http://dx.doi.org/10.7840/kics.2014.39B.6.360

수중 음파 센서 네트워크 환경에 적합한 경량화된 인증 및 키 발급 프로토콜

박 민 하◆, 김 역*, 이 옥 연°

Light Weight Authentication and Key Establishment Protocol for Underwater Acoustic Sensor Networks

Minha Park◆, Yeog Kim*, Okyoen Yi°

요 약

수중 음파 센서 네트워크를 이용하여 수중 환경의 자료를 수집하고 이를 이용하여 오염도를 측정하거나 자연 재해를 예방하는 등의 연구가 진행되고 있다. 수중에서 수집된 자료는 음파 통신으로 지상의 통신 개체로 전달된다. 수중 환경은 지상 환경에 비해 전송 속도가 낮고, 전송 지연이 빈번히 일어나는 등 통신 성능이 좋지 않기 때문에 지상의 무선 통신에서 사용되는 보안 기술을 그대로 적용시키는 것이 어렵다. 이로 인해 보안 기술을 배제한 체 통신 기술만 사용할 경우 전송되는 자료가 공격자에 의해 탈취되거나 위·변조 되는 등의 보안 위협에 노출될 수 있다. 그렇기 때문에 개체 간의 신뢰성을 입증해 주고, 암호화 통신을 위한 비밀키를 공유하는 인증 및 키 발급 프로토콜 등과 같은 보안 기술이 요구된다. 따라서 본 논문에서는 수중 환경을 위해 경량화한 인증 및 키 발급 프로토콜인 UW-AKE을 제안한다.

Key Words : Underwater Acoustic Sensor Networks, Authentication, Secret Key, Key Establishment, Light-weight

ABSTRACT

Underwater Acoustic Sensor Networks(UASN) enables varied study from collected data of underwater environments such as pollution monitoring, disaster prevention. The collected data is transmitted from underwater to terrestrial communication entity by acoustic communication. Because of the constraints of underwater environments include low data rate and propagation delay, it is difficult to apply cryptographic techniques of terrestrial wireless communication to UASN. For this reason, if the cryptographic techniques are excluded, then collected data will be exposed to security threats, such as extortion and forgery, during transmission of data. So, the cryptographic techniques, such as the authentication and key establishment protocol which can confirm reliability of communication entities and help them share secret key for encryption of data, must need for protecting transmitted data against security threats. Thus, in this paper, we propose the light weight authentication and key establishment protocol.

※ 본 연구는 해양수산부의 지원으로 수행하고 있는 "수중 광역 이동통신 시스템 개발" 사업 결과의 일부임을 밝히며 지원에 감사드립니다.

◆ First Author : Dept. of Financial Information Security, Graduate School, Kookmin University, mhpark@kookmin.ac.kr, 정회원
° Corresponding Author : Dept. of Mathematics, Kookmin University, oyyi@kookmin.ac.kr, 정회원
* Cryptography & Information Security Institute, Kookmin University, yeogkim@gmail.com
논문번호 : KICS2014-05-001, Received May 15, 2014; Revised June 3, 2014; Accepted June 3, 2014

Ⅰ. 서 론

수중 환경에서 수온, 수압, 염분, 해류 등의 자료를 수집하고 이를 이용하여 자연 상태를 파악하여 오염도를 측정하거나 자연 재해를 예방하는 것이 중요해지고 있다. 현재 수중 환경에서 자료를 수집하는 통신 기술로 수중 음파 센서 네트워크가 있다[1,8]. 수중 음파 센서 네트워크는 다수의 센서들이 수중에 배치되어 주변 자료들을 수집하여 상위 개체로 전달하도록 구성된다. 수중 환경은 지상 환경과 달리 물을 매질로 사용하기 때문에 음파 통신을 한다. 따라서 통신 속도가 약 1.5km/s로 지상의 무선 통신 속도인 약 3×10^5km/s 보다 20만 배 낮으며, 사용 가능한 주파수 대역도 10~50kHz로 지상의 무선 통신에 사용되는 주파수 대역인 300MHz ~30GHz에 비해 좁다. 또한, 수중 음파 통신의 경우 대역폭이 약 5kHz로 20MHz 대역을 사용하는 지상의 무선 통신보다 좁다[13]. 뿐만 아니라 다중 경로 전파도 빈번히 일어나 데이터 전송 시 지연과 충돌 및 간섭 등이 빈번히 일어나 지상의 전파 통신보다 통신 성능이 좋지 않다. 또한 수중에 배치된 센서들은 배터리로 전원을 공급받기 때문에 전력 사용이 제한적인 단점이 있다. 따라서 지상의 무선 통신에서 사용되는 보안 기술을 그대로 적용하는 것은 거의 불가능하다. 이로 인해 수중 음파 센서 네트워크에서 보안 기능을 배제한 체 통신 기술만 사용하게 되면 센서들이 수집한 자료를 상위개체로 전달하는 과정에서 공격자에 의해 탈취되어간 위・변조 되는 등의 보안 위협에 노출될 수 있다. 따라서 수집된 자료를 공격의 위협으로부터 안전하게 보호하기 위해 통신 개체 간의 신뢰성을 입증하는 인증 프로토콜과 암호화 통신에 사용되는 비밀키를 공유하는 키 발급 프로토콜이 필요하다. 이 과정을 통해 상호 신뢰성이 입증되면 상위 개체에서 정당한 센서가 보낸 자료는 수용하고, 인증되지 않은 센서가 보낸 자료는 무시할 수 있다. 또한 개체 간에 공유된 비밀키를 이용하여 자료를 암호화하여 전송함으로써 비밀키를 소유하고 있지 않은 공격자로부터 보호할 수 있다. 센서들이 자료를 수집한 뒤 자료를 비밀키로 암호화하여 지상의 통신 개체에게 전송하면 공격자는 암호화된 자료로부터 자료의 내용을 확인할 수 없기 때문에 탈취 및 위・변조의 위협으로부터 자료를 보호할 수 있다. 또한 비밀키로 자료의 MAC(Message Authentication code) 값을 계산하여 함께 전송함으로써 자료의 손상 여부를 확인할 수 있기 때문에 인증 및 키 발급 프로토콜이 반드시 필요하다.

