수중무선통신 환경에 적합한 AES, ARIA 블록암호 기반 CCM-UW 구현 및 성능 분석

이재훈* · 박민하* · 윤남열* · 이옥연* · 박수현*

*국민대학교

Implementation and Analysis Performance of CCM-UW based AES, ARIA Blockcipher for Underwater Environment

Jae-Hoon Lee* · Minha Park* · Nam-Yeol Yun* · Okyeon Yi* · Soo-Hyun Park*

*Kookmin University

guderian88@kookmin.ac.kr, mhpark@kookmin.ac.kr, anuice@naver.com, oyyi@kookmin.ac.kr, shpark21@kookmin.ac.kr

요 약

수중무선통신 시스템은 수질 조사, 해양 자원 탐사 및 개발, 해양환경 분석 및 군사적인 정보 수집 수단 등 다양한 분야에 활용 가능하다. 하지만 수중무선통신 환경에서는 매질의 특성과 다양한 지형적 요소, 의도된 공격 등으로 인해 데이터 손실이 발생하고 데이터 위변조를 포함한 다양한 보안위협이 존재한다. 이를 해결하기 위해서 본 논문에서는 데이터 기밀성, 무결성, 출처인증, 그리고 재공격 방지기능을 제공하는 CCM 운영모드를 수중무선통신 환경에 적합하게 변형한 CCM-UW(CCM Underwater)운영모드를 제안한다. 이를 수중무선통신 MAC 프로토콜인 MACA Protocol에 구현하고 통신 속도를 측정해서 CCM-UW의 보안적용 가능성과 통신환경에 미치는 영향을 분석하고자 한다.

ABSTRACT

Underwater Wireless Communication System can be useful for research of quality of water, ocean resources exploration, analysis ocean environment and so on. However, there exist security threats including data loss, data forgery, and another variety of security threats, because of characteristics of water, various geographical factors, intended attack, etc. To solve these problem, in this paper, we propose a CCM-UW mode of operation modified form of CCM mode of operation, providing data confidentiality, integrity, origin authentication and anti-attack prevent, for the Underwater Wireless Communication System. By implementing CCM-UW in MACA protocol(Underwater Wireless Communication MAC Protocol) and measuring speed of communication, we confirm the applicability of the security and analyze the communication environment impact.

키워드

Underwater Wireless Communication System, Underwater Security, CCM, CCM-UW

Ⅰ. 서 론

최근 스마트 디바이스와 센서네트워크, 유비쿼터스 연구가 활발히 진행되면서 소형장비를 활용한 다양한 응용기술들이 개발되고 있다. 특히 지상의 무선통신환경을 활용한 홈 네트워크, 의료, 산업제어, 스마트 오피스, 군사시설 등 다양한 응용분야들이 있다.

이와 비슷한 연구가 수중환경에서도 진행되고 있다. 강이나 넓은 바다에 각종 센서를 장착한 계측장비들을 설치하여 필요한 정보를 수집하고 수집된 정보는 육상으로 전송되어 실시간으로 관측할 수 있다. 이를 통해 수온의 변화, PH농도 및 BOD, COD등 수중환경 관측이 가능하며, 바다 온난화 관측, 수중 해류변화 관측, 기상 예측 등에 실시간으로 분석, 대응할 수 있게 된다. 또한 수심이 깊은 심해처럼 사람이 직접 수행하기 힘든 수중 환경 작업이 쉬워진다. 특히 우리나라 영해에 잠수함, 함정 등 탐지할 수 있는 센서를 설치하면 적국의 침입이나 군사적인 움직임과 같은 다양한 군사적 정보수집 용도로도 활용될 수 있다. 이외에도 수산업, 어업 등에 활용하면 경제에 긍정적인 영향을 줄 수 있다.[1~3]

하지만 수중무선통신은 지상 무선통신과 달리

통신환경이 매우 열악하다. 수중의 경우 전파가 아닌 음파를 이용한 무선통신을 한다. 음파를 이용한 무선통신은 전파에 비해 전송속도가 느리며, 전달할 수 있는 데이터양도 제한적이다. 또한 음파는 물의 염도, 온도, 흐름 등 매질 특성과 불규칙한 해양지형구조에 따른 다중경로로 인한 데이터 손실이 발생한다. 따라서 수중무선통신에는 데이터 무결성 확인이 반드시 필요하다.

