무선백홀 시스템 보안계층 구현

문진명, 배정숙, 손경열, 이 훈
한국전자통신연구원

{moonjinmyung, jsbae, kysohn, hlee}@etri.re.kr

Security Layer Implementation for Wireless Backhaul systems

Jinmyoung Moon, JungSook Bae, Kyung Yeol Sohn, Hoon Lee

Electronics and Telecommunication Research Institute (ETRI)

요 약

본 논문은 “5G 융합 서비스를 위한 20Gbps P2MP 무선백홀 기술 개발”과제에서 개발하는 고정 점대점(P2P)와 점대다중점(P2MP) 무선백홀 시스템의 허브(HUB)와 터미널(TMN) 간의 보안계층 기술 개발 및 구현 구조에 대해 설명한다.

Ⅰ. 서 론

최근 국내에서 5G 이동통신 상용 서비스가 본격화 되면서 5G 서비스에 대한 수요가 늘고 있는 가운데 3GPP LTE(Long Term Evolution) 및 밀리미터파가 적용된 NR(New Radio access technology)을 기반으로 하는 4G/5G 이동통신에서는 음영지역 해소를 위해 많은 수의 소형셀 운영이 불가피하게 되고 매크로 기지국, 소형셀, 코어망 간의 효율적인 정합을 위해 무선 백홀의 필요성이 높아지고 있다.[1] 한국전자통신연구원에서는 5G 융합서비스를 위한 20Gbps 무선백홀 기술 개발 과제인 GKWBH(Giga KOREA Wireless Back-haul)를 진행 하고 있으며 E-Band 대역에서 최대 25Gbps 의 전송율을 지원 하는 무선백홀 시스템을 개발 중에 있다.

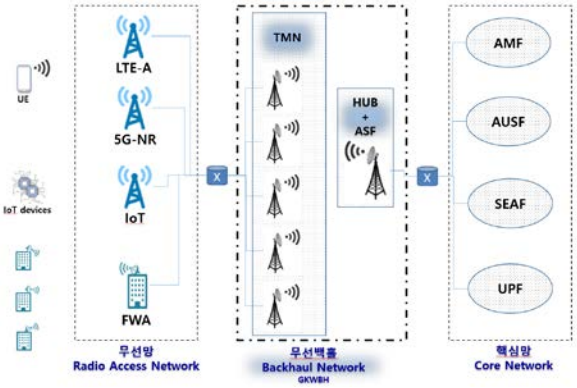

그림 1. GKWBH 네트워크 구조

본 논문에서는 GKWBH 시스템에서 보안계층의 기술 개발과 구현 구조에 대해 설명한다.

Ⅱ. 본론

GKWBH 시스템에서 고정 점대점(P2P) 및 점대다중점(P2MP) 허브와 터미널 간의 보안 계층은 상호인증 및 키 교환, 데이터 보호를 목적으로 설계하였다.

보안 계층의 기능 요소는 크게 인증 및 보안 키 교환을 위한 프로토콜 처리를 위하여 범용 프로세서 기반으로 설계된 “*보안 프로토콜 기능*”과 서브프레임 단위의 고속 처리를 위하여 FPGA 를 기반으로 설계된 “*데이터 보호 기능*” 이 있다.

GKWBH 보안 프로토콜 기능의 주요 특징은 각 TMN 인증, 각 TMN 에 대한 다중 보안키, TMN 과 HUB 간 다중 보안키 사용의 순서를 정의한 키 패턴 비트맵을 지원하는데 있다.

초기 인증 단계 혹은 키 업데이트, 정책 갱신 단계에 의해서 무결성 보호 키 IK 와 암호화 키 CK 가 결정되고, 적용할 암호화 알고리즘이 설정되면 이를 바탕으로 데이터 보호 단계가 수행된다.

GKWBH 데이터 보호 기능은 암호화 블록과 무결성 보호 블록으로 나뉜다. (그림 2 참조)

암호화 블록은 L2 MAC 계층으로 받은 MAC PDU 에 대하여 암호화를 수행하고 L1 PHY 계층에서 받은 전송블록(TB)에 대하여 복호화를 수행하며 주고받는 기본 시간단위는 subframe 단위로 한다. 무결성 보호 블록은 L3 OAM 계층에서 요구하는 OAM 메시지에 대한 무결성 보호코드 MAC-I/XMAC-I 를 생성한다.

