on the security of underwater acoustic communication networks. Therefore, in this paper analyzes the differences between the terrestrial communication networks and underwater acoustic communication networks, and identifies issues that are the starting points of underwater communication networks security research.

Key words: UWASN Security, Consideration for UWASN Security, Issues for UWASN Security

1. 서 론

바다는 지구 전체 면적의 약 70%이상을 차지하지만 지금까지 육상에 비해 관심을 덜 받아왔다. 하지만 육상 자원의 고갈과 해양에 대한 관심이 고조되면서 최근 몇 년간 해양자원에 대한 탐사, 개발, 활용에 대한 중요성이 증대되었으며, 이에 따라 해양 자원 탐사를 위한 해양 환경 모니터링 등을 위한 장비 등의 개발에 관심이 높아지고 있다 [1]. 그 중 대표적으로 수중 환경을 모니터링 할 수 있는 수중 음파 센서네트워크 시스템이 현재 개발되어 운용되고 있다 [2,3,4].

수중에서 사용하는 센서네트워크는 활용 분야 및 새로운 패러다임의 영향으로 새롭게 도출된 요구사항을 반영하여 발전됨에 따라 수중 음파 센서네트워크에 대한 보안 위협들이 생겨나고 있다. 수중 센서네트워크에서 발생하는 보안 위협은 기존 지상 통신 네트워크에서 발생하는 보안 위협들의 종류는 같지만 발생 장소가 다를 뿐이다. 이러한 보안 위협에 대응하기 위해서는 기밀성, 무결성 등에 해당하는 보안의 요소들을 만족하는 수중 음파 센서네트워크 환경에 적합한 보안이 필요하다.

※ Corresponding Author : Changhwa Kim, Address: (26403) 150, Namwon-ro, Heungop-myeon, Wonju-si, Gangwon-do, Korea, TEL : +82-33-760-8663, FAX : +82-33-760-8718, E-mail : kch@gwnu.ac.kr
Receipt date : Sep. 15, 2017, Revision date : Nov. 10, 2017
Approval date : Nov. 30. 2017
[†] Department of Computer Science & Engineering, Gangneung-Wonju National University
(E-mail : dhshin@cs.gwnu.ac.kr)
[††] Department of Computer Science & Engineering, Gangneung-Wonju National University
(E-mail : sjlee@cs.gwnu.ac.kr)
[†††] Department of Computer Science & Engineering, Gangneung-Wonju National University
※ This research was a part of the project titled "Development of the wide-band underwater mobile communication systems" funded by the Ministry of Oceans and Fisheries, Korea.

그러나 기존 지상에서의 보안에 대한 연구는 오래 전부터 진행되어왔지만 수중에 대한 연구 자체가 시작 된지 얼마 되지 않았기 때문에 수중 보안 연구도 충분히 진행되지 못했다. 따라서 수중 환경은 지상 환경과 보안위협이 거의 동일하기 때문에 수중 음파 센서네트워크에 지상에서 연구된 보안 기법을 적용하는 것으로 생각해볼 수 있다. 하지만 수중 환경의 경우 지상 환경에 비해 높은 에너지 소모, 한정된 메모리, 높은 에러율 등의 제약사항으로 인해 지상의 보안을 곧바로 적용하기 어렵다 [5,6]. 따라서 수중 음파 센서네트워크에 지상 환경에서 연구된 보안을 적용하기 위해서는 수중 환경에 적합하도록 수정해야 한다. 이를 위해 본 논문에서는 지상에서 연구된 보안을 수중 음파 센서네트워크 보안에 적용할 때 발생하는 문제점과 요구사항을 분석하고, 지상에서 연구되었던 보안을 수중 음파 센서네트워크에 적용하기 위한 이슈와 논쟁점들을 다룬다.

본 논문은 2절에서 관련 연구, 3절에서 수중 음파 통신 센서네트워크의 특성을 비교하고, 두 네트워크의 차이로 인해 발생하는 문제점으로 인해 고려해야 할 사항을 4절에서 다룬다. 5절에서는 수중 음파 센서네트워크에 보안을 적용하기 위한 이슈와 논쟁점을 다루며, 6절에서 결론으로 마무리 짓는다.

2. 관련연구

기존 연구에서는 보안을 위해 크게 4가지 보안 요소가 지켜져야 한다는 결론을 얻었다. 이 보안 요소에는 대표적으로 인가되지 않은 개체에게는 데이터를 공개하지 않으며, 오직 인가된 개체에게만 데이터를 공개하는 것을 말하는 기밀성, 원래의 데이터가 전송, 저장 등에도 변함없이 유지되고 있음을 증명하는 성질인 무결성, 통신 개체에 대한 신원 정보를 확인하여 유효성을 확립하는 인증, 적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근할 수 있도록 통제하는 접근제어가 있다 [7].

이 보안요소들은 물리층의 Jamming 공격, 데이터링크층의 Collision, Exhaustion 공격, 네트워크층의 Neglect, Greed, Misdirection, Black holes, Worm-hole 공격 등의 보안 위협들을 예방하는데 효과를 줄 수 있으며 지상 환경에는 위에서 나열한 보안 위협들을 예방하기 위한 보안 연구가 활발하게 진행되었다. 지금까지 수중 환경에 대한 연구 자체가 활발하게 연구되지 않았기 때문에 수중 환경에 보안을 적용하기 위한 보안 연구 또한 지상에 비해 많이 부족한 상황이다. 수중 환경에서의 보안 위협은 지상 환경에서의 보안 위협과 거의 동일하기 때문에 지상 환경의 보안을 수중 환경에 적용해볼 수 있다고 생각하지만 수중 환경의 경우 지상과 달리 노드의 제한된 메모리, 느린 전파지연, 높은 통신 에러율, 에너지 소모 등의 제약사항 때문에 지상에서 사용 중인 보안을 그대로 적용하기란 어렵기 때문에 수중 환경의 특징을 고려한 보안이 필요하다 [8,9].

