KCMVP를 위한 MICOM 환경에서의 ARIA-CCM, ARIA-GCM 구현 및 성능분석 비교

이재훈* · 박민하* · 황누리* · 이옥연* · 김기헌**

*국민대학교, **NSRI

Implementation and Analysis Performance of CCM, GCM based ARIA Block CIpher for Korea CMVP.

Jae-Hoon Lee* · Minha Park* · Nu-Ri Hwang* · Okyeon Yi* · Kiheon Kim**

*Kookmin University, **NSRI

guderian88@kookmin.ac.kr, mhpark@kookmin.ac.kr, yubkinuri@kookmin.ac.kr, oyyi@kookmin.ac.kr, khkim@ensec.re.kr.

요 약

최근 스마트 디바이스 연구가 진행되면서 MICOM과 같은 경량 디바이스에서도 정보보호 기능을 제공해야 한다는 요구가 늘어가고 있다. Zigbee의 경우 IEEE 802.15.4 표준에 정의된 AES-CCM*를 적용함으로서 정보보호 기능을 제공하고 있다. 하지만 국내에서는 정보보호법에 의해 KCMVP(국내 암호모듈 평가인증제도)를 받은 제품만이 공공기관 및 관공서에서 사용될 수 있다. 따라서 본 논문은 IEEE 802.15.4 표준에 정의된 예약영역(Reserved)에 KCMVP용 ARIA-CCM, ARIA-GCM이 활용될 수 있는 방안을 제시한다. 또한 MICOM 환경에서 IEEE 802.15.4 표준에 적용된 ARIA-CCM, ARIA-GCM 성능분석을 위해 AES-CCM*와 속도비교 결과를 제시한다.

ABSTRACT

As Smart Device research processes, the needs of information security in light devices is increasing. For example, Zigbee provide Information Security by applying AES-CCM* defined IEEE 802.15.4 standard. However, according to information security law in Korea, only devices with KCMVP certification can be used in government organization and facilities. Therefore, this paper provide a solution to apply ARIA-CCM and ARIA-GCM for KCMVP in reserved field of IEEE 802.15.4 standard. For analyzing performance, we provide the speed test result of ARIA-CCM and ARIA-GCM comparing with AES-CCM*.

키워드

IEEE std 802.15.4 security, CCM*, MICOM security, ARIA-CCM, ARIA-GCM

Ⅰ. 서 론

2012년 12월 31일 이후 국내에서는 아날로그 방송 서비스를 종료하고 디지털 방송 서비스로 전환하였다. 디지털 방송 서비스는 아날로그 방송 서비스에 비해 적은 주파수 대역을 사용하기 때문에 디지털 방송 서비스로의 전환으로 인해 사용하지 않는 빈 주파수 대역이 발생하게 되었다. 이를 TVWS(TV White Space)라 하는데 이 주파수 대역을 이용하여 무선 가입자 망을 늘리거나, 환경 정보 혹은 재난 발생 시 관련 정보를 수집 하는 서비스 등이 가능하게 되었다. 현재 미국, 영국, 일본 등 국외에서도 TVWS를 이용하여 광대역 인터넷 서비스, 스마트 도시 구축 등의 다양한 서비스를 위한 연구들이 활발하게 진행되고 있다. 국내에서도 TVWS를 활용한 다양한 서비스를 제공하기 위해 많은 연구들이 진행되고 있다. 특히 지능형 전력망 시스템과 같은 국가적인 사업을

위해 TVWS가 사용되기 위한 연구가 지속되고 있다. 이와 같이 국내/외 모두 TVWS에 관심을 갖고 이와 관련된 기술 개발을 진행하고 있으며 저속도 무선 개인망 통신을 위한 표준인 IEEE 802.15.4를 이용하여 TVWS 대역을 이용한 무선 통신을 위한 기술의 표준화 작업도 진행 중에 있다[1].

더불어 스마트 디바이스 연구도 함께 활발히 진행되면서 다양한 분야에서 MICOM과 같은 소형 장비가 사용되고 있다. 헬스케어, 홈네트워크, 산업제어 시스템, 스마트그리드, 수중통신 등 분야가 점점 확대되어가고 있으며 이러한 서비스들이 TVWS를 통해 제공되기 위한 연구들이 진행되고 있다.

이러한 연구들이 진행되는 과정에서 단순히 기술적인 서비스뿐만 아니라 안전한 통신을 위한 보안 기술도 함께 연구되고 제공되어야 한다는 요구가 증가하고 있다. 스마트 디바이스의 대표 개발기구로는 Zigbee Alliance가 있다. Zigbee Alliance는 IEEE 802.15.4기반의 PHY/MAC을 기반하여 네트워크 계층과 어플리케이션 계층을 정의하고 있다. 여기서 Zigbee Alliance는 IEEE 802.15.4 표준에 정의되어 있는 AES-CCM*를 활용하여 네트워크 계층과 어플리케이션 계층의 보안기능을 제공하고 있다[2].