현재 지상의 무선 센서 네트워크를 위한 인증 및 키 발급 프로토콜은 다양하게 존재한다[8-11]. 무선 센서 네트워크에서 사용되는 대표적인 인증 프로토콜로 ZigBee Alliance에서 제공하는 프로토콜이 있다[8]. 이 프로토콜은 모든 이웃 개체와 인증을 수행하기 때문에 인증 횟수가 많다. Ibriq의 인증 기법[10]은 중간 노드가 다수의 센서들의 인증 정보를 모두 저장하고 전송해야하기 때문에 처리할 데이터양이 많다. Kyusuk의 인증 기법[11]은 위의 프로토콜들과는 달리 재 인증 과정을 통해 인증이 간소화될 수 있도록 설계하였다. 이 과정은 중간 노드가 이웃의 중간 노드들의 정보를 알고 있어야하며, 이들 간의 통신이 빈번히 발생할 수 있다. 이 인증 기법들은 지상의 무선 통신을 위해 설계된 것으로 전송 속도가 낮고, 지연이 빈번히 일어나는 등의 수중 환경의 제한사항들을 고려하지 않아 그대로 적용시키기에는 어려움이 있다. 따라서 수중 음파 센서 네트워크에서 사용되는 보안 프로토콜의 경우 지상 환경에서 사용되는 보안 프로토콜과 달리 전송 속도나 지연 발생 가능성 등과 같은 제한사항을 고려함으로써 경량화되어야 하며 열악한 환경에서도 제대로 동작하기 위한 효율적인 설계가 필요하다.

본 논문에서는 열악한 수중 환경을 고려하여 인증 메시지 크기와 메시지 전송 횟수를 감소시켜 경량화함으로써 수중 음파 센서 네트워크의 MAC 계층에서 실행 가능한 인증 및 키 발급 프로토콜인 UW-AKE(Underwater Authentication and Key Establishment protocol)를 제안한다. 또한 수중 환경의 특징인 해류나 어류들로 인해 센서들이 예기치 못하게 이동하여 네트워크 토폴로지가 변하는 경우를 고려한 센서 이동 시 인증 프로토콜도 함께 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 소개하고, 3장에서는 제안하는 인증 및 키 발급 프로토콜에 대해 기술한다. 4장에서는 제안하는 프로토콜과 기존의 연구들의 보안 위협 대응 방안 및 경량화 정도를 비교한 뒤 5장에서 결론을 내린다.

Ⅱ. 관련 연구

2.1 수중 음파 센서 네트워크

수중 음파 센서 네트워크는 Cluster-head 기반 토폴로지 또는 Ad-hoc 기반의 토폴로지로 구성한다[6].

Cluster-head 기반의 토폴로지는 하나의 Cluster-head와 다수의 Sensor들이 Cluster를 형성하여 통신하는 네트워크 토폴로지로 Sensor들이 수집한 데이터를 Cluster-head가 모두 취합하여 상위 개체에게 전달

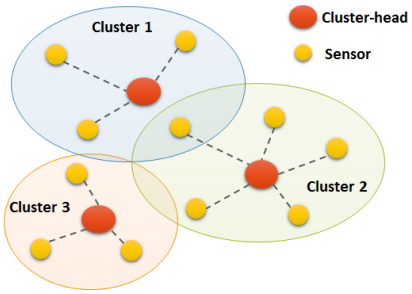

그림 1. Cluster-head 기반 토폴로지
Fig. 1. Cluster-head based network topology

한다. 이는 Sensor마다 데이터 전송 가능 시간을 분배하여 다중경로 전송으로 인한 패킷 충돌을 방지한다. 그렇기 때문에 실시간으로 데이터를 전송하는 것은 제공하지 않으며, 만약 Cluster-head에게 문제가 발생할 경우 해당 Cluster 내의 네트워크 성능이 저하되는 단점이 있다.

Ad-hoc 기반의 토폴로지는 Sensor들 간에 multi-hop 통신으로 데이터를 주고받는 네트워크 위상으로 Sensor들이 수집한 데이터를 실시간으로 전송한다. 이는 multi-hop 통신을 위해 많은 수의 Sensor들이 필요하며, Ad-hoc 통신이 가능하도록 일정 간격 내에 이웃 Sensor들이 존재해야한다. 무엇보다 Sensor들이 데이터를 실시간으로 전송하기 때문에 다중경로

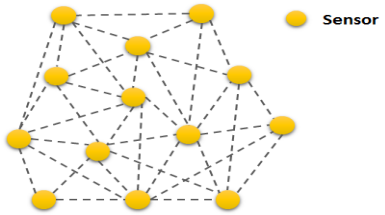

Fig. 2. Ad-hoc based network topology
그림 2. Ad-hoc 기반 토폴로지

표 1. 네트워크 비교
Table 1. Comparison of two networks

	Cluster-head based	Ad-hoc based
Entities	- Sensor node - Cluster-head	- Sensor node
Merits	- Nodes are distributed in time intervals - To avoid packet collision	- Be suitable for real-time data transmission
Demerits	- Difficult real-time data transmission - The problem of cluster head causes network performance	- Packet collision

전송으로 인한 패킷 충돌이나 간섭은 방지할 수 없는 단점이 있다.