GKWBH 시스템내에서 암호화 기능에 대한 책임은 L2 MAC 계층에 있으며 무결성 보호 기능에 대한 책임은 L3 OAM 계층에 있다.

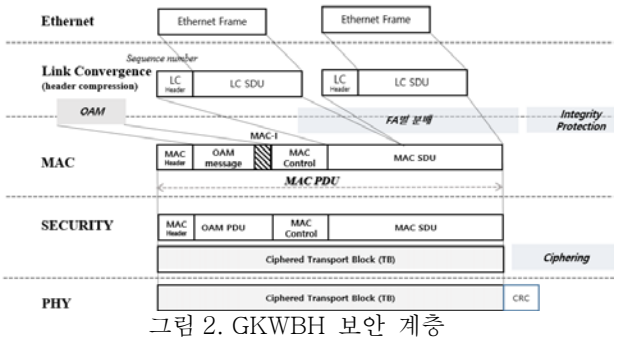

그림 2. GKWBH 보안 계층

암호화/복호화 블록은 GKWBH 시스템의 성능 지표인 25Gbps 를 만족하기 위하여 효율적인 병렬 처리가 가능한 AES-CTR 모드를 지원하는 3GPP TS 33.501 에서 명시한 128-NEA2 를 기반으로 변형하여 기본 암호화 알고리즘으로 하였으며 그 특징은 다음과 같다.

암호화/복호화 블록에 입력되는 주요 키 입력 값들은 표 1 과 같다.

CK[3]	128 bits	Cipher Key (multi key)
COUNT-C	32 bits	Ciphering sequence number - Subframe Number
DIRECTION	1 bits	Uplink(0)/Downlink(1)
LENGTH	16 bits	Length of MAC PDU - Transport Block Size(TB Size)

표 1. 암호화 블록 키 입력 값

다중 암호화 키를 지원하는 암호화 구조도는 그림 3 과 같으며 키 사용순서를 정의한 그림 3-1 의 키 패턴(KEY-PATTERN)에 따라서 다중 키(CK[3])의 순서가 재정의된다.

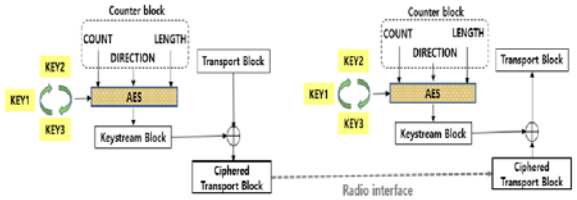

그림 3. 다중 키를 포함한 암호화 구조도

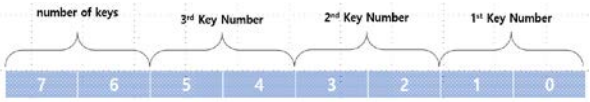

그림 3-1. 다중키를 정의한 키 패턴

그 외에 그림 4. T1 Counter Block 의 입력 값 중에서 COUNT 는 그림 5. GKWBH 의 무선프레임 에서 7.58us 주기의 1320 개의 Subframe Number 을 사용한다.

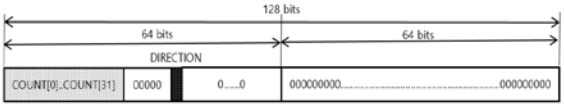

그림 4. T1 Counter Block

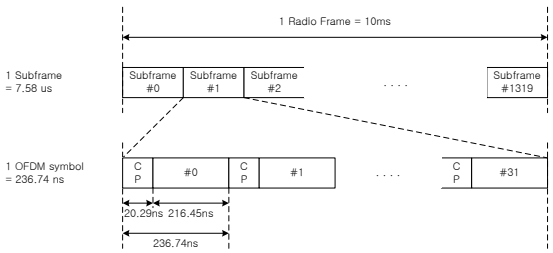

그림 5. 무선프레임 구조

그림 6. 암호화 타이밍 도는 암호화 블록에 수신된 전송블록(TB)에 대하여 GKWBH 시스템의 TTI 인 subframe 을 기준으로 128 비트로 쪼개진 N 번의 횟수만큼 시간적으로 Tn 번 암호화를 수행하게 되며 그에 따라서 키 사용 순서를 정의한 키 패턴에 따라서 다중 키가 사용되는 시간적 흐름을 설명하고 있다.