최근에는 열악한 수중 환경에 보안을 적용하기 위한 연구들이 하나씩 진행되고 있다. 수중 환경에서 안테나의 통신 구역을 활용하여 웜홀 공격을 판단하는 방법에 대한 연구 [10], 수중 환경에 적합한 암호화 키 경량화 알고리즘[11,12], 수중 환경에 암호알고리즘을 적용하기 위한 성능 비교 [13] 등이 연구되었다. 하지만 현재까지 진행된 대부분의 연구들은 수중 환경에 적합한 암호화 알고리즘 경량화에 주로 초점이 맞추어져있다. 따라서 지상의 보안을 수중 환경에 적용하기 위한 요구사항을 일부만 반영하여 곧바로 적용할 수 없는 문제를 가지고 있다.

3. 수중 음파 통신 센서네트워크의 특성

본 절에서는 수중 음파 통신 센서네트워크가 갖는 특성에 대해 서술한다. 수중 환경에서는 RF 통신을 사용할 수 없기 때문에 지상 환경과는 달리 주로 음파 통신을 사용한다. 3.1절에서는 수중 음파 통신의 특성을 살펴보고, 3.2절에서는 수중 음파 통신을 사용하는 센서 네트워크의 특성을 분석한다. 3.3절에서는 3.1절과 3.2절에서 분석한 내용을 바탕으로 수중과 지상 통신에는 어떠한 차이가 있는지 비교한다.

3.1 수중 음파 통신의 특성

수중 음파 통신의 특성은 여러 방면에서 지상의 RF 통신과는 다른 특성을 갖는다. 본 절에서는 대표적으로 7가지 항목에 대한 특성을 다룬다. 수중 음파 통신의 7가지 특성에 대한 자세한 내용은 다음과 같이 정리할 수 있다.

- 운영환경 : 수중 환경에서는 지상 환경과는 다르게 음파 통신을 주로 사용한다. 지상에서 사용하는 RF 통신은 음파 통신에 비해 빠른 전파 속도, 다양한

주파수 대역폭과 사용 가능한 채널 등의 장점이 존재함에도 불구하고 수중에서 RF 통신을 사용할 경우 빛의 감쇠 현상으로 인해 통신이 불가능하기 때문이다.

• 전파속도 : 지상 환경에서 사용하는 RF 통신의 경우 300,000Km/s의 전파 속도를 갖지만 수중 환경에서 사용하는 음파통신의 전파 속도는 평균적으로 1.5Km/s의 전파 속도를 갖는다. 게다가 음파통신은 노드 간의 통신 거리, 수압, 염도, 온도, 탁도 등에 민감하게 영향을 받기 때문에 전파 속도와 거리가 일정하지 않은 특성을 갖는다.

• 주파수 대역폭 : 수중 환경에서 사용하는 주파수 대역폭은 일반적으로 3~70KHz 대역을 사용하고 있다. 지상에 비해 굉장히 한정적인 주파수 대역폭을 가지고 있기 때문에 통신을 위해 사용 가능한 채널의 수도 굉장히 제한적이며 한정적인 주파수 대역으로 인한 간섭 현상도 많이 발생하는 특성을 갖는다.

• 통신 에러율: 수중 음파 통신은 환경 요소에 굉장히 가변적이고 경로 손실, 멀티 패스, 도플러 효과, 지표면 덕트(Surface Duct), 해저 반사(Bottom Bounce) 등의 특성으로 인해 높은 통신 에러율을 갖는다. 이로 인해 데이터 손실률이 지상에 비해 더 높으며, 수중 통신에서의 최대 패킷 크기는 지상에 비해 더 작은 특성을 갖는다.

• 높은 전력 소비 : 수중 환경에서 사용하는 음파 통신은 지상에서 사용하는 RF 통신에 비해 더 높은 소비전력을 갖는다.

• 센서 노드의 이동성 : 수중 환경에는 지상에 비해 노드를 고정시키기 어려운 특성을 갖는다. 그렇기 때문에 수중 바닥에 노드를 설치하지 않는 이상 수중에 설치된 노드는 물의 흐름에 굉장히 민감한 영향을 받아 노드의 위치가 심하게 이동할 수 있는 특성을 갖는다.

• 3D 위치인식 : 수중 환경에 설치된 노드들은 수중에서 물의 흐름에 따라 수평, 수직 방향으로 이동하게 된다. 따라서 수중 노드의 위치를 파악하기 위해서는 3D 네트워크 구조를 통해 노드의 위치를 인식할 수 있으며, 이 방법은 2D 구조에서 노드의 위치를 인식하는 것보다 훨씬 복잡한 특성을 갖는다.

3.2 수중 음파 통신 센서네트워크의 특성과 문제점

수중 음파 통신 센서네트워크는 Fig. 1과 같이 센서 노드, 수중 싱크 노드, 수표면 게이트웨이 등으로 구성된다. 센서 노드는 수중에 설치되어 수중 환경 정보를 센싱하고 주위의 센서 노드 혹은 수중 싱크 노드에게 데이터를 전달한다. 데이터를 전달받은 노드는 최종적으로 수표면에 있는 게이트웨이를 통해 목적지 까지 데이터를 전달한다. 이러한 수중 음파 통신 센서네트워크는 일반적으로 지상에서 운용되

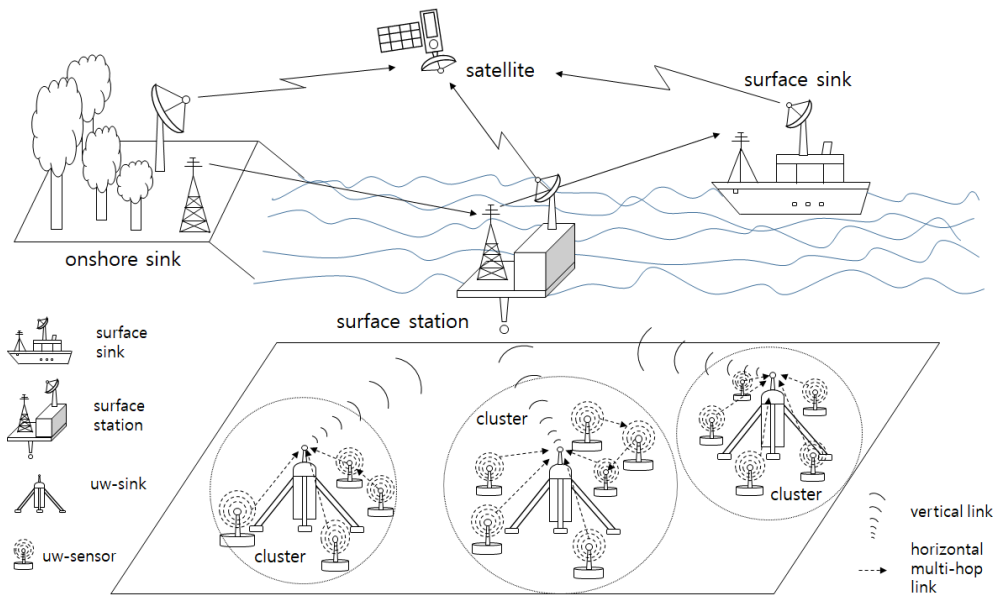

Fig. 1. Structure of Underwater Acoustic Communication Sensor Network.