하지만 AES-CCM*는 KCMVP(국내 암호모듈 평가인증제도)에 비검증 블록암호알고리즘을 사용하고 있다. 현재 국내에서는 전자정부법 정보보호법에 따라 국가기관 및 공공기관에서는 정보보호 제품에는 KCMVP인증을 받은 보안제품을 사용해야 한다. 이로 인해 Zigbee와 같은 무선 센서네트워크 장비를 국내에서는 사용이 제한되고 있다.

따라서 본 논문은 무선 센서네트워크에 적합한 MICOM환경에서 KCVMP인증을 받을 수 있는 ARIA-CCM*와 ARIA-GCM을 구현함으로써 구현적 합성을 평가하고 기존의 AES-CCM*와 성능비교를 통해 성능을 검증하고자 한다.

Ⅱ. 관련 연구

본 장에서는 IEEE 802.15.4 표준에 정의된 Security를 살펴보고자 한다. IEEE 802.15.4 “Low-Rate Wireless Personal Area Network”는 저전력을 목표로 무선 센서 네트워크의 PHY/MAC을 정의한 표준이다[3].

본 논문에서는 IEEE 802.15.4 표준을 살펴봄으로써 MAC계층에서 제공하는 정보보호 기능이 어떻게 설계되어 있는지 파악하고 이를 KCMVP 인증의 검증대상 알고리즘인 ARIA와 운영모드 CCM*, GCM을 적용시킬 방법을 제안한다.

1. MAC 계층 데이터 프레임 구조

IEEE 802.15.4 표준에 정의된 일반적인 데이터 프레임 구조는 그림 1과 같다. 그림 1에 표기된 Octet은 1Byte 크기를 의미하고 Bit는 1bit 크기를 의미하며 숫자는 각 영역의 크기를 말한다.

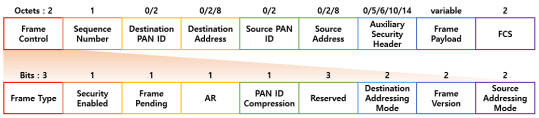

그림 1. 데이터 프레임 구조와 Frame Control 데이터

위 영역 중 정보보호 기능에 관여하는 영역은 다음과 같다.

- Frame control
- Auxiliary Security Header

Frame control 영역에서 Security Enable값과 Prime Version값을 통해 정보보호 기능의 적용 여부를 판단 할 수 있다. Security Enable값이 ‘0’으로 설정되어 있으면 정보보호기능이 제공돼지 않은 것을 의미하고 ‘1’로 설정되어 있으면 보안 기능이 제공되고 있음을 의미한다. Prime Version값의 경우 IEEE 802.15.4 표준의 버전을 의미하며 2003년 버전과 2011년 버전으로 구분되어 사용되고 있다.

보조보안헤더(Auxiliary Security Header)는 Frame control 영역에서 Security Enable값이 ‘1’로 설정되어 있을 경우에만 존재한다. 이 영역은 보안 기능이 적용된 프레임에 대한 보안요소 정보가 들어있는 영역으로 그림 2와 같다.

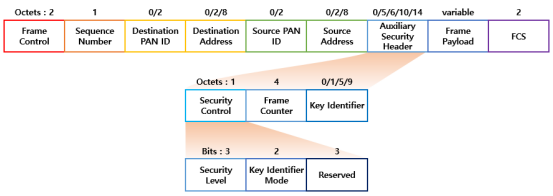

그림 2. Auxiliary Security Header 영역 데이터

보조보안헤더에는 데이터 프레임에 보안 기능을 동작하기 위해 필요한 추가적인 보안 요소 정보들이 포함된다. 먼저 Security control영역을 살펴보자. Security Level은 보안강도를 의미하며 표 1과 같이 8단계의 보안강도를 갖는다.

Key Identifier Mode는 Key Identifier를 활용해 사용할 키를 결정할 때 사용되며 표준에는 4가지 모드를 지원한다. Key Identifier Mode값에 따라 Key Identifier의 크기는 0바이트에서 9바이트의 가변적인 길이를 갖는다.(본 논문에서는 자세히 다루지 않는다.)