또한 수중무선통신도 지상무선통신과 마찬가지로 데이터에 대한 노출 및 위변조 위협이 존재한다. 특히 군사적인 목적으로 수집된 정보같은 중요 정보들은 노출에 대한 보호가 필요하다. 제한된 전력을 가진 계측 장비나 센서들은 통신에 방해가 되는 데이터를 차단함으로서 효율적인 전원관리를 수행해야 한다. 따라서 데이터에 출처인증 기능을 부여하여 선별적으로 수신해야 한다.[4~5]

본 논문은 다양한 응용분야에 활용될 수중무선통신에 존재하는 다양한 위협들에 대응방안으로 암호학적인 방법을 제시한다. 데이터 기밀성과 무결성 및 출처인증기능을 제공하는 CCM과 CCM*를 분석하여 수중무선통신에 적합한 CCM-UW (CCM Underwater)운영모드를 제안한다.

본 논문의 구성은 1장 서론을 시작으로 2장에서는 무선 센서네트워크 환경과 수중무선통신환경의 유사성을 분석하고 무선 센서네트워크에서 제안하는 CCM*의 내용에 착안한 CCM-UW을 3장에서 설명하고자 한다. 4장에서는 CCM-UW를 실험한 환경과 성능 분석 방법 및 분석한 결과를 제시하고 마지막 5장에서 결론 및 향후 연구 내용을 서술한다.

Ⅱ. 관련 연구

IEEE 802.15.4 표준 LR-WPAN(Low-Rate Wireless PAN)은 저전력을 목적으로 하는 무선 센서네트워크의 PHY/MAC 계층을 정의한 표준이다. 센서네트워크에 활용되는 장비들은 한정적인 자원을 활용한 모듈로 구성되며 지속적인 전원공급이 어려기 때문에 균형적인 전력관리가 필요하다. 이에 IEEE 802.15.4 표준은 RFD(Reduced Function Device)와 FFD (Full Function Device)로 구분하고 코디네이터를 지정하여 클러스터를 기반으로 관리한다.[6] 이러한 네트워크 구성은 수중무선통신 환경과 매우 흡사하다.

IEEE 802.15.4 표준은 무선 센서네트워크에 존재하는 다양한 위협원에 대한 대응방안으로 많은 전력소모와 자원을 요구하는 공개키 알고리즘 대신 국제 표준 블록암호 알고리즘 AES-CCM*운영모드(기존의 CCM운영모드(그림 1)를 변형한 형태)를 통해 표 1에 제시된 보안기능들을 제공한다.

CCM*는 기존 CCM에 보안레벨을 설정함으로써 정해진 8단계 보안레벨에 따라 동작한다.

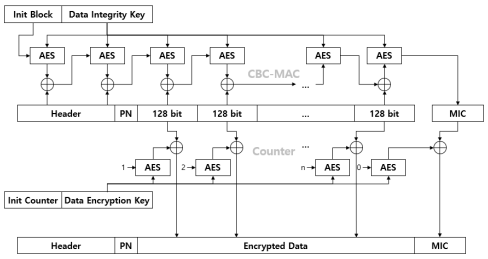

그림 1. CCM 운영모드

표 1. CCM* 보안레벨

보안레벨	Encrypt	Integrity
0	No	No
1	No	MIC-32 bit
2	No	MIC-64 bit
3	No	MIC-128 bit
4	Encrypt	No
5	Encrypt	MIC-32 bit
6	Encrypt	MIC-64 bit
7	Encrypt	MIC-128 bit

하지만 CCM*가 동작하기 위해선 추가적인 보안요소가 보조보안헤더(Auxiliary Security Header)에 할당되어 있으며 반드시 필요하다. 보조보안헤더는 표2와 같다.