2.2 수중 환경

수중 환경은 지상 환경과 달리 물을 매질로 사용하기 때문에 음파 통신을 사용한다. 이로 인해 수중 환경은 데이터 전송 속도가 약 1.5km/s로 지상의 무선 통신 속도인 약 3×105km/s 보다 20만 배 낮다. 또한 사용 가능한 주파수 대역도 10~50kHz로 지상의 무선 통신에 사용되는 주파수 대역인 300 MHz ~ 30GHz에 비해 좁고, 주로 사용되는 수중 모뎀의 경우 약 5 kHz의 대역폭을 가지고 있어 지상의 대표적인 무선 통신인 LTE의 최대 대역폭인 20MHz 대역보다 굉장히 좁다[13].

뿐만 아니라 데이터가 전달 될 때 해면과 복잡한 수직 음속 구조의 영향을 받아 다중 경로 전파가 빈번히 발생기 때문에 수중 환경에서는 데이터 전송 시 지연이 빈번히 발생하며, 간섭 혹은 충돌 등으로 인해 통신 성능이 좋지 않다. 그렇기 때문에 본 논문에서는 인증 메시지 크기와 메시지 전송 횟수를 최소화하여 낮은 전송 속도와 빈번히 발생하는 통신 지연의 영향을 적게 받는 인증 및 키 발급 프로토콜을 제안한다.

표 2. 네트워크 환경 비교
Table 2. Comparison of two networks environments

	Underwater environment	Terrestrial environment
Communication method	Acoustic	RF (Radio Frequency)
Data rate (about)	1.5km/s	3 × 10^5 km/s
Frequency range	10 ~ 50kHz	300MHz ~ 30GHz
Bandwidth (about)	5kHz	1.4~20MHz (LTE)
remark	Multipath propagation	-

Ⅲ. 수중 환경을 위해 경량화한 인증 및 키 발급 프로토콜(UW-AKE)

3.1 고려 사항

3.1.1 네트워크 토폴로지

본 논문에서는 데이터 전송 시 발생하는 패킷 충돌, 간섭 등을 방지하여 통신의 효율성을 높이는 것에 초점을 맞춘 Cluster-head 기반의 토폴로지로 네트워크 환경을 선택하여 그림 3과 같이 구성하였다.

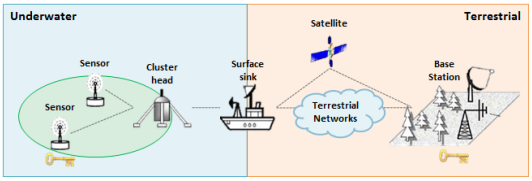

그림 3. 수중 음파 센서 네트워크 환경
Fig. 3. Underwater Acoustic Sensor Network Environments

네트워크 구성 개체로는 Sensor node, Cluster head, Surface station, Base station이 있다. Sensor node는 수중에 배치되어 직접 데이터를 수집하는 개체로 수집한 데이터를 저장하고 있다가 주기적으로 Cluster head에게 전송한다. Cluster head는 각 Cluster 내의 Sensor node들을 관리하는 개체로 Sensor node들로부터 수신한 정보들을 취합하여 Surface station에게 전달한다. 이때, 각 Cluster는 다수의 Sensor node들로 형성된다. Surface station은 해수면 위에 존재하는 네트워크 개체로서 Cluster head로부터 전달받은 데이터를 지상에 있는 Base station까지 전달한다. Base station은 네트워크 개체를 모두 관리하면서 Sensor node들이 수집한 데이터를 모으는 최종 개체로 관제 센터 등이 Base station에 포함된다.

Sensor node와 Cluster head, Surface station는 수중 음파 통신을 이용하여 데이터를 주고받으며 Surface station과 Base station은 지상의 무선 통신을 이용하여 데이터를 주고받게 된다. 이때 사용되는 지상의 무선 네트워크 망으로 이동통신 망, 와이파이 망, 위성통신 망 등이 있으며 본 논문에서는 지상의 무선 네트워크 망은 가정하지 않는다.

이렇게 구성된 수중 음파 센서 네트워크는 먼저 인증 프로토콜을 통해 각 개체 간의 상호 인증을 수행하여 정당성을 입증한다. 인증이 성공한 후에 전송되는 데이터를 보호하기 위해 Sensor node는 수집한 데이터를 암호화하여 Cluster head와 Surface station을 통해 Base station에게 전송한다. 데이터를 수신한 Base station은 해당 Sensor node와 공유한 비밀키인 세션키를 이용하여 데이터를 복호화하여 해당 데이터를 수집하게 된다. 위와 같은 과정으로 Sensor node와 Base station 사이에 데이터가 전송될 때 데이터를 보호한다.

3.1.2 기호 정리

제안하는 프로토콜에서 사용되는 기호들과 인증에 사용되는 각 파라미터들의 크기를 표 3에서 정리한다.

인증키는 인증 과정에서 사용되는 비밀키이고 세션키는 인증이 완료된 후 암호화에 사용되는 비밀키로 각 16바이트로 설정함으로써 128비트 이상의 보안 강도를 갖는다. 또한, 중복되지 않는 난수인 nonce 값을 사용함으로써 재전송 공격을 방지하고, 이 nonce 값과 인증키를 통해 계산된 MAC 값으로 Base station과 각 통신 개체들 간의 인증이 이루어진다. 이때 nonce 값은 8바이트로 설정하고 MAC 값은 4바이트로 설정함으로써 인증 메시지의 크기를 줄였다.