표 1. CCM* Security Level

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

Reserved는 예약된 값으로 사용자가 원하는 영역으로 사용가능하다. 예약영역은 3bit로 논리적으로 8개의 값을 할당할 수 있다. 본 논문에서는 이 영역을 활용하여 블록암호 알고리즘와 운영모드를 선택적으로 사용할 수 있도록 설계하였다. 이 영역을 활용하여 국제 표준 알고리즘 AES와 국내 표준 알고리즘 ARIA 및 운영모드 CCM, GCM을 선택적으로 사용할 수 있도록 정의한다. (표 2 참고)

표 2. Reserved 영역(논문에서 제안함)

값(이진수)	블록암호 운영모드
000	AES-CCM*
001	AES-GCM
010	ARIA-CCM*
011	ARIA-GCM

2. 운영모드[4~6]

본 논문에서 사용되는 블록암호 알고리즘 기반 운영모드는 CCM 모드와 GCM모드이다. CCM 운영모드는 NIST 800-38C에 정의되어 있고 GCM 운영모드는 NIST 800-38D에 정의되어 있다. 본 절에서는 간단하게 CCM과 GCM을 알아보도록 하겠다.

CCM 모드와 GCM 모드에서 사용하는 용어는 다음과 같다.

- P : 평문
- K : 비밀키
- C : 암호문
- H : 128bit 변수
- A : 128bit 부가 인증 데이터
- $Counter i$: i 번째 증가 값

CCM 모드와 GCM 모드에서 사용되는 연산은 다음과 같다.

- $\odot$: 유한체 곱 연산
- $|$: 비트열의 연접
- $\oplus$: bit 또는 bit열의 베타적 논리합 연산

(1) CCM(Counter with CBC-MAC) 모드

KCMVP의 검증대상 보호함수 블록 암호알고리즘 기반 운영모드 중 하나로 데이터 기밀성과 데이터 무결성, 출처인증을 동시에 제공하는 블록암호 운영모드이다. Counter모드를 이용해서 데이터 기밀성을 제공하고 CBC-MAC은 데이터 무결성과 동시에 입력값 A를 추가함으로서 출처인증 기능도 제공된다.

다음 그림 3는 CCM을 표현한 그림이다.

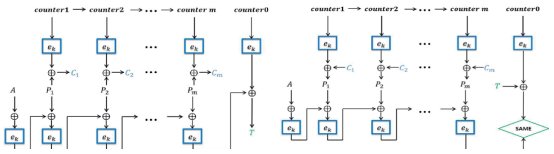

그림 3. CCM 모드 암호화(좌) & 복호화(우)

(2) GCM(Calois/Counter Mode) 모드

KCMVP 검증대상 보호함수 블록 암호알고리즘 기반 운영모드 중 하나로 데이터 기밀성과 데이터 무결성, 출처인증을 동시에 제공하는 불록암호 운영모드이다. Counter모드를 이용해서 데이터 기밀성을 제공하고 유한체 곱 연산을 이용하여 데이터 무결성과 동시에 입력값 A를 추가함으로서 출처인증 긴으도 제공된다.

다음 그림 4는 GCM을 표현한 그림이다.

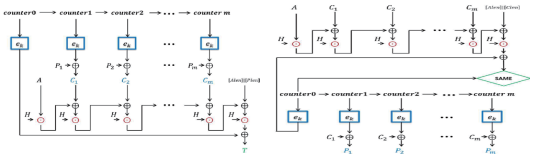

그림 4. GCM 모드 암호화(좌) & 복호화(우)

Ⅲ. 실험환경 및 결과

본 연구에서는 IEEE 802.15.4 표준에 정의된 MAC Protocol 중 보안에 관련된 부분을 선별적으로 구현하여 MICOM 장비와 PC간의 통신을 진행하면서 실험을 진행하였다. 실제 MAC 프로토콜에서 보안을 담당하는 Security 영역만을 구현하여 데이터의 암호화 복호화를 진행하고 그에 따라 소비되는 시간을 측정하였다.

실험은 ATmega128A 개발보드로 AVRStudio 6.1 IDE에서 C언어로 개발하였다. ATmega128A보드는 128KB 코드메모리와 4KB 데이터 메모리를 가지고 있으며 firmware형태로 구현된 소스는 Program Memory 20478bytes(15.6%), Data Memorty 3288 bytes(80.3%)를 사용하고 있다. PC로부터 MAC Frame을 송수신하며 UART 시리얼 인터페이스를 통해서 통신한다. ATmega 128A보

드는 PC로부터 받은 MAC Frame에 Encapsulation을 수행한다. 실험은 PC에서 ATmega128A보드에 MAC Frame을 송수신을 측정하였다. 실험 결과는 그림 5와 같다.