표 2. 보조보안헤더

Octets : 1	4	0/1/5/9
Security Control	Frame Counter	Key Identifier

보조보안헤더는 최소 5바이트에서 최대 14바이트 길이를 갖는데 열악한 수중환경에서 활용하기에는 너무 많은 데이터가 생성된다. 따라서 본 저자는 CCM과 CCM*를 분석을 통해 보조보안헤더를 수정한 CCM-UW를 제안한다.

Ⅲ. CCM-UW 운영모드

CCM(Counter with CBC-MAC)운영모드는 Counter Mode와 CBC-MAC이 결합된 운영모드이며 국제표준 NIST Pub 800-38C에 정의되어 있다. CCM은 데이터 기밀성뿐 아니라 TAG (CBC-MAC)값을 통해 데이터의 무결성과 출처인증을 제공한다.[7] IEEE 802.15.4 표준은 CCM의 TAG값 길이를 0, 4, 8, 16바이트로 제한하고 데이터 기밀성 선택에 따라 8개의 보안레벨로 정의한다. 하지만 200bps 무선 통신환경을 가지고 있는 수중환경에서 16바이트의 TAG값을 전송하는 것은 실제 보내는 데이터의 길이보다 보안요소 데이터의 길이가가 더 길어지는 결과를 초래한다.

따라서 기존의 CCM*이 CCM운영모드에서 길이

를 고정하여 변형한 것처럼 16바이트를 제외한 0, 4, 8바이트만 정의해서 사용한다.(표 3)

표 3. CCM-UW 보안레벨

보안레벨	Encrypt	Integrity
0	No	No
1	No	MIC-32 bit
2	No	MIC-64 bit
3	Encrypt	No
4	Encrypt	MIC-32 bit
5	Encrypt	MIC-64 bit

또한 기존 CCM*를 사용하기 위해 필요한 보조보안헤더는 최대 14바이트가 필요하다. 이는 대부분 키 확장성을 고려한 Key Identifier값 때문에 발생되는 데이터들이다. 따라서 본 논문에서는 수중통신환경에 적합하게 Frame Counter를 2바이트로 줄이고, Key Identifier는 상위 계층에 도움을 받도록 설계하여 생성된 키는 보조보안헤더 Key Identifier Mode를 통해 기능별, 역할별로 구분하여 선택적으로 사용할 수 있도록 설계했다. 결과적으로 기존의 최대 14바이트에서 4바이트로 줄임으로써 데이터 증가량을 줄였다.(그림 2)

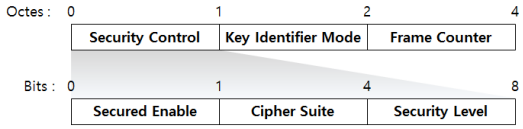

그림 2. CCM-UW 보조보안헤더

IEEE 802.15.4는 국제 표준 블록암호알고리즘인 AES를 기반으로 CCM*운영모드를 정의하고 있다. 하지만 AES는 국내 CMVP기준에 비검증 암호로써 정부 및 관공서 등에서는 사용할 수 없는 암호알고리즘이다. 따라서 국내 CMVP 검증필 암호알고리즘인 ARIA를 탑재하고 AES와 선택적으로 동작할 수 있도록 Cipher Suite field를 추가하여 국내외 모두 사용가능하도록 설계하였다.