는 센서네트워크의 특징과 수중 음파 통신을 사용함으로써 갖는 수중 음파 통신의 특성을 함께 가지고 있다. 일반적인 센서네트워크는 일반적으로 저가격, 초소형으로 만들어져 넓게 분포되기 때문에 하드웨어 자원이 제한적이며, 그로 인해 센서네트워크가 갖는 일반적인 특징은 다음과 같다.

첫째, 한정된 메모리 공간을 갖는다. 메모리 소형화 기술은 점점 발전되고 있지만 그만큼 가격은 비싸지게 된다. 센서네트워크를 구성하는 노드는 저가격, 초소형으로 만들어야 되기 때문에 가격이 낮으면서 초소형으로 만들기에는 메모리 공간이 한정적일 수밖에 없다.

둘째, 느린 처리속도를 갖는다. 한정된 메모리 공간과 마찬가지로 가격과 성능을 고려하여 MCU를 제작하여야하기 때문에 MCU의 성능 또한 일반적인 PC, 스마트폰 등에 비해 낮다.

셋째, 에너지 효율이 중요하다. 센서네트워크는 기본적으로 인간이 쉽게 접근할 수 없는 곳에 설치되어 센서 데이터들을 수집하기 때문에 주로 무선 배터리를 사용한다. 따라서 주기적인 배터리의 교체가 필요하며, 배터리 교체가 쉽지 않기 때문에 에너지 효율이 굉장히 중요하다.

지상에서 운용되는 일반적인 센서네트워크와 수중 음파 통신의 특성을 함께 가지고 있는 수중 음파 통신 센서네트워크의 특성은 다음과 같이 정리할 수 있다.

첫째, 수중 환경에 센서네트워크가 설치되어 운용된다. 수중 음파 통신 센서네트워크는 수중 환경의 데이터를 수집하여 활용하기 때문에 설치 또한 수중 환경에서 이루어진다.

둘째, 노드의 설치 간격이 좁다. 수중 통신은 통신 에러율이 높고 전파 시간이 길기 때문에 지상 환경보다 노드를 더욱 촘촘히 배치할 수밖에 없다.

셋째, 통신 에러율이 높다. 수중 환경에서 사용하는 음파통신의 경우 좁은 주파수 대역폭과 도플러 현상 등으로 인해 통신 에러율이 높다. 이로 인해 센서 데이터가 손실될 확률이 더 높아질 수 있다.

넷째, 에너지 효율이 중요하다. 센서네트워크는 인간이 쉽게 접근할 수 없는 곳에 주로 설치되기 때문에 에너지 효율에 대한 문제는 항상 고려해야 할 문제이다. 하지만 수중 환경의 경우 음파 통신이 지상에서 사용하는 RF 통신에 비해 더 많은 에너지를 소모하고, 지상에 비해 배터리 교체의 수월성이 더 낮기 때문에 지상의 센서네트워크보다 에너지 효율을 더욱 고려해야 한다.

마지막으로 수중 채널환경이 좋지 않다. 수중 통신의 대역폭은 약 3~100KHz로 RF통신에 비해 굉장히 제약적이기 때문에 수중 채널도 제한되어있다. 뿐만 아니라 수중 환경에서 사용하는 수중 음파 통신의 경우 노이즈에 굉장히 취약하다.

3.3 수중 음파 통신과 지상 통신의 비교

Table 1은 3.1절과 3.2절에서 다룬 내용을 바탕으로 수중 음파 통신 센서네트워크와 지상 센서네트워크를 포함한 지상 통신 네트워크의 특징을 비교한 것이다. 수중 음파 통신 센서네트워크와 비교대상이 되는 지상 통신 네트워크의 종류는 와이파이, 블루투스, 모바일, 지상 센서네트워크가 있다.

수중 음파 센서네트워크는 기본적으로 음파를 이용하여 통신을 하며 전파속도는 RF 통신에 비해 약 20만배 이상 느린 특성을 갖는다. 수중 음파 센서네트워크는 음파 통신을 사용하기 때문에 음파 통신의 특성으로 인해 사용가능한 통신 채널의 수도 굉장히 제한적이다. 또한 일반적으로 지상 환경보다 수중 환경은 배터리 교체가 더 어렵고, 통신 시 에너지를 더 많이 소모하기 때문에 에너지 효율이 굉장히 중요한 특징을 가진다. 기타 자세한 내용은 Table 1을 참고하면 된다.

4. 수중 음파 센서네트워크의 보안 고려사항

본 절에서는 3절에서 식별된 수중 음파 통신 센서네트워크의 특성을 기반으로 기존 지상 중심의 무선네트워크에 적용된 보안을 수중 음파센서네트워크 보안에 적용할 경우의 고려사항에 대해서 논의하도록 한다. 4.1절에서는 수중 음파 통신에 기존의 보안을 적용하기 위한 고려사항에 대해 분석하고, 4.2절에서는 수중 음파 통신에 기존의 보안을 적용하기 위한 문제점과 고려사항의 관계에 대해 정리한다.