표 3. 기호 정리
Table 3. Notation

Symbol	Description	Size	note
N	Identity of Sensor Node(Sensor)	1byte	N/A
C	Identity of Cluster Head(CH)	1byte	N/A
S	Identity of Surface Station(Surf)	1byte	N/A
B	Identity of Base Station(BS)	1byte	N/A
K_{NB}	Authentication key shared with Sensor and BS	16bytes	more than 128-bit security strength
K_{CB}	Authentication key shared with CH and BS	16bytes	
K_{SB}	Authentication key shared with Surf and BS	16bytes	
SK	Shared session key between Sensor and BS	16bytes	
$nonce$	Random number used only once	8bytes	prevent replay attack
MAC	Message Authentication Code for entity authentication	4bytes	N/A

3.2 UW-AKE

본 절에서는 제안하는 인증 및 키 발급 프로토콜인 UW-AKE에 대해 기술한다. 제안 기법은 두 가지 과정으로 구분된다. 첫 번째 과정은 최초 인증 프로토콜로서, 네트워크가 최초로 형성되었거나 새로운 Sensor node가 새로 네트워크에 추가된 경우 진행되는 과정이다. 두 번째 과정은 이미 BS와 인증 된 Sensor node가 이동하여 다른 Cluster head와 통신할 경우 진행되는 인증 프로토콜이다. 이 과정은 Sensor node가 해류로 인해 이동하거나 혹은 네트워크의 재배치가 될 경우 진행되는 과정으로, 최초 인증 프로토콜을 사용하는 것 보다 효율적으로 인증이 진행되기 위해 제안한다. 만약 이 과정이 원활하게 이루어지지 않을 경우 최초 인증 프로토콜 과정을 통해 인증을 수행한다.

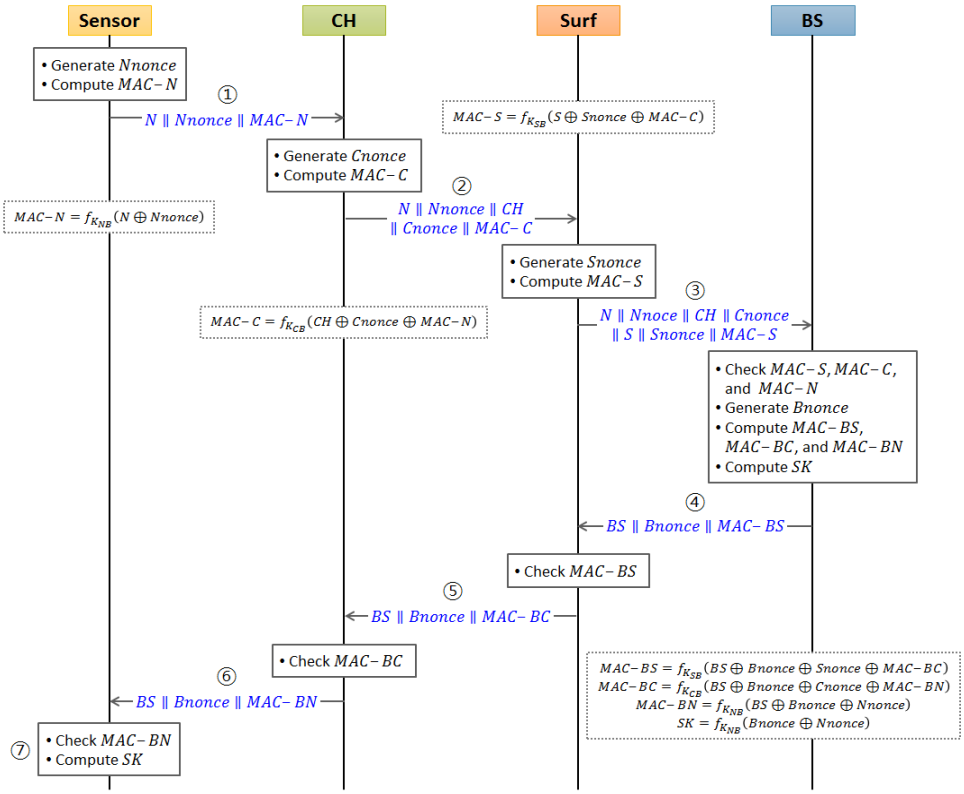

Fig. 4. Initial authentication and key establish protocol
그림 4. 최초 인증 및 키 발급 프로토콜

3.2.1 최초 인증 프로토콜

최초 인증 프로토콜은 네트워크가 처음 형성 되었을 경우 Sensor node와 Cluster head, Surface station이 Base station과 인증하는 과정으로 각 개체들과 Base station 간에 사전에 미리 나눠가진 인증키를 사용하여 [그림 4]의 과정으로 진행된다.

① 먼저 Sensor가 난수 $Nnonce$를 생성 후 BS와 사전에 공유한 인증키(K_{NB})와 자신의 ID인 N 값을 이용하여 BS가 Sensor를 인증할 수 있는 메시지 인증 코드 값인 $MAC-N$을 계산한다.

$$MAC-N = f_{K_{NB}}(N \oplus Nnonce) \quad (1)$$

Sensor는 자신의 신원 정보인 N과 $Nnonce$, $MAC-N$ 값을 CH에게 전송하여 최초 인증 프로토콜을 시작한다.

② CH는 자신의 난수 $Cnonce$를 생성한 후 자신의 신원 정보인 CH 값과 Sensor로부터 전송받은 $MAC-N$ 값을 BS와 사전에 공유한 인증키(K_{CB})를 이용하여 BS가 CH를 인증할 수 있는 $MAC-C$를 계산한다.

$$MAC-C = f_{K_{CB}}(CH \oplus Cnonce \oplus MAC-N) \quad (2)$$

이후 CH는 Sensor에게 받은 N, $Nnonce$와 함께 CH, $Cnonce$, $MAC-C$를 CH에게 전송한다.

③ Surf는 메시지 수신 후 자신의 난수 $Snonce$를 생성한 후 자신의 ID인 S 값과 CH로부터 전송받은 $MAC-C$ 값을 BS와 사전에 공유한 인증키(K_{SB})를 이용하여 BS가 Surf를 인증할 수 있는 $MAC-S$를 계산한다.

$$MAC-S = f_{K_{SB}}(S \oplus Snonce \oplus MAC-C) \quad (3)$$

그 다음 Surf는 N, $Nnonce$, CH, $Cnonce$와 함께 S, $Snonce$, $MAC-S$를 BS에게 전송한다.

