LR-WPAN을 제어하기 위한 WLAN에서의 보안 매커니즘 설계

이재원° 홍충선
경희대학교 컴퓨터공학과
jwlee@networking.khu.ac.kr°, cshong@khu.ac.kr

A Design of Security Mechanism to control LR-WPAN in WLAN

Jae Won Lee° , Choong Seon Hong
Dept. of Computer Engineering , Kyung Hee University Graduate School

요 약

저렴한 비용, 매우 작은 파워 소비와 낮은 데이터 전송속도를 지원 하는 IEEE 802.15.4 LR-WPAN (Wireless Personal Area Network) 기술은 앞으로 다가올 유비쿼터스 시대의 핵심이라고 할 수 있다. 도래할 유비쿼터스 시대에는 댁내에 LR-WPAN 기술을 적용한 다양한 상품이 보급될 것이다. 그러나 LR-WPAN은 매우 낮은 전력 소비를 위해 네트워크 기능을 최소화 하였기 때문에 응용에 있어 LAN 또는 WLAN(Wireless Local Area Network)등 기존 네트워크와의 통신 및 보안이 아직 고려되지 않아 보완이 필요하다. 본 논문에서는 WLAN의 Station이 LR-WPAN을 보안적으로 안전하게 제어할 수 있도록 AP(Acess Point)와 WLAN의 Station 그리고 LR-WPAN의 PAN Coodinator 간의 새로운 Message와 Function를 정의하고, 다른 두 네트워크간의 효율적이고 보안이 유지되는 프레임 프로세싱 매커니즘을 제안한다.

1. 서 론

앞으로 다가 올 유비쿼터스 시대에는 RFID를 비롯하여 센서 기술을 응용한 홈네트워크 산업이 확산되어 눈부신 성장을 할 것이다. 한 예로, IEEE 802.15.4 LR-WPAN[3]을 이용한 ZigBee[5]를 들 수 있는데 가정에서 스위치와 형광등이 ZigBee 디바이스가 되어 무선으로 제어가 가능하며 온도 및 습도를 감지하여 그에 따른 홈 가전제품을 제어하는 등 그 활용도가 무궁무진하다.

그러나 LR-WPAN은 매우 낮은 전력 소비를 위해 네트워크의 기능을 최소화하였기 때문에 LR-WPAN 영역 안에서만 앞서 언급한 다양한 활용이 가능하며 다른 네트워크를 통한 활용은 고려하지 않았다.

따라서 본 연구는 기존의 네트워크와의 호환이라는 사항을 해결하기 위해 WLAN의 AP(Access Point)에 Gateway 역할을 부여하고, 서로 다른 네트워크의 가장 큰 차이점인 Address 크기를 해결하기 위해 해쉬함수를 이용한 AMT(Address Mapping Table)을 구성한다. 또한 서로 다른 네트워크의 통신에 있어 보안을 유지 하기 위해 각 네트워크의 AES-CCM[4]이라는 공통적인 Cipher Suite를 이용 암호화 및 복호화를 수행한다. 이를 위해 AP는 Pairwise Key를 생성하여 부여한다. 그리고 WLAN의 Station이 LR-WPAN을 보안적으로 안전하게 제어할 수 있도록 AP와 Station 그리고 PAN Coodinator 간의 새로운 Message와 Function을 정의하고, 다른 두 네트워크간의 효율적이고 보안이 유지되는 Frame Processing 매커니즘을 제안한다.

2. WLAN과 LR-WPAN의 프레임 컨트롤, 어드레싱, 암호화 기능

This work was supported by MIC

서론에서 제안한 매커니즘에 있어 필요한 각 네트워크의 프레임 포멧 중 프레임 컨트롤 필드를 비교해 보면, 그림 1과 그림 2와 같다.