4.1 수중 음파 센서네트워크에 보안 적용을 위한 고려사항

4.1.1 암호화 키 경량화

평문을 암호화 시키기 위해서는 암호화 키를 사용

Table 1. Comparison of Underwater Acoustic Sensor Networks and Terrestrial Communication Networks

	Wi-Fi	Bluetooth	Mobile	Terrestrial Sensor Network	Underwater Acoustic Sensor Network
Communication Type	RF	RF	RF	RF	Acoustic
Wire/Wireless	Wireless	Wireless	Wireless	Wire/Wireless	Wire/Wireless
Frequency	2.4GHz, 5GHz	2.4GHz	2.1GHz	445~2450MHz	3~100KHz
Communication Environment	Terrestrial	Terrestrial	Terrestrial	Terrestrial	Underwater
Bit rate	10Mbps	1Mbps	144Kbps~384Kbps	20~250Kbps	40bps~15Kbps
Node Type	Smart Phone, Laptop, etc.	Smart Phone, Laptop, etc.	Smart Phone, etc.	Embedded Device	Embedded Device
Memory	512MB	512MB	512MB	Up to 1MB	Up to 1MB
Battery Using	None	Yes/None	Yes	Yes	Yes
Battery Replacement	N/A	Easy	Easy	Difficult	Difficult
Energy Consumption	High	Low	Low	Low	Very High
Propagation Delay	300,000Km	300,000Km	300,000Km	300,000Km	1.5Km
Mobility	Yes	Yes	Yes	Yes/No	Yes/No

하여 암호화를 하게 되며 암호화 키는 암호화 알고리즘에 의해 사용된다. 암호화 키의 길이가 길수록 평문을 암호화 하는데 더욱 복잡해지며 Fig. 2와 같이 그에 따른 처리 시간과 처리 능력, 에너지 소모가 요구된다. 수중 음파 통신 센서네트워크는 하드웨어의 제약으로 인해 메모리가 한정적이고 처리 시간이 오래 걸릴 뿐만 아니라 음파 통신 사용 시 일반적인 RF 통신에 비해 에너지가 더 많이 소모되는 특징을 가지고 있다.

따라서 수중 음파 통신 센서네트워크에서 암호화 키를 사용하기 위해서는 처리 시간, 처리 능력, 에너지 소모를 줄이기 위해 암호화 키를 경량화 할 필요가 있다. 암호화 키의 길이가 길어질수록 암호화 레벨은 높아지지만 그만큼 암호화 키를 생성하는데 소요되는 시간과 에너지가 소모되므로 이 트레이드 오프 관계를 고려하여 수중 환경에 적합한 암호화 키 경량화 기술이 요구된다.

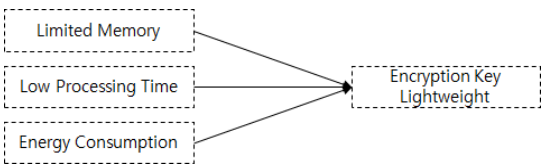

Fig. 2. Issues to Consider for Encryption Key Lightweight.

4.1.2 암호화 알고리즘 경량화

암호화 키를 이용하여 평문을 암호화 할 수 있는데 암호화 된 문서를 읽기 위해서는 암호화된 문서를 복호화 해야 한다. 이때 암호화 키를 이용하여 평문을 암호화 하고, 암호화된 문서를 다시 평문화 하는데 사용되는 모든 알고리즘이 암호화 알고리즘이며, 보안의 기밀성, 무결성, 인증을 유지시켜주는 중요한 요소이다. 암호화 알고리즘에 사용되는 키의 종류에 따라 암호화 키와 복호화 키가 같은 대칭 암호 알고리즘, 암호화 키와 복호화 키가 서로 다른 비대칭 암호화 알고리즘으로 나눌 수 있으며, 대칭 암호 알고리즘에는 대표적으로 DES, AES 알고리즘이 비대칭 알고리즘은 대표적으로 RSA 알고리즘이 존재한다.

암호화 알고리즘은 키 길이, 연산에 대한 성능이 요구되기 때문에 Fig. 3과 같이 암호화 키 경량화에서 고려해야 할 수중 통신의 특성을 함께 고려해야 한다. 따라서 에너지 효율이 중요하고 낮은 처리 능

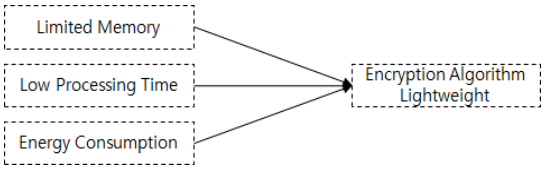

Fig. 3. Issues to Consider for Encryption Algorithm Lightweight.

력을 갖는 수중 음파 통신 센서네트워크에 암호화 알고리즘을 적용하기 위해서는 암호화 알고리즘의 경량화가 요구된다.

4.1.3 보안 메시지 길이 최소화

평문을 암호화하여 목적지로 전송하는 메세지를 보안 메세지라고 한다. 수중 음파 통신 센서네트워크에서는 보안 메시지의 길이 또한 최소화 시켜야 한다. 수중에서 사용하는 음파통신은 지상에서 사용하는 RF 통신에 비해 낮은 비트율과 높은 통신 에러율을 갖기 때문이다.

수중 음파 통신은 물의 온도, 노이즈, 탁도 등에 높은 영향을 받게 되는데, 이로 인해 통신 에러율이 높아지게 된다. 보안 메시지가 길어지면 보안 메시지를 분할하여 여러 번 전송해야 하는데, 이 경우 에너지 소모 문제가 발생할 뿐만 아니라 수중 음파 통신의 경우 Fig. 4와 같이 대역폭이 굉장히 제한적이고, 채널 환경이 매우 불안하므로 메시지 전송 시 음파의 간섭 현상이 일어나 메시지가 손실되어 메시지를 다시 재전송해야 할 가능성도 높아진다. 따라서 보안 메시지 길이를 최소화함과 동시에 수중 음파 통신 센서네트워크에서 요구하는 보안 레벨을 함께 만족해야 한다.

4.1.4 보안을 위한 통신 횟수 최소화

보안을 위해서는 보안 메시지를 송・수신하는 것

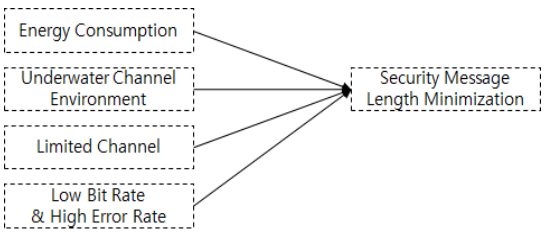

Fig. 4. Issues to Consider for Security Message Length Minimization.

