# UW-ASN 환경에 적합한 메시지인증코드 분석 연구

정재욱°, 전희승*, 원동호†
°*성균관대학교 정보통신보호연구실
e-mail:{jwjung°, hsjeon, dhwon}@security.re.kr

# A Study on Analysis of Suitable MAC in UW-ASN Environment

Jaewook Jung°, Huiseung Jeon*, Dongho Won†
°Information Security Group, Sungkyunkwan University

● 요 약 ●

수중 음향 센서 네트워크(Underwater Acoustic Sensor Network, UW-ASN) 환경에서 센서노드간 데이터를 안전하게 전송하기 위해 우선적으로 암호화 알고리즘을 사용하지만, 암호화 알고리즘만으로는 충분한 안전성을 제공하지 못한다. 암호화 알고리즘은 기밀성을 제공하지만 무결성은 제공하지 못하기 때문이다. 그렇기 때문에 수중 통신 환경에서도 암호화 기술 이외에, 전송된 데이터가 변경되지 않고 안전하게 전송되었다는 무결성을 보장할 수 있는 암호화 기술이 적용되어야 한다. 이에 본 논문에서는 무결성 보장을 위한 메시지 인증 기술에 대한 연구를 진행하며, 수중 환경에 가장 적합한 메시지 인증코드(MAC)의 도출을 위한 분석 절차를 제안한다.

**키워드:** 수중 음향 센서 네트워크, MAC, NMAC, HMAC, UMAC, CMAC

## I. 서론

수중 음향 센서 네트워크 환경에서 데이터를 안전하게 전송하기 위해 우선적으로 암호화 알고리즘을 사용하지만 무결성(Integrity)은 보장하지 못하기 때문에 충분한 안전성을 제공하지 못한다. 그렇기 때문에 수중 통신 환경에서도 전송된 데이터가 변경되지 않고 안전하게 전송되었다는 무결성을 보장할 수 있는 기술이 적용되어야 한다. 또한, 무결성과 함께 메시지 인증(Authentication) 기술도 함께 적용되어야 한다.

이에 본 논문에서는 수중 통신 환경에 적합한 MAC을 선정하기 위한 분석 절차를 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 현재 널리 사용되고 있는 MAC 종류에 대한 분석을 진행한다. 3장에서는 수중 센서 네트워크 환경에 적합한 MAC 도출을 위한 방법론을 제안하며, 마지막으로 4장에서 결론을 맺는다.

## II. 관련 연구

본 장에서는 현재 널리 쓰이는 해시함수 기반의 MAC(HMAC, NMAC, UMAC)과 블록 암호 기반의 MAC(CMAC)에 대하여 살펴본다.

### 2.1 NMAC(Nested MAC)

NMAC은 SHA-1과 같은 해시 함수를 반복적으로 사용하는 구조를 바탕으로 MAC값을 생성한다. 또한 MAC값을 생성하고 검증하는데 있어 두 개의 비밀키가 사용되는데, 이는 반복적으로 사용되는 해시 함수 구조에 대한 위조를 방지하기 위함이다.

### 2.2 HMAC(Hash-based MAC)[2]

HMAC 또한 SHA-1과 같은 해시 함수를 반복적으로 사용해서 MAC값을 생성한다. HMAC은 MAC값을 생성하고 검증하는데 있어서 하나의 비밀키를 사용한다. 단순한 NMAC보다는 조금 더 복잡하며, 패딩(ipad, opad)이 추가된 키 값과 초기화벡터(IV)값이 해시 함수의 입력으로 사용된다. 현재, HMAC에 사용할 수 있는 해시함수로는 SHA-1, MD5, 그리고 RIPEMD-128/160등이 있다.

### 2.3 UMAC(Universal hashing[1] MAC)[3]

UMAC은 높은 성능을 위해 속도가 빠른 Universal 해시 함수를 사용한 메시지 인증 코드 방식이다. Universal 해시함수를 사용하여 입력된 메시지에 대한 짧은 문자열(Short string)을 생성한다. 생성된 문자열은 의사난수 패드(Pseudorandom Pad)와 XOR 연산을 통해 UMAC 태그(Tag)의 생성이 가능하다.

### 2.4 CMAC(Cipher-based MAC)

CMAC은 AES와 같은 대칭키 블록 암호화 방식을 기반으로,

† 교신저자, dhwon@security.re.kr

1) Universal hashing: 해시함수를 선택하기 위한 확률적 알고리즘

키를 이용하는 해시함수다. AES-CMAC은 비밀키, 가변길이의 메시지, 그리고 메시지의 길이를 입력으로 받고, 고정길이의 MAC을 생성한다. AES-CMAC의 핵심은 CBC-MAC이며, 메시지에 대한 인증을 제공하기 위해 CBC-MAC을 사용한다. CMAC의 동작방식은 패딩이 필요한 경우와 필요하지 않은 경우 이렇게 두 가지로 분류할 수 있다.

## III. UW-ASN 환경에 적합한 MAC 도출

본 장에서는 수중센서 네트워크 환경에 적합한 메시지 인증 코드의 도출을 위한 방법 절차를 제안한다. 제안한 분석 절차는 아래 그림 1과 같다.


그림 1. 분석 절차
Fig. 1. Analysis Procedure

먼저 수중 통신 환경에 존재하는 위협에는 도청, 전력소모공격(센서노드의 전력소모 공격), 정보의 위·변조 공격 등이 가능하다. 또한, 수중 통신 환경에 존재하는 제약사항으로는 짧은 배터리 수명, 좁은 대역폭, 제한된 메모리 공간 그리고 전송 메시지의 손상 및 변경이 제약사항으로 작용할 수 있다.

이에 본 논문에서는 앞서 언급한 위협 및 제약사항을 해결하기 위한 요구사항으로 다음 네 가지 항목들을 도출하였다.

- 확장성(센서노드의 추가 및 변경 고려)
- 저장값 최소화(센서노드의 제한된 메모리 공간 고려)
- 전송량 최소화(수중환경의 좁은 대역폭 고려)
- 연산량(센서노드의 전력소모 최소화)

도출한 네 가지 요구사항을 기준으로 앞서 소개한 NMAC, HMAC, UMAC, CMAC에 대한 비교 분석을 진행한다. 분석 결과를 바탕으로 최종적으로 수중환경에 가장 적합한 메시지 인증 코드를 도출한다.

## IV. 결론

수중 음향 센서 네트워크 환경에서도 전송된 데이터가 변경되지 않고 안전하게 전송되었다는 '무결성'을 보장할 수 있는 기술이 적용되어야 한다.

이에 본 논문에서는 수중 통신 환경에 적합한 MAC을 선정하기 위한 분석 절차를 제안하였다. 향후 연구 과제로는 제안한 분석 절차를 바탕으로, 직접 수중 통신 환경에 가장 적합한 MAC을 선정하도록 한다.

## 참고문헌

[1] M Bellare, J Kilian…, "The security of the cipher block chaining message authentication code", Journal of Computer and System Sciences Volume 61, Issue 3, December 2000, Pages 362-399.

[2] H Krawczyk, R Canetti…, "HMAC: Keyed-hashing for message authentication", RFC 2104, February 1997.

[3] J. Black, S. Halevi,..., "UMAC: Fast and Secure Message Authentication", Lecture Notes in Computer Science, 1999, Volume 1666/1999, 79.

## Acknowledge

본 연구는 방송통신위원회의 방송통신융합미디어원천기술개발사업의 연구결과로 수행되었음(KCA-2012-12-912-06-003)