Ⅳ. 구현환경 설명 및 실험 결과

CCM-UW(CCM Underwater)의 성능 평가를 위해 MACA 프로토콜이 구현된 MAC base board에서 실험을 진행했다. MAC based board는 저가형 응용프로그램에 최적화된 Cortex-M3 계열 32bit 72MHz MCU로 128kB 프로그램 메모리, 20kB 데이터 RAM 메모리를 가지고 있다.(그림3) 수중모뎀의 성능은 최대 통신 범위가 350m이고, 최대 2kbps 데이터 처리 능력을 가지고 있다.(그림 4)

그림 3. MAC based board

그림 4. 수중모뎀

C언어 기반으로 구현된 MACA Protocol에 블록암호 AES, ARIA, 운영모드 CCM-UW도 C언어로 구현했다. IDE는 IAR Assembler for ARM 5.41.0.51741이다. 기존의 C언어로 구현된 MACA Protocol에 CCM-UW를 구현하기 전과 후의 컴파일 결과는 표 3과 같다.

표 3. CCM-UW 적용 전후 컴파일 결과

	orignal MACA	MACA with CCM-UW
Code memory	15,350bytes	23,772bytes
Data memory (read only)	2,815bytes	5,149bytes
Data memory (read&write)	4,694bytes	11,190bytes

실험은 가로 세로 1.8m×1.8m 크기인 수조에서 진행했다. 넓은 수중 환경에서는 최대 2kbps속도로 테스트가 가능하지만 수조는 다중 경로로 발생되는 에러율을 줄이기 위해서 200bps로 낮춰서 실험하였다. 실험에는 상위 계층에서 키 관리 기능을 통해 키가 미리 발급되어 있다고 가정했다. MACA Protocol은 상위 계층으로부터 받은 Key Security Control, Data를 통해 보조암호헤더를 생성하고, 생성된 보조암호헤더와 Key Identifier Mode값으로 송신 노드는 데이터 암호화를 진행하며 수신 노드는 데이터 복호화를 진행한다.

송신노드가 상위계층에서 데이터를 받아 수신노드의 상위계층에 데이터가 도착할 때까지의 시간을 측정한다. 데이터 크기는 10bytes로 고정하여 보안레벨과 블록암호 알고리즘 두 기준으로 통신 시간을 측정했다.

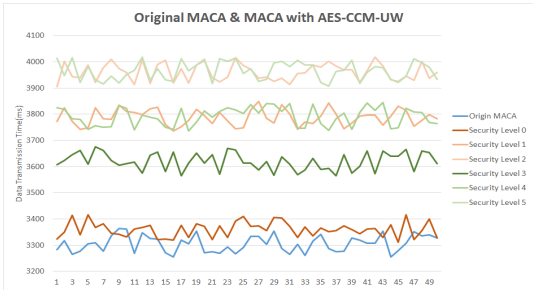

그림 5. AES-CCM-UW 적용전후 보안레벨별 전송시간

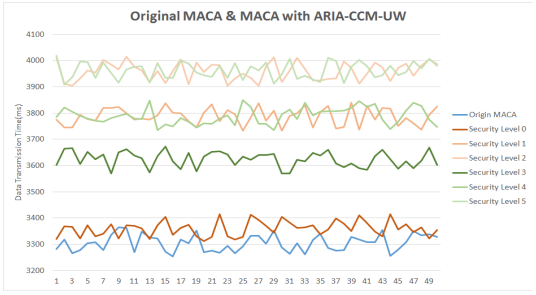

그림 6. ARIA-CCM-UW 적용전후 보안레벨별 전송시간

그림 5와 그림 6은 각각 AES와 ARIA의 보안레벨별 전송 시간(ms)를 측정한 결과이다. 보안을 적용함으로서 발생되는 시간을 확인 할 수 있다. 증가된 시간은 크게 두 가지 요인이 있다. 첫 번째는 암호알고리즘이 동작시간이고 두 번째는 보조보안헤더와 TAG값을 전송하는데 소요된 시간이다. 큰 특징으로는 TAG값 생성으로 발생되는 시간을 볼 수 있는데, 3600ms에서 4000ms에 크게 3부분으로 들어난다. 이 부분이 보조보안헤더와 TAG값을 보내는데 소요된 시간으로 볼 수 있다.