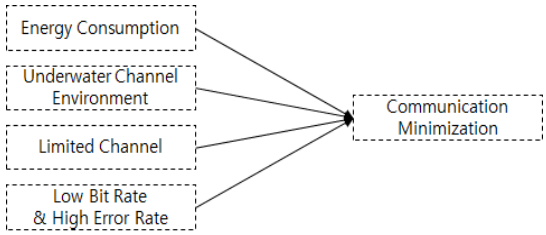

Fig. 5. Issues to Consider for Communication Minimization.

뿐만 아니라 보안을 위한 통신도 함께 요구된다. 수중 음파 통신 센서네트워크는 Fig. 5와 같이 에너지 효율이 중요하고 높은 통신 에러율의 특징을 갖기 때문이다. 또한 한정된 수중 음파 통신 채널로 인해 통신 횟수가 증가할수록 다른 노드들의 통신을 방해할 수 있게 되고, 수중 음파 통신 센서네트워크의 전체적인 에너지 소모가 함께 증가할 수 있기 때문이다. 따라서 수중 음파 통신 센서네트워크에 통신 횟수를 최소화 해야 한다.

4.1.5 이동성에 따른 보안 관리

일반적인 지상 센서네트워크에서의 노드는 이동성을 거의 가지고 있지 않지만 수중 음파 통신 센서네트워크에 설치된 노드들은 수표면, 수중 등에 설치되기 때문에 물의 흐름에 따라 이동을 하게 된다. 수중 혹은 수표면의 노드가 이동하게 되면 기존 라우팅 경로에서 벗어나게 되어 라우팅 경로가 재설정 되게 되는데 이러한 상황에서도 보안을 유지해야 한다.

특히 이동성을 위한 보안을 적용할 때에는 암호화 키, 보안 알고리즘, 보안 메시지 길이와 통신 횟수에 대한 내용이 모두 포함되기 때문에 Fig. 6과 같이 수

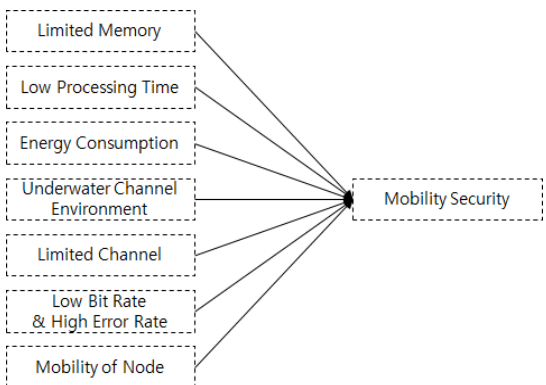

Fig. 6. Issues to Consider for Mobility Security.

중 음파 통신과 수중 음파 통신 센서네트워크의 문제점 중 제한된 메모리, 느린 처리속도, 에너지 소모, 수중 통신 환경, 한정된 채널, 낮은 비트율과 높은 에러율, 이동성을 모두 고려하여 보안을 적용해야 한다.

4.2 수중 음파 통신 센서네트워크 보안 적용의 문제점과 고려사항

수중 음파 통신 센서네트워크는 크게 제한된 메모리, 느린 처리시간, 에너지 소모, 수중 채널 환경, 제한된 채널, 낮은 비트율과 높은 에러율, 이동성의 문제를 가지며 이 문제들을 고려하여 수중 음파 통신 센서네트워크에 보안을 적용하기 위해서는 암호화 키 경량화, 암호화 알고리즘 경량화, 보안 메시지 길이 최소화, 통신 최소화, 이동성에 대한 보안이 요구되며 이들 간의 관계는 다음과 같다.

- 암호화 키 경량화 : 제한된 메모리, 느린 처리시간, 에너지 소모
- 암호화 알고리즘 경량화 : 제한된 메모리, 느린 처리시간, 에너지 소모
- 보안 메시지 길이 최소화 : 에너지 소모, 수중 채널 환경, 제한된 채널, 낮은 비트율과 높은 에러율
- 통신 횟수 최소화 : 에너지 소모, 수중 채널 환경, 제한된 채널, 낮은 비트율과 높은 에러율
- 이동성에 대한 보안 : 제한된 메모리, 느린 처리시간, 에너지 소모, 수중 채널 환경, 제한된 채널, 낮은 비트율과 높은 에러율, 노드의 이동성

암호화 키 경량화와 암호화 알고리즘 경량화 설계 시 지상 무선 네트워크에서 사용되는 노드와 다르게 수중 음파 센서 네트워크의 노드에서 사용될 수 있는 노드는 저가 및 낮은 사양과 지속적인 에너지 공급의 어려움으로 인해 한정된 메모리 공간, 느린 처리 속도, 에너지 소모를 고려해야 하며, 보안 메시지 길이 최소화와 통신 횟수 최소화는 긴 전파 지연 시간과 수중 환경에 따라 에러율이 급변하게 변화하는 음파 통신의 특성으로 인해 전송률, 수중 채널 환경, 에너지 소모, 통신 채널 상태를 고려해야 한다. 특히 통신 에러율을 감소시키기 위해 수중 환경에서 메시지를 작은 크기로 잘라서 여러 번 전송할 경우 노드의 에너지 소모와 통신 채널 점유율이 증가하기 때문에 적절한 트레이드오프 관계 설정이 중요하다. 마지막으로 이동성에 대한 보안은 기존에 식별된 모든 문제점을 포함하여 노드의 이동성을 고려하여 보안을 설계해야 한다.

5. 수중 음파 통신 센서네트워크 보안 이슈와 논쟁점

본 절에서는 수중 음파 통신 센서네트워크에 기존의 보안을 적용하기 위한 이슈와 논쟁점에 대하여 서술한다. 4절에서 식별한 수중 음파 통신 센서네트워크에 기존의 보안을 적용할 경우의 문제점과 고려사항을 수중 음파 통신 환경에 적합한 토폴로지, 수중 음파 통신 센서네트워크 암호화를 위한 경량화와 수중 음파 통신 센서네트워크 통신에 대한 경량화, 수중에서의 이동성에 따른 보안관리로 나누어 보안 이슈와 논쟁점을 다루며, 해당 내용은 각각 5.1절부터 5.4절에서 상세히 다룬다.