④ 인증 메시지를 받은 BS는 $MAC-N$, $MAC-C$, $MAC-S$를 계산한 뒤 수신한 값들과 비교하여 Sensor, CH, Surf를 인증한다. 만약 값이 맞지 않을 경우 인증 실패로 해당 개체의 신원 정보와 함

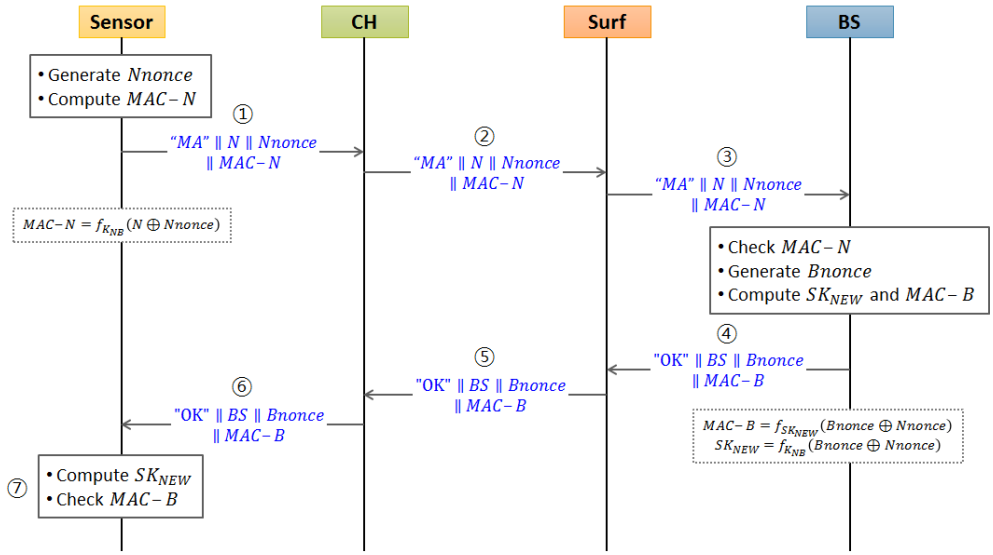

Fig. 5. Authentication protocol for moved sensor node
그림 5. Sensor node 이동 시 인증 프로토콜

께 실패 메시지를 다른 개체들에게 전송한다. 인증값이 모두 일치하면 BS는 난수 $Bnonce$를 생성한 후 각 개체들이 BS를 인증할 수 있는 값인 $MAC-BS$, $MAC-BC$, $MAC-BN$과 실제 암·복호화 통신을 하는 Sensor와 공유할 세션 키(SK)를 계산한다. 이때, $MAC-BN$은 $MAC-BC$ 계산에, $MAC-BC$는 $MAC-BS$ 계산에 사용되어 BS가 MAC 값 하나만 전달하도록 한다.

$$MAC-BS = f_{K_{SB}}(BS \oplus Bnonce \oplus Snonce \oplus MAC-BC) \quad (4)$$

$$MAC-BC = f_{K_{CB}}(BS \oplus Bnonce \oplus Chonce \oplus MAC-BN) \quad (5)$$

$$MAC-BN = f_{K_{NB}}(BS \oplus Bnonce \oplus Nnonce) \quad (6)$$

$$SK = f_{K_{NB}}(Bnonce \oplus Nnonce) \quad (7)$$

이후 BS는 BS, $Bnonce$, $MAC-BS$를 연접하여 Surf에게 전송한다.

⑤ 인증 응답 메시지를 받은 Surf은 $MAC-BS$를 계산한 뒤 수신한 값과 비교함으로써 BS를 인증한다. 값이 일치할 경우 인증 성공으로 $MAC-BC$를 추출하여 CH에게 BS, $Bnonce$, $MAC-BC$를 전송한다.

⑥ CH는 $MAC-BC$를 계산한 후 수신한 값과 비교하여 BS를 인증한다. 값이 일치할 경우 인증 성공으로 $MAC-BN$을 추출하여 Sensor에게 BS, $Bnonce$, $MAC-BN$을 전송한다.

⑦ Sensor는 $MAC-BN$을 계산한 후 수신한 값과 비교하여 BS를 인증한다. 값이 일치할 경우 인증 성공으로 BS와 암·복호화 통신을 위한 세션 키(SK)를 계산한다.

3.2.2 Sensor node 이동 시 인증 프로토콜

이미 Base station과 인증된 Sensor node가 해류 등으로 인해 이동하여 새로운 Cluster head에 접속 할 경우에도 새롭게 인증이 진행되어야 한다. 수중 환경에서는 Sensor node의 이동이 빈번히 일어날 수 있기 때문에 최초 인증 프로토콜 과정 그대로 진행하는 것보다 더 간단한 방법으로 인증하는 것이 좋다. 따라서 본 논문에서는 Sensor node 이동 시 인증 프로토콜도 함께 제안함으로써 이전에 Base station과 인증된 Sensor node가 이동하여 새로운 Cluster head에 접속할 경우 최초 인증 프로토콜보다는 간단하게 인증할 수 있도록 한다.

① Sensor는 새로운 CH에게 접속하면 $Nnonce$를 생성한 뒤 $MAC-N$을 계산하여 인증을 시작한다.

$$MAC-N = f_{K_{NB}}(N \oplus Nnonce) \quad (8)$$

"MA(Movement Authentication)"메시지와 함께

N, $Nnonce$, $MAC-N$을 CH에게 전송한다.

② CH는 수신한 메시지를 그대로 Surf에게 전송한다.