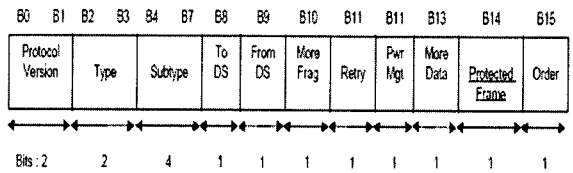

그림 1. IEEE 802.11i의 프레임 컨트롤 필드

Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame type	Security enabled	Frame pending	Ack. request	Intra-PAN	Reserved	Dest. addressing mode	Reserved	Source addressing mode

그림 2. IEEE 802.15.4의 프레임 컨트롤 필드

그림 1의 Type와 Subtype 및 그림 2의 FrameType는 새로운 Message와 Function을 정의하기 위해 필요한데 이는 3.3절과 3.4절에서 구체적으로 서술되어있다.

다음으로 IEEE 802.11의 Address는 6 octet이고 IEEE 802.15.4의 Address는 8 octet으로 크기가 다른데 본 논문에서는 해쉬함수를 이용한 AMT(Address Mapping Table)을 통하여 해결하고 이는 3.2절에 구체적으로 서술되어 있다.

또한 같은 무선 환경이라는 공통점이외에도 보안이 유지되는 통신을 위해 필요한 암호화 Key 및 암호화 알고리즘(Cipher Suite)이 공통적으로 존재하여 다른 네트워크간의 보안유지에 효율적으로 접근할 수 있다. IEEE 802.11에서 보안적인 취약점을 개선한 IEEE 802.11i[2]에서는 Cipher suite으로 TKIP와

CCMP를 제안하였는데 이중 CCMP는 128bit 암호화 Key를 가지며 암호화 알고리즘으로 AES-CCM[4]을 사용한다. 마찬가지로 IEEE 802.15.4 에서도 여러 Cipher suite중 AES-CCM을 사용하며 128bit 암호화 Key를 사용한다. 따라서 다른 두 네트워크간 동일한 키(Piarwise Key)를 전송해 준다면 보안을 유지할 수 있다.

3. 제 안 사 항

2절에서 언급하였듯이 WLAN의 Station이 LR-WPAN을 보안적으로 안전하게 제어하기 위해서는 서로 다른 네트워크의 상이함을 해결하고 기존에는 정의하지 않았던 새로운 Message와 Function이 정의되어야 하고 Frame Processing 매커니즘이 필요하다.

3.1 Architecture 및 Mechanism

WLAN의 Station으로부터 받은 LR-WPAN 제어 메시지를 효율적으로 처리하고 PANCoodinator로 전송하기위해 AP에 WLPAN Management Entity(그림 3)를 추가하였는데 이는 WLAN과 LR-WPAN의 서로 다른 네트워크간의 통신 및 보안의 처리를 담당한다.

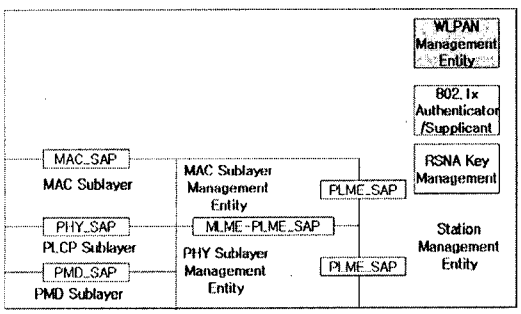

그림 3. Proposed Architecture

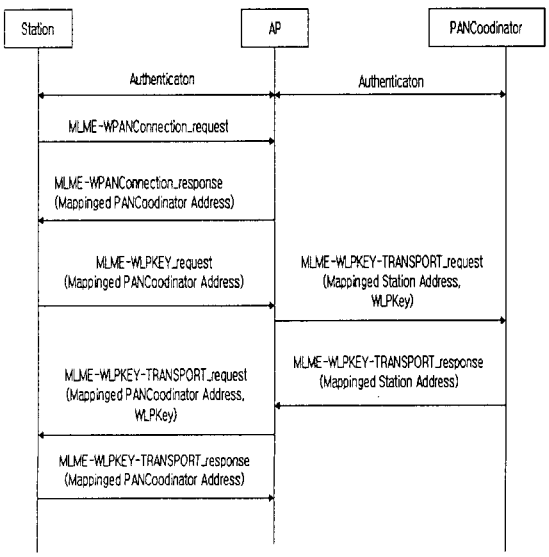

그림 4. Proposed Mechanism

또한 그림 4에서와 같이 WLAN의 Station 및 AP 그리고 LR-WPAN의 PAN Coodinator 간의 전체적인 매카니즘을 새로 정의 하였다.