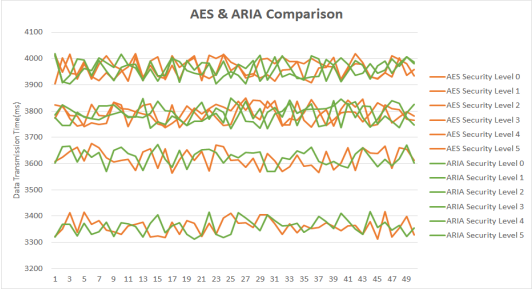

그림 7. CCM-UW 보안레벨별 AES와 ARIA비교

표 4. AES와 ARIA 보안레벨별 소요시간(ms) 평균

	레벨0	레벨1	레벨2	레벨3	레벨4	레벨5
AES	3360.049	3788.090	3960.479	3620.107	3791.287	3965.699
ARIA	3368.231	3787.511	3959.101	3624.070	3789.182	3962.523

그림 7은 AES와 ARIA의 보안레벨별 테스트한 결과를 한 그래프에 표현한 그림이다. 그래프의 위치나 값을 비교해 보면 AES나 ARIA의 큰 차이를 보기 힘들다. 즉, AES와 ARIA가 같은 보안강도를 가지는 블록암호 알고리즘으로서[8] 통신에 미치는 영향의 차이는 거의 없다고 봐도 무관하다. 두 알고리즘 비교결과는 표 4와 같다.

Ⅴ. 결론

수중무선통신 환경의 연구가 새로운 분야로서 활발하게 연구되면서 다양한 분야에 활용되고 중요정보들이 수집될 것이다. 데이터 노출과 위변조가 가능한 수중환경에서의 보안은 불가피하다.

CCM-UW는 CCM과 CCM*에서 제공하는 데이터 기밀성과 무결성, 출처인증 보안기능을 제공함으로서 데이터를 보호하고 선별적으로 데이터를 수신할 수 있다. 또한 AES와 비교해 보았을 때 성능차이가 없는 ARIA를 사용함으로써 국내 정보보호법을 만족하는 수중무선통신이 가능하다.

하지만 보안이 적용됨에 따라 발생되는 데이터와 암호알고리즘 동작으로 인해 발생하는 지연은 수중무선통신에 방해요인으로 작용할 수 있다. 따라서 데이터 길이와 암호알고리즘을 개선하여 통신환경에 미치는 영향을 줄일 방안에 대한 연구가 필요할 것이다.

참고문헌

[1] I. F. Akyildiz, D. Pompili, and T. Melodia, “Underwater acoustic sensor networks : research challenges,” Ad Hoc Networks (Elsevier), Vol. 3, no. 4, pp. 257-279, May 2005.

[2] J. Heidemann, W. Ye, J. Wills, A. Syed, and Y. Li, “Research challenges and applications for underwater sensor networking,” IEEE WCNC, 2006.

[3] 박성준, 박수현, 김상경, 김창화, “수중통신과 해양센서네트워크 기술,” 정보과학회지 제28권 제7호, pp. 79-88, 2010.7

[4] Adrian Perring, John Stankovic and David Wagner. “Security in Wireless Sensor Networks” Communication of the ACM. 47(6), 53-57. 2004.

[5] W. Wang et al, “Visualization of Wormholes in Underwater Sensor Networks: A Distributed Approach” Int’l J.Security Net, vol. 3, no. 1, 2008, pp.10-23.

[6] IEEE standard 802.15.4 : IEEE Standard Local and metropolitan area networks-Part 15.4 : Low-Rate Wireless Personal Area Networks (LR-WPANs), 2011.

[7] Morris Dworkin, “Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality” NIST 800-38C, 2004.

[8] KS X 1213 : 128비트 블록암호 알고리즘 ARIA, 2004

ACKNOWLEDGE

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