③ Surf는 수신한 메시지를 그대로 BS에게 전송한다.

④ 인증 메시지를 받은 BS는 $MAC-N$을 계산하여 수신한 값과 비교함으로써 Sensor를 인증한다. 값이 일치하면 인증 성공으로 새로운 난수$Bnonce$를 생성한 뒤 새로운 세션키(SK_{NEW})와 $MAC-B$를 계산한다. $MAC-B$는 Sensor가 BS를 인증하기 위한 값이다.

$$SK_{\neq W} = f_{K_{NB}}(Bnonce \oplus Nnonce) \quad (9)$$

$$MAC-N = f_{SK_{\neq W}}(N \oplus Nnonce) \quad (10)$$

그 다음 BS는 "OK"메시지와 함께 BS, $Bnonce$, $MAC-B$를 Surf에게 전송한다.

⑤ Surf는 수신한 메시지를 CH에게 전송한다.

⑥ CH는 수신한 메시지를 Sensor에게 전송한다.

⑦ Sensor는 먼저 새로운 세션키(SK_{NEW})를 계산한 뒤 $MAC-B$를 계산하여 수신한 값과 비교함으로써 BS를 인증한다.

위의 과정은 최초 인증 프로토콜과는 달리 Cluster head와 Surface station은 메시지를 전달만 할 뿐 실제 인증 과정에는 참여하지 않기 때문에 좀 더 빠르고 간단하게 수행된다.

Ⅳ. 제안된 프로토콜 분석

4.1 보안 공격에 대한 대응 방안

본 절에서는 인증 프로토콜에 대한 보안 위협을 살펴보고, 각 보안 위협에 대한 제안한 인증 및 키 발급 프로토콜의 대응 방법에 대해 서술한다. 먼저 인증 프로토콜에 대한 공격 위협과 이에 대응할 수 있는 기법은 다음과 같다[12].

- 재전송 공격 : 과거에 전송된 하나의 메시지를 저장하였다가 이후에 재전송하여 정당한 사용자로 가장하는 공격으로, 이 공격은 반복되지 않는 난수인 nonce 값을 사용하거나 메시지에 신원 정보를 포함시켜 전송하는 등의 방법으로 방지할 수 있다.
- 중재자 공격 : 통신 개체 사이에서 전달되는 메시지를 모두 수집하여 관찰하는 공격으로, 이를 통해 재전송 공격을 시도할 수 있다. 이 공격은 프로토콜의 메시지에 chained nonce를 사용함으로써 방지할 수 있다.
- 반사 공격 : 송신자가 생성한 메시지를 가로챈 후 이를 이용하여 응답 메시지를 얻은 후 다시 송신자에게 재전송하여 접근 권한을 얻는 공격으로, 이 공격은 응답 메시지에 신원 정보를 포함시켜 전송하거나 메시지 형태를 매번 다르게 구성함으로써 방지할 수 있다.
- 선택 메시지 공격 : 시도-응답 프로토콜에 해당하는 공격으로 어떠한 정보를 얻기 위해 시도 메시지를 가공하여 전송하는 공격으로, 이 공격은 각 개체에서 생성한 난수를 사용함으로써 방지할 수 있다.

본 논문에서는 제안한 인증 및 키 일치 프로토콜 설계 시 보안 공격에 모두 대응하기 위해 각 공격에 대한 대응 방안을 모두 고려했다. 제안한 프로토콜은 각 개체에서 인증 메시지를 전송할 때 자신의 nonce 값을 생성하여 인증 값과 함께 전송함으로써 재전송 공격과 선택 메시지 공격에 대응한다. 그리고 인증 메시지를 전달 받은 Cluster head와 Surface station은 수신한 MAC 값과 자신이 생성한 nonce 값을 이용하여 새로운 MAC 값을 만들어 상위 개체에게 전송함으로써 nonce 값과 MAC 값이 연결될 수 있도록 하여 중재자 공격에 대응한다. 게다가 전송되는 메시지에 각 개체들의 신원 정보를 포함하기 때문에 재전송 공격과 반사 공격에 대응한다. 이와 같이 제안한 프로토콜은 4가지 공격 유형을 모두 고려하여 설계된 것을 확인할 수 있다.

현재 수중 음파 센서 네트워크와 유사한 지상의 무선 센서 네트워크를 위한 인증 프로토콜에 대한 연구가 존재한다[8-11]. 각 프로토콜들은 4가지 보안 공격에 어떤 방법으로 대응하였는지 표 4에서 제안한 프로토콜과 비교하였다. Ibriq[10]와 Kyusuk[11]의 프로토콜은 제안 프로토콜과 유사한 방법으로 대응하였으며, ZigBee[8]와 Abraham의 프로토콜[9]은 중재자 공격과 반사 공격에는 대응하지 못했다.

4.2 경량화 분석

본 절에서는 제안한 프로토콜과 기존의 프로토콜들[8-11]이 사용되는 네트워크 환경과 인증에 참여하는 개체, 인증 시 전송되는 메시지 크기 비교를 통해 제안 프로토콜의 성능에 대해 서술한다. 표 4는 각 프로토콜의 적용 환경과 인증 시 전송되는 메시지 크기를 비교한 자료이다. 표 5를 통해 제안한 프로토콜이 기존의 프로토콜보다 경량화 되었음을 확인할 수 있다.