그림 5의 결과는 각각 보안 레벨 별로 데이터 평문의 크기를 16, 32, 64, 96바이트로 설정하여 각각 AES-CCM*, AES-GCM, ARIA-CCM*, ARIA-GCM으로 Encapsulation하는 처리시간을 ms 단위로 측정한 결과이다.

Encapsulation 처리시간은 GCM모드가 CCM에 비해 작게는 2배에서 크게는 3배정도 느린 속도를 보였다. GCM의 경우 4bit, 8bit, 16bit 단위로 유한체 연산을 수행함으로서 속도를 개선하는 방법이 존재한다.[7] 하지만 본 논문에서는 호환성과 국내 KCMVP를 위해 블록암호알고리즘 AES와 ARIA, 운영모드 CCM, GCM을 선택적으로 사용할 수 있도록 구현했다. 이로 인해 GCM 고속화 알고리즘에 필요한 메모리 부족으로 구현하지 못했지만 메모리 환경이 좋은 환경이라면 GCM의 고속화 알고리즘을 적용함으로써 좀 더 좋은 성능을 보일 수 있다.[8]

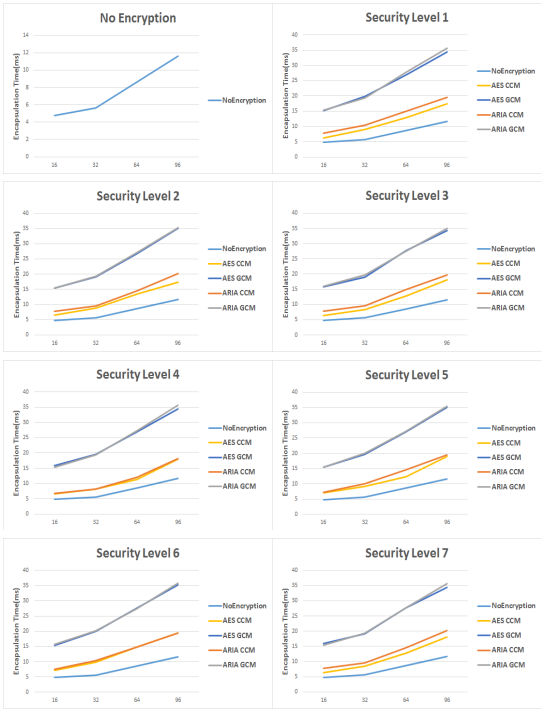

그림 5. 보안레벨별 블록암호와 운영모드 비교

또한 위 결과와 같이 AES가 ARIA에 비해 16바이트를 처리하는데 최대 1.2ms, 64바이트를 처리하는데 최대 3.6ms로 빠른 속도를 보이지만 이는 16바이트 전체 처리속도에 비하면 극히 작은 차이다. 따라서 송수신 데이터가 적고 빈번하지 않은 센서네트워크 환경에 ARIA을 적용해도 AES와 큰 성능 차이를 보이지 않을 것이다.

Ⅳ. 결론

유휴 주파수를 활용한 TVWS나 스마트 디바이스, 수중음파통신과 같이 소형장비를 활용한 응용분야가 활발히 연구되고 있다. 하지만 국내에서는 KCMVP의 비검증 대상 알고리즘 AES를 탑재한 제품은 사용할 수 없다. 이에 본 논문은 무선 센서네트워크의 PHY/MAC을 정의한 IEEE 802.15.4 표준에 정의된 MAC Frame의 Reserved영역을 사용하여 기존의 AES와 함께 KCMVP 검증 대상 알고리즘 ARIA을 사용할 방법을 제시하였고 더불어 CCM*뿐 아니라 GCM도 사용할 수 있다. 이를 통해 국내에서도 ARIA가 탑재된 센서네트워크 장비를 사용할 수 있게 되면서 다양한 응용분야에 활용할 수 있게 되었다.

참고문헌

[1] 장재혁, “TV White Space 생태계 및 상용/시험 서비스 도입 현황”, ETRI, 2013

[2] “ZigBee Specification”, ZigBee Alliance, 2007

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

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

[5] Morris Dworkin, “Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode(GCM) and GMAC” NIST 800-38D, 2007.

[6] KS X 1213 - 2 : 128비트 블록 암호 알고리즘 ARIA - 제2부 : 운용모드, 2009.

[7] David A. McGrew, John Veiga, “The Galois/Counter Mode of Operation(GCM)”

[8] P.Szalachowski, B.Ksiezopolski, Z.Kotulski, “CMAC, CCM and GCM/GMAC: Advanced modes of operation of symmetric block ciphers in wireless sensor networks”, Information Processing Letters 110 p.247-251, 2010.