5.1 수중 음파 통신 환경에 적합한 토폴로지

수중 음파 통신의 경우 비트 에러율이 약 10^{-3}으로 지상 RF 기반 통신에 비해 1,000~10만배 이상 비트 에러율이 높을 뿐만 아니라, 전파 지연의 경우 약 1.5 km/s로 지상에 비해 20만배 느리고, 주파수 대역폭이 20~70KHz로 제한적이다. 데이터율도 지상에 비해 굉장히 낮으며, 수중 채널 상태 또한 불안정하기 때문에 통신 오류가 빈번하다. 따라서 인증, 키 분배 등의 보안을 위한 통신을 여러 번 진행해야 하는 문제가 발생하고 이로 인해 채널 점유율이 높아지는 문제가 생기게 된다. 따라서 Fig. 7과 같이 수중 환경에서는 클러스터 헤드 기반 구조를 따른다.

클러스터 헤드 기반은 클러스터 헤드와 1홉으로

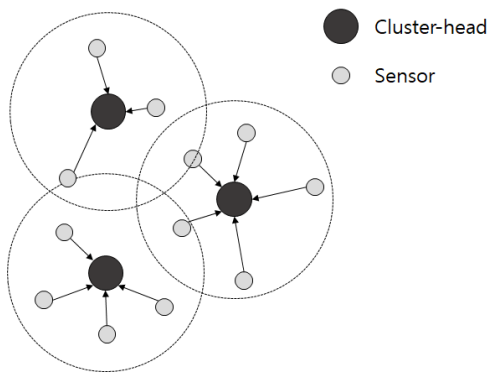

Fig. 7. Cluster-head based Network Topology.

연결되어 있으며, 클러스터 헤드는 다른 헤드와 바로 통신이 가능하기 때문에 주파수 채널 대역폭이 낮고, 비트 에러율이 높은 등의 열악한 수중 환경에서 인증, 암호화 키 분배 등을 위한 메시지 전송이 한 번의 통신으로 이루어지기 때문에 메시지 전송이 성공할 확률이 높은 장점을 가지고 있다.

클러스트 헤드 토폴로지의 클러스트 헤드는 키 분배, 인증 노드의 역할을 함께 할 수 있고, 제한된 주파수 채널 대역폭, 낮은 전파지연, 낮은 데이터율로 인한 채널 점유 현상이 빈번하기 때문에 채널을 효율적으로 관리할 수 있어야 한다. 이러한 클러스터 헤드 토폴로지에 DTN 의 개념을 함께 도입하면, 최초 노드에서 인증, 키 분배 등 목적의 메시지 전송 시 통신 장애로 메시지 전송이 실패할 경우 중간 노드에서 메시지를 보관 후 통신이 복구되면 메시지를 재전송할 수 있다.

5.2 암호화를 위한 경량화

4절에서 식별한 수중 음파 통신 센서네트워크에 기존의 보안을 적용하기 위해서 고려해야 할 사항 5가지 중 암호화 키 경량화와 암호화 알고리즘 경량화는 수중 음파 통신 센서네트워크의 암호화를 위한 경량화, 노드의 이동성으로 인해 필요한 고려사항은 이동성 보안을 위한 이슈로 종합할 수 있다.

암호화를 위한 경량화에는 크게 수중 서비스 종류에 따른 암호화 키 및 알고리즘의 경량화, 보안 수준 결정, 수중 음파 통신에 적합한 보안 방법 추천에 대한 이슈와 논쟁점이 존재하며 자세한 내용은 다음과 같다.

• 암호화 키 및 알고리즘의 경량화 : 지상 센서네트워크에서 주로 사용되는 Zigbee 통신은 최대 254byte의 패킷 길이를 가진다. 그러나 수중 음파 통신의 최대 패킷 길이는 약 32byte로 지상의 최대 패킷 길이의 약 1/8배에 불과하다. 또한 보안을 위한 패킷은 보안 정보로 인하여 패킷의 길이가 길어지게 되는데, 패킷의 길이가 길어지면 패킷을 분할하여 전송해야 한다. 같은 크기의 메시지를 분할하여 전송해야 한다면 수중 음파 통신 환경에서는 지상에서 메시지를 전송할 때 보다 약 8배 이상을 전송해야한다. 또한 8개의 메시지에 대해 각각 암호화를 해야 하기 때문에 지상과 동일한 암호화 알고리즘을 사용하여 암호화 하는 경우 8배 이상의 시간과 에너지가 소모된다. 따라서 수중 환경에 적합한 암호화 알고리즘과 암호화 키를 경량화 해야 한다.

• 수중 서비스 종류에 따른 보안 수준 결정 : 암호화 수준은 일반적으로 완전할 수 없다. 그 이유는 암호화 및 복호화를 복잡하게 설정할수록 보안 레벨은 굉장히 높아지지만 그만큼 자원도 많이 소모해야하기 때문이다. 따라서 실제적으로 보안을 풀기 위해 얻는 이득이 보안을 풀기 위해 소요되는 비용보다 더 낮은 수준이 되도록 보안 레벨을 설정해야 한다. 특히 수중 환경의 경우 지상 통신에서 사용되는 MCU와 비교하여 메모리 연산 능력이 떨어지고 에너지 소모가 많으며 전파 지연, 통신 속도 등이 느리기 때문에 이를 고려한 보안 수준을 설정하기 위해 더 많은 어려움을 가지고 있다. 따라서 수중 환경에 보안을 적용하기 위해 지상 환경과 다른 수중 환경의 요소들을 고려하여 보안 수준을 결정해야 한다. 이 때, 수중 서비스 종류에 따른 보안 수준을 결정할 때, 서비스의 중요도에 따라 중요한 서비스의 경우 암호화 및 복호화에 시간이 많이 요구되더라도 암호화 수준을 높일 수 있다.

• 수중 음파 통신에 적합한 보안 방법 추천 : 수중 서비스 종류에 따른 보안 수준이 결정되면 그에 따른 암호화 키, 알고리즘, 보안 메시지 길이 등이 복합적으로 결정되어야 한다. 보안 수준을 결정하는 것은 굉장히 많은 요소들을 고려해야 하고 힘든 작업이지만 보안 수준이 결정되고 그에 따른 암호화 키, 알고리즘, 보안 메시지 길이 등을 결정하는 것 또한 굉장히 힘든 작업이 될 수 있다. 따라서 보안 수준이 결정되면 그에 적합한 암호화 키의 길이, 알고리즘의 복잡도, 보안 메시지의 길이 등이 추천될 수 있는 연구도 필요하다. 이를 위해 수중 환경의 응용에서 작용할 수 있는 통신 거리, 응용의 중요도 등의 특성들을 식별하고, 특성들의 점수에 따라 수중 음파 통신에 적합한 보안을 추천할 수 있는 방법이 있다.