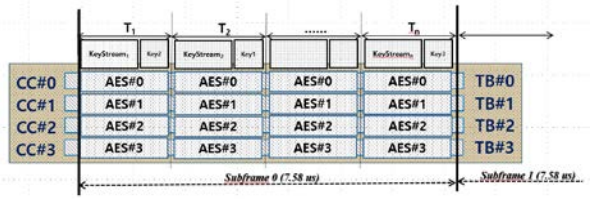

그림 6. 암호화 타이밍 도

GKWBH 시스템의 성능목표인 최대 25Gbps 의 대역폭을 지원하기 위하여 그림 7 과 같이 8 개의 전송블록(TB)을 동시에 지원하도록 GKWBH 암호화 모듈(WBHEA)을 구성하였다.

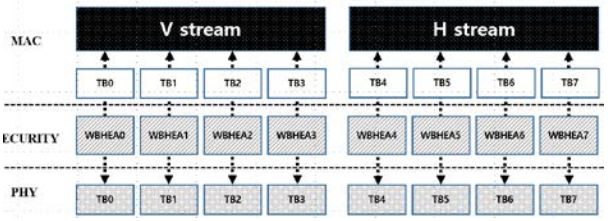

그림 7. GKWBH 암호화 인터페이스

무결성 보호 블록은 AES-128-CMAC(Cipher-based MAC) 알고리즘을 명시하는 128-NIA2 를 기반으로 변형하여 기본 무결성 보호 알고리즘으로 하였으며 그 특징은 다음과 같다.

무결성 보호 블록에 입력되는 주요 키 입력 값들은 암호화 블록과 같으며 LENGTH 는 보호의 주체인 L3 OAM PDU 에 따른다.

GKWBH 무결성보호 알고리즘인 WBHIA 는 OAM 메시지 중 Tail 32 비트를 예약한다.

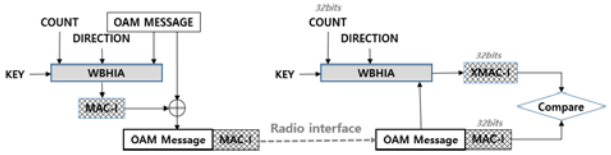

그림 8. GKWBH 무결성 보호 기본구조

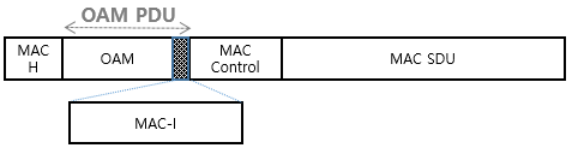

그림 9. GKWBH 무결성 보호 코드의 위치

Ⅲ. 결론

본 논문에서는 무선백홀 시스템에서 보안계층의 구조와 그 구현에 대하여 설명하였다. 최대 25Gbps 의 고속 전송 속도를 처리하기 위한 암호화 모듈의 구조 및 무선백홀 환경에서 도/감청 보호를 위한 키순서 패턴에 의한 다중 키 사용 및 subframe 에 기반한 Counter Block 등을 통하여 향상된 데이터 보호를 제공하리라 판단된다. 향후 5G-AutoDrive 및 5G-Mdedia 실증 사업과의 연계 시연이 예정되어 있어 5G 무선백홀의 광범위한 활용이 기대 된다.

ACKNOWLEDGMENT

이 논문은 2020 년도 정부(과학기술정보통신부)의 재원으로 '범부처 Giga KOREA 사업'의 지원을 받아 수행된 연구임(No.GK20N0600, 5G 융합서비스를 위한 20Gbps P2MP 무선백홀 기술 개발)

참 고 문 헌

[1] X. Ge, H. Cheng, M. Guizani, and T. Han, "5G Wireless Backhaul Networks: Challenges and Research Advances," IEEE Network, Nov. 2014, pp. 6-11