수중 환경을 위해 제안된 프로토콜과 함께 지상의 무선 센서 네트워크를 위한 기존 연구들은 각각 Cluster-head 기반 네트워크 토폴로지 또는 Ad-hoc

표 4. 공격 대응 방법 비교
Table 4. The comparison of counter-measure

Attacks	proposed protocol		existing authentication protocol for wireless sensor network							
	UW-AKE		Abraham's [9]		Ibriq's [10]		Kyusuk's [11]		ZigBee [8]	
	O/X	counter-measure	O/X	counter-measure	O/X	counter-measure	O/X	counter-measure	O/X	counter-measure
• Replay Attack	O	use of nonce and identity	O	use of random number	O	use of random number and identity	O	use of nonce and identity	O	use of random number
• Interleaving Attack	O	use of chained nonce(MAC)	X	-	O	use of chained nonce(MAC)	O	use of chained nonce(MAC)	X	-
• Reflection Attack	O	use of identity	X	-	O	use of identity	O	use of identity	X	-
• Chosen-Text Attack	O	use of nonce	O	use of random number	O	use of random number	O	use of nonce	O	use of random number

표 5. 각 프로토콜의 네트워크 환경 및 전송 데이터 크기
Table 5. The network environments and message size of protocols

List	proposed protocol		existing authentication protocol for wireless sensor network			
	UW-AKE		Abraham's [9]	Ibriq's [10]	Kyusuk's [11]	ZigBee [8]
• Network topology	Cluster-head based network topology		Cluster-head based network topology	Cluster-head based network topology	Cluster-head based network topology	Ad-hoc based network topology
• Authentication entities	- Sensor node - Cluster head - Surface sink - Base station		- Node - Cluster head - Intermediate CH - Base station	- Node u - Node v - Cluster head - Base station	- Sensor node - sink 1 - sink 2 - Base station	- Sensor
• Transmitted message size (min ~ max)	UW	TE	46 ~ 70	54 ~ 71	9 ~ 42	8 ~ 10
	13~22	13~31				
• Total message size for one sensor authentication	UW	TE	324	341	167	36
	61	44				
	total : 105					

※ Message size : byte ※ min : minimum ※ max : maximum

기반 네트워크 토폴로지에서의 인증 프로토콜을 설계하였다. 각각 설정된 네트워크 토폴로지에 따라 각 인증 프로토콜에 참여하는 개체도 설정되어 동일한 네트워크 토폴로지일 경우 인증 개체가 유사하다.

인증 시 전송되는 메시지 크기는 각 연구에서 제시하고 있는 데이터 크기와 본 논문에서 제시하고 있는 데이터의 크기로 계산하여 전송되는 메시지의 최소값과 최대값, 전체 메시지의 크기를 비교하였다. 그 결과 센서 하나를 인증하는데 사용되는 메시지 크기를 보면 Ibriq의 프로토콜[10]에서 사용되는 인증 메시지가 가장 크고, ZigBee의 인증 프로토콜[8]에서 사용되는 메시지가 가장 작다. 제안한 프로토콜은 최소 21바이트에서 최대 55바이트까지 전송이 되며 전체 인증 수행 시 189바이트의 메시지가 전송된다. 제안 프로토콜의 경우 수중 음파 통신을 하는 구간과 지상의 무선 통신을 이용하는 구간이 구분되기 때문에 수중 음파 통신을 하는 구간에서는 최소 13바이트에서 최대 22바이트 크기로 전송되며 지상의 통신 구간에서는 최소 13바이트에서 최대 31바이트 크기로 전송되어 전체 인증 수행 시 105바이트의 메시지가 전송된다.

Abraham의 프로토콜[9]은 센서들 간의 그룹 통신을 위한 그룹 키 분배를 고려하여 설계하였으며, Ibriq의 프로토콜[10]은 Cluster head가 다수의 Node들의 인증 메시지와 키 정보를 테이블에 저장하였다가 한꺼번에 Base station에게 인증을 요청하여 인증을 진행하기 때문에 Cluster head와 Base station 간에 큰 메시지를 전송하게 된다. 이를 수중 환경에서 사용하면 Cluster head와 Base station이 통신하는 구간에서 음파 통신 시 전송 지연, 패킷 충돌 등의 문제가 발생하여 인증 메시지가 제대로 전송되지 않을 수 있기 때문에 수중 환경에 적용하는 것에 어려움이 있다. Kyusuk의 프로토콜[11]은 재 인증 과정을 통해 인증이 간소화되도록

설계하였는데, 이 과정은 Sink가 이웃 Sink들의 정보를 알고 있어야하며 이들 간의 통신이 빈번히 발생할 수 있다. 그렇기 때문에 이 프로토콜을 수중환경에 적용할 경우 데이터 전송에 대한 제한 사항을 극복할 수 없다. ZigBee[8]는 Ad-hoc 기반의 네트워크 토폴로지를 위한 것으로 하나의 센서가 주변의 센서들과 모두 인증을 해야 하기 때문에 이웃 센서들의 수가 증가할수록 전송되는 메시지도 많아진다. 즉, 제안된 프로토콜은 각 Sensor node마다 단독적으로 인증이 진행되는 반면, ZigBee의 경우 주변 센서들과 모두 인증을 수행해야하기 때문에 센서의 수가 증가할수록 인증 횟수가 증가하기 때문에 제안 기법이 더 적은 횟수로 인증이 수행된다.

따라서 본 논문에서 제안한 프로토콜은 인증 프로토콜에 대한 4가지 보안 위협에 모두 대응하면서 수중 환경의 열악한 통신 성능을 고려하여 전송 메시지 크기와 메시지 전송 횟수를 감소시킴으로써 경량화하였다.

V. 결 론

수중 음파 센서 네트워크를 이용한 수중 환경의 자료 수집을 통해 오염도 측정, 자연 재해 예방 등 다양한 연구가 진행되고 있다. 하지만 이러한 수중 환경에서 수집된 자료는 전송하는 과정에서 탈취되거나 위·변조 되는 등의 보안 위협에 노출되어 있다. 따라서 이러한 보안 위협에 대응하기 위해 먼저 각 통신 개체 간의 신뢰성을 입증하고, 정당한 개체 간에 비밀키를 공유하는 인증 및 키 발급 프로토콜이 필요하다. 이를 통해 공유된 비밀키를 이용하여 수집된 자료를 암호화하여 전송하거나 위·변조 여부를 확인할 수 있는 MAC 값을 함께 전송하는 보안 기술을 사용할 수 있다.