5.3 통신을 위한 경량화

통신을 위한 경량화에는 보안 메시지 길이 최소화, 통신 횟수 최소화에 대한 이슈와 논쟁점이 존재하며, 이에 대해 앞으로 더욱 연구되어야 할 부분은 다음과 같이 정리할 수 있다.

• 암호화 키 분배 : 지상 센서네트워크에서 주로

사용되는 Zigbee 통신의 경우 주파수 대역폭은 800 MHz~900MHz, 2.4GHz~2.5GHz 이지만, 수중 음파 통신의 주파수 대역폭은 20~70KHz에 불과하다. 이것은 수중 음파 통신의 채널 대역폭이 지상 센서네트워크에 비해 굉장히 한정적이며, 데이터 대역폭 또한 한정적인 것을 의미한다. 이러한 특징과 전파 지연이 낮아 수중 음파 통신에서의 보안 위협 중 하나인 Reply 공격에 대응하기 위하여 주기적으로 암호화 키를 갱신해야 하는데 수중 음파 통신 채널 주파수 대역폭과 데이터 대역폭, 데이터율이 낮기 때문에 채널 점유율도 함께 증가하는 문제가 발생하게 된다. 따라서 암호화 키 분배가 제대로 되지 않아 암호화 및 복호화를 적시에 할 수 없는 문제가 발생할 수 있다. 이를 위해 수중 환경에서 클러스터 헤드 기반의 토폴로지를 사용하면, 대부분 1홉 이내에서 통신이 가능하기 때문에 한 번에 키 분배를 위한 통신이 성공할 확률이 더 높아지게 되어 암호화 및 복호화를 적시에 할 수 있게 된다.

• 통신 에러율을 고려한 보안 메시지 길이 최소화 : 보안을 위해 평문을 암호화하게 된다면 보안 메시지 길이는 더욱 길어지게 된다. 수중 음파 통신 센서네트워크의 경우 지상 RF 통신에 비해 높은 에러율을 갖기 때문에 한번에 전송할 수 있는 최대 메시지 크기 또한 작을 수밖에 없다. 이때 메시지의 크기를 늘리기 위해서는 보안 레벨을 낮춰야하기 때문에 보안을 위한 요구사항에 적합하지 않게 될 수 있으며, 보안 레벨을 높이기 위해서는 메시지의 크기를 줄여야하기 때문에 통신 횟수 증가로 인한 에너지소모 증가, 채널의 혼잡성 등의 문제가 발생하게 된다. 따라서 이들 간의 트레이드오프 관계를 고려한 적절한 보안 메시지 길이는 어느 정도로 설정해야 하는 연구가 필요하다. 만약 수중 환경에서 음파 통신과 짧은 거리에서의 RF 통신을 함께 사용하고, 보안 레벨이 높아야 하는 메시지의 목적지까지의 RF 통신 경로가 존재한다면 이 메시지를 RF 통신 경로를 통해 전송하면 수중 환경의 제약으로 인한 메시지 길이 최소화 문제를 해결할 수 있다.

• 통신 횟수 최소화 : 통신 횟수 최소화 이슈는 통신 에러율을 고려한 보안 메시지 길이 최소화와 많은 연관이 있다. 보안 레벨을 높이기 위해 메시지의 크기를 줄이게 되면 메시지를 전송하기 위한 통신 횟수가 증가되게 되는데, 이 경우 에너지 소모가 증가하고 통신 채널이 바빠지게 되어 다른 노드들의 통신을 방해할 수 있는 문제가 발생할 수 있다. 결국 통신 횟수 최소화는 통신 에러율을 고려한 보안 메시지 길이 최소화를 함께 고려하여 더욱 심도 있는 연구가 진행되어야 하며, 수중 음파 통신 센서네트워크에 보안을 적용하는데 어려움을 주는 논쟁거리 중 하나이다. 통신 횟수를 최소화할 때 수중 환경에 요구되는 서비스의 보안 레벨과 수중 노드의 수를 고려하여 통신 횟수를 조절할 수 있다.

5.4 이동성 보안을 위한 이슈

마지막으로 노드의 이동성을 위해 필요한 보안에 대한 이슈와 논쟁점은 다음과 같이 정리할 수 있다.

• 노드의 이동성 : 수중 노드는 파도, 해류, 바람 등으로 인해 끊임없이 노드가 이동하게 되지만, 지상 센서네트워크의 경우 일반적으로 지상에 고정되어 설치되기 때문에 이동이 거의 없다. 따라서 수중 노드는 통신 범위를 자주 벗어나게 되어 재라우팅을 빈번하게 수행하거나, 새로운 노드가 나타남으로 인해 네트워크에 가입해야 하는 일들이 빈번한데, 이때마다 보안 인증절차를 거쳐야 해서 보안 인증으로 인한 시간과 에너지가 소모된다. 이를 위해 재라우팅 시 인증과정을 간소화 하여 진행할 수 있는 수중환경에 적합한 보안 인증 프로토콜이 필요할 수 있다. 한 가지 예로, 한 노드가 클러스터에 가입되어 있는 상태에서 노드의 이동으로 클러스터에 재가입 할 경우 클러스터 헤드에 메시지 인증 코드를 전송하면, 상위 노드들은 베이스 스테이션까지 인증 코드를 전송만 하고, 실제 인증은 베이스스테이션에서 진행하는 방법이 있다.

6. 결 론

수중 음파 센서네트워크는 지상의 센서네트워크의 노드와 비교했을 때 매우 낮은 연산 능력, 제한된 메모리 등으로 인하여 기존의 센서네트워크에서 사용되는 보안 프로토콜 및 알고리즘 등을 수중 음파 센서네트워크에 그대로 적용할 수 없다. 또한 수중 환경에서는 음파 통신을 사용하기 때문에 지상에서 사용하는 전파 통신에 비해 훨씬 느린 데이터 전송 속도, 높은 에러율, 제한된 대역폭 등으로 인해 지상 센서네트워크에서 사용되는 보안 프로토콜 역시 그

대로 적용할 수 없었다. 수중 환경에 보안을 적용하기 위해서는 수중 환경에 적합한 보안 알고리즘을 새롭게 개발하거나 기존의 지상에서 사용 중인 보안을 수중 환경에 적합하도록 수정하여 적용하는 등의 방법이 존재할 수 있다.