다른 네트워크간 인증절차가 끝나고 Station은 AP에게 제어할 수 있는 LR-WPAN이 있는지 질의 하게 되고 AP는 연결된 LR-WPAN이 있다면 PANCoodinator의 주소를 Station에게 전송하여 준다. 이 때 다른 사이즈의 주소 해결은 3.2절에서 설명한다. 그리고 나서 Station은 보안적으로 안전하게 LR-WPAN을 제어하기 위해 AP에게 Pairwise Key를 요청한다. AP는 Station과 PAN Coodinator에게 분배할 키를 생성하고 이를 각각 전송한다. 이로써 Stantion은 AP를 통해 WPAN을 보안적으로 안전하게 제어할 수 있게된다.

3.2 AMT(Address Mapping Table)

IEEE 802.11과 IEEE 802.15.4의 Address 크기가 다르므로 8 octet의 IEEE 802.15.4의 Address를 6 octet의 IEEE 802.11의 Address로 만들기 위해 해쉬함수를 이용한다. 해쉬함수는 HMAC-SHA-1을 이용하며 Address를 생성한다음 표 1과 같이 AMT에 저장한다.

표 1. AMT(Address Mapping Table)

	WLAN Address	WPAN Address
WPAN Coodinator	0xC6A5F884EE8D	0xC0C1C2C3 C4C5C6C7
...	...	...

3.3 WLAN에서의 추가적인 Message와 Function

본 논문에서 제안하는 사항은 2절에서 설명한 그림 1에서 Frame Contol의 Type와 Subtype의 기존에 정의 되지 않은 reserved값을 이용해 추가적인 Message와 Fuction을 정의한다.(표 2)

표 2. Proposed Message

Type	Sub Type	Message
11	0000	MLME-WPANConnection_request
11	0001	MLME-WPANConnection_request
11	0010	MLME-WLPKEY_request
11	0011	MLME-WLPKEY-TRANSPORT_request
11	0100	MLME-WLPKEY-TRANSPORT_response
11	0101	MLME-WLPAN-COMMAND_request
11	0110	MLME-WLPAN-COMMAND_response

MLME-WPANConnection_request는 Station이 AP에게 제어할 수 있는 WPAN이 있는지 질의 하기 위한 Message이며 AP는 연결된 WPAN이 있다면 AMT(Address Mapping Table)을 검색하여 매핑된 Address를 Station에게 MLME-WPANConnection_response를 통해 전송하고 연결된 LR-WPAN이 없다면 연결된 LR-WPAN이 없다는 에러메시지를 전송한다.

MLME-WLPKEY_request는 Station이 AP에게 LR-WPAN을

제어하기 위한 가장 기본적인 절차로 Pairwise Key를 분배해줄 것을 요청하는 Message이며 AP는 Pairwise Key를 생성하고 Stantion과 PAN Coodinator에게 각각 MLME-WLPKEY-TRANSPORT_request message를 통해 전송한다.

Pairwise Key를 전송받은 Station과 PAN Coodinator는 MLME-WLPKEY-TRANSPORT_response 메시지를 통해 Pairwise Key를 성공적으로 수신했음을 응답한다.

Station이 LR-WPAN을 제어하는 것은 COMMAND message를 AP에게 전송하는 것으로 이루어 지는데 MLME-WLPANCOMMAND_request Message를 전송하고 Station과 PAN Coodinator는 성공적으로 COMMAND를 처리했음을 MLME-WLPANCOMMAND_response message를 통해 응답한다.