수중 환경은 좁은 대역폭의 사용으로 전송 속도가 낮고, 전송 지연이 빈번하게 발생하며, 패킷 충돌이나 간섭 등으로 인해 추가적인 오버헤드가 발생하기 때문에 통신 성능이 좋지 않다. 그렇기 때문에 본 논문에서는 프로토콜 상에서 전송되는 메시지 크기를 최소화하여 수중 환경의 제한사항을 극복하는 경량화한 인증 및 키 발급 프로토콜인 UW-AKE를 제안하였다. 제안한 인증 및 키 발급 프로토콜은 nonce 값과 신원 정보 등을 이용하여 설계함으로써 재전송 공격이나 선택 메시지 공격 등과 같은 인증프로토콜에 대한 공격에 대응하여 경량화한 것뿐만 아니라 보안성도 함께 고려하였다.

본 논문에서 제안한 인증 및 키 발급 프로토콜을 이용하면 Base station과 Sensor node, Cluster head, Surface station 간의 신뢰성을 입증하고, Sensor node와 Base station 간에는 비밀키를 공유하게 된다. 신뢰성이 입증되면 Base station은 정당한 Sensor node로부터 온 자료는 수용하고, 인증되지 않은 Sensor node로부터 온 자료는 무시할 수 있다. Sensor node는 공유된 비밀키로 수집한 자료를 암호화하여 전송함으로써 공격자에게 자료가 그대로 노출되는 것을 방지할 수 있다. 또, 전송되는 데이터에 MAC 값을 포함시켜 전송함으로써 데이터의 위·변조 여부도 확인할 수 있기 때문에 보안 기술은 반드시 필요하다. 따라서 수중 음파 센서 네트워크 환경을 고려하여 이에 적합한 보안 기술의 연구가 더욱 활발히 이루어져야한다.

References

[1] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: research challenges," *Ad Hoc Network 3, Elsevier*, pp. 257-279, 2005

[2] Y. Cong, G. Yang, Z. Wei, and W. Zhou, "Security in underwater sensor network," *2010 Int. Conf. Commun. Mobile Comput.*, pp. 162-168, Shenzhen, China, Apr. 2010.

[3] R. B. Manjual and S. S. Manvi, "Issues in underwater acoustic sensor networks," *Int. J. Comput. Electrical Eng.*, vol. 3, no. 1, pp. 101-110, Feb. 2011.

[4] Z. Jiang, "Underwater acoustic networks – issues and solutions," *Int. J. Intelligent Control Syst.*, vol. 13, no. 3, pp. 152-161, Sept. 2008.

[5] G. Dini and A. L. Duca, "SeFLODD: A secure network discovery protocol for underwater acoustic networks," *ISCC 2011 IEEE*, pp. 636-638, Kerkyra, Jun.-Jul. 2011.

[6] J.-Y. Lee, N.-Y. Yun, S. Muminov, S.-Y. Shin, Y.-S. Ryuh, and S.-H. Park, "A focus on practical assessment of MAC protocols for underwater acoustic communication with regard to network architecture," *IETE Tech. Rev.*, vol. 30, no. 5, pp. 375-381, Sept.-Oct. 2013.

[7] J.-E. Kim, N.-Y. Yun, Y.-P. Kim, S.-Y. Shin, S.-H. Park, J.-H. Jeon, S.-J. Park, S. K. Kim,

and C.-H. Kim, “Design and performance evaluation of hierarchical protocol for underwater acoustic sensor networks,” *J. Korea Soc. Simulation*, vol. 20, no. 4, pp. 157-166, Dec. 2011.

[8] ZigBee Alliance, ZigBee Specifications, 2007

[9] J. Abraham and K. S. Ramanatha, “An efficient protocol for authentication and initial shared key establishment in clustered wireless sensor networks,” *Wirel. Optical Commun. Netw., 2006 IFIP Int. Conf.*, Bangalore, 2006.

[10] J. Ibriq and I. Mahgoub, “A hierarchical key establishment scheme for wireless sensor networks,” in *Proc. AINA’07*, pp. 210-219, Niagara Falls, Canada, May 2007.

[11] K. Han and T. Shon, “Sensor authentication in dynamic wireless sensor network environments,” *Int. J. RFID Security and Cryptography (IJRFIDSC)*, vol. 1, no. 1-4, Mar.-Dec. 2012.

[12] A. J. Menezes, et al., Chapter 10 in *Handbook of Applied Cryptography*, CRC Press, 1996.

[13] WHOI Acoustic Communications: Micro-Mode, available from: http://acomms.whoi.edu/umdem

박 민 하 (Minha Park)

2013년 2월 : 국민대학교 수학과 졸업

2013년 3월~현재 : 국민대학교 금융정보보안학과 석사과정

<관심분야> 정보보안, 무선통신/이동통신 보안, TVWS

김 역 (Yeog Kim)

1992년 2월 : 성신여자대학교 전산학과(이학사)

2002년 2월 : 고려대학교 정보보호대학원(공학석사)

2010년 8월 : 고려대학교 정보보호대학원(공학박사)

2011년 9월~현재 : 국민대학교 정보보안연구소 연구원

<관심분야> 이동통신 보안, 암호모듈 검증, 포렌식

이 옥 연 (Okyeon Yi)

1988년 2월 : 고려대학교 수학과 졸업

1990년 2월 : 고려대학교 대학원 (이학석사)

1996년 8월 : Univ. of Kentucky (이학박사)

현재 : 국민대학교 수학과 교수

<관심분야> 이동통신 보안, 스마트그리드 보안, 화이트박스 암호