본 논문에서는 여러 방안 중 수중 환경에 보안을 적용하기 위해 지상에서 사용 중인 보안을 수중 환경에 적합하도록 수정하기 위해 발생하는 문제점과 고려사항들에 대하여 분석하였다. 그 결과 수중 환경은 제한된 메모리, 낮은 전파 지연시간, 느린 처리시간 등의 문제로 암호화 키 경량화, 암호화 알고리즘 경량화, 암호화 메시지 크기 최소화 등의 요구사항이 분석되었다. 뿐만 아니라 수중 환경에 보안을 적용하기 위해 고려해야 할 사항들에 대한 이슈를 함께 다루었다. 최근에는 수중 환경에 보안을 적용하기 위한 연구가 진행되고 있지만, 주로 암호화 키 경량화 혹은 알고리즘에 연구의 초점이 맞추어져 있어 지상 환경의 보안을 수중 환경에 곧바로 적용하기는 어려웠다.

본 논문에서 분석한 지상 환경의 보안을 수중 환경에 적용하기 위한 문제점과 요구사항을 통해 수중 환경에 보안 적용 시 가이드라인을 제공할 뿐만 아니라 수중 환경에 보안을 적용할 때 필요한 이슈와 논쟁점 등을 통해 수중 음파 센서네트워크에 적합한 또 다른 보안 프로토콜과 알고리즘 등을 연구하기 위한 지표가 될 수 있을 것으로 기대된다.

향후 연구로는 본 논문에서 제안한 보안 고려사항을 기반으로 하여 수중 음파 센서 네트워크에 적합한 보안 프로토콜을 제안하도록 한다.

REFERENCE

[1] S.J. Park, S.H. Park, S.K. Kim, and C.H. Kim, “Underwater Communication and Ocean Sensor Network Technology," *Communications of the Korean Institute of Information Scientists and Engineers*, Vol. 28, No. 7, pp. 79-88, 2010.

[2] H.W. Nam, S.S. An, C.H. Kim, S.H. Park, Y.H. Kim, and S.H. Lim, “Remote Monitoring System Based on Ocean Sensor Networks for Offshore Aquaculture,” *Proceeding of IEEE Oceanic Engineering Society*, pp. 14-19, 2014.

[3] D.H. Shin and C.H. Kim, “Sensor Network System for Littoral Sea Cage Culture Monitoring,” *Korea Information Proceesing Society Transaction on Computer and Communication System,* Vol. 5, No. 9, pp. 247-260, 2016.

[4] D.H. Shin and C.H. Kim, “Data Compression Method for Reducing Sensor Data Loss and Error in Wireless Sensor Network,” *Journal of Korea Multimedia Society,* Vol. 19, No. 2, pp. 360-374, 2016.

[5] R. Martin and S. Rajasekaran, “Data Centric Approach to Analyzing Security Threats in Underwater Sensor Networks,” *Proceeding of OCEANS 2016 Marine Technology Society/ IEEE Monterey*, pp. 1-5, 2016.

[6] G. Han, J. Jiang, N. Sun, and L. Shu, “Secure Communication for Underwater Acoustic Sensor Networks,” *IEEE Communication Magazine*, Vol. 53, No. 8, pp. 54-60, 2015.

[7] E. Michael, Whitman and J. Herbert Mattord, *Principles of Information Security*, CENGAGE Learning, U.K., 2017.

[8] H.J. Seo and H.W. Kim, “On Dynamic Voltage Scale Based Protocol Low Power Underwater Secure Communications on Sensor Network,” *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 18, No. 3, pp. 586-594, 2014.

[9] H. Li, Y. He, X. Cheng, H. Zhu, and L. Sun, “Security and Privacy in Localization for Underwater Sensor Networks,” *IEEE Communications Magazine*, Vol. 53, No. 11, pp. 56-62, 2015.

[10] S.J. Lee, D.H. Shin, and C.H. Kim, “Improvement of Verified Neighbor Discovery Protocol Based on Directional Antenna to Detect Wormhole in Underwater Acoustic Sensor Networks,” *Proceeding of the 2017 World Congress on Information Technology Applications and Services*, pp. 1-8, 2017.

[11] M.H. Park, Y. Kim, and O.Y. Yi, “Light Weight Authentication and Key Establishment Protocol for Underwater Acoustic Sensor Networks,”

Journal of the Korea Institute of Information and Communication Engineering B, Vol. 39, No. 6, pp. 360-369, 2014.

[12] A.H. Moon, U. Iqbal, and G.M. Bhat, "Light Weight Authentication Framework for WSN," *Proceeding of International Conference on Electrical, Electronics, and Optimization Techniques*, pp. 3099-2105, 2016.

[13] C.W. Yun, J.H. Lee, O.Y. Yi, S.Y. Shin, and S.H. Park, "Analysis of the Cryptographic Algorithms's Performance on Various Devices Suitable for Underwater Communications", *Korea Information Proceesing Society Transaction on Computer and Communications System*, Vol. 5, No. 3, pp. 71-78, 2016.

신 동 현

2014년 강릉원주대학교 컴퓨터공학 공학사
2014년~2016년 강릉원주대학교 컴퓨터공학 공학석사
2016년~현재 강릉원주대학교 컴퓨터공학 박사과정

관심분야 : Underwater Communication, IoT/IoUT, WSN (Wireless Sensor Network), Data Mining

이 승 준

2017년 강릉원주대학교 컴퓨터공학 공학사
관심분야 : WSN (Wireless Sensor Network), Underwater Security,

김 창 화

1985년 고려대학교 수학교육과 이학사
1987년 고려대학교 전산학전공 이학석사
1990년 고려대학교 전산학전공 이학박사
1994년~1995년 University of Toronto, Enterprise Integration Lab. Post-Doc. & Visiting Professor
2002년~2004년 미국 Texas A&M대학 Visiting Scholar
1989년~현재 강릉원주대학교 컴퓨터공학과 교수
2005년~현재 강릉원주대학교 해양센서네트워크시스템 기술연구센터 센터장
관심분야 : Underwater Communication and Sensor Network, IoT/IoUT, Distributed System, Intelligent System