3.4 LR-WPAN에서의 추가적인 Message와 Function

본 논문에서 제안하는 사항은 2절에서 설명한 그림 2에서 Frame Contol의 Frame Type의 기존에 정의 되지 않은 reserved값을 이용해 추가적인 Message와 Fuction을 정의한다.(표 3)

표 3. Proposed Message

Frame Type	Message
100	MLME-WLPKEY-TRANSPORT_request
101	MLME-WLPKEY-TRANSPORT_response
110	MLME-WLPANCOMMAND_request
111	MLME-WLPANCOMMAND_response

이 중 COMMAND Message를 전송하는 절차는 그림 5를 통해 알 수 있다.

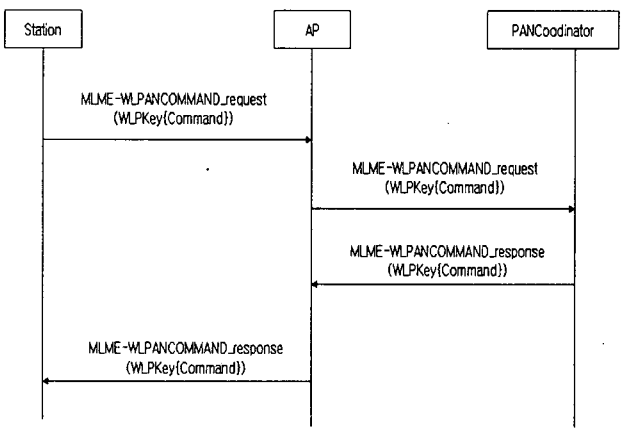

그림 5. COMMAND Message 전송 절차

4. 결 론

IEEE 802.15.4 Wireless PAN은 저전력 소비의 목적을 달성하기 위하여 네트워크의 기능을 최소화하여 설계되어 스마트홈 기술 및 미래 유비쿼터스 환경과의 융합등 무궁무진한 응용에도 불구하고 기존 네트워크와의 호환이 되지 않는다.

본 논문에서는 이러한 문제점을 IEEE 802.11 Wireless LAN과 Wireless PAN의 통신에 있어 보안을 유지 하고 효율적으로 제어할 수 있도록 제안하였다. 이를 위해 각 네트워크에 추가적으로 Message와 Fuction을 부여하고 Gateway의 역할을 할 Access Point에 AMT(Address Mapping Table)과 Frame Processing 매커니즘을 설계하였다.

따라서 가정에 WLAN이 구축되어 있고 LR-WPAN으로 구성된 조명 시스템이 있다면 제안한 매커니즘을 통해 WLAN의 Stantion인 Laptop으로도 AP(Access Point)를 통해 LR-WPAN의 조명 시스템중 스위치라고 할 수 있는 PAN Coodinator를 제어하여 형광등의 불을 켜고 끄는 등의 제어가 가능하다.

그리고 향후 WLAN을 이용한 LR-WPAN 제어에 있어 세부 COMMAND Message 정의와 더욱 효율적인 Address Mapping기술과 보다 안전한 암호화 기능을 위한 개선이 필요하다.

나아가 WLAN이 아닌 기존 LAN을 통한 LR-WPAN의 제어하기 위한 Gateway의 설계도 필요할 것이다.

참 고 문 헌

[1] ANSI/IEEE Std 802.11, 1999 Edition Part 11:Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications

[2] IEEE Std 802.11i™-2004, Part 11:Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications Amendment 6: Medium Access Control(MAC) Security Enhancements

[3] IEEE Std 802.15.4™-2003, Part 15.4: Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specfications for Low-Rate Wireless Personal Area Networks(LR-WPANs)

[4] NIST FIPS Pub 197: Advanced Encryption Standard (AES), Federeal Information Processing Standards Publication 197, U.S. Department of Commerce/N.I.S.T., November 2001

[5] Http://www.zigbee.org