편재형 센서 네트워크에서의 802.15.4 보안 연구

조승환[O] 박승민
한국전자통신연구원 편재형컴퓨팅미들웨어 연구팀
{hongcha[O], minpark }@etri.re.kr

A study of 802.15.4 security in ubiquitous sensor network

SeungHwan Jo[0] Seungmin Park
Ubiquitous Computing Middleware Research Team, ETRI

요 약

편재형 컴퓨팅 환경에서는 수많은 기기들이 유무선으로 연결되어 통신을 하기 때문에 항상 정보유출의 위험성을 가지고 있다. 특히 무선에서는 누구나 도청할 수 있기 때문에 개인의 정보보호나 네트워크상의 중요한 정보에 대한 보안이 반드시 필요하다. 하지만 소형의 센서들이 이루는 네트워크는 디바이스가 저전력, 저자원으로 컴퓨팅이 이루어지기 때문에 기존 네트워크에서의 보안과 다른 고려사항을 가진다. 이 논문에서는 센서를 위한 무선통신 인터페이스로 주목받는 802.15.4에서의 보안 메커니즘을 살펴보고 편재형 컴퓨팅 환경에서 고려해야 할 보안 사항을 고찰해본다.

1. 서 론

언제 어디서나 어떤 디바이스로나 통신을 하여 필요한 컴퓨팅 환경을 구성하거나 필요한 정보를 수집할 수 있는 편재형 컴퓨팅 환경에 관한 많은 요소 기술들이 연구 되고 있다. 이 때 주변환경을 감지하고 상황에 따라 특정한 동작을 취할 수 있는 센서는 편재형 컴퓨팅 혹은 유비쿼터스 환경을 구성하는 가장 기본적인 단위이다.

과거의 센서들은 적외선 감지나 화재감지기 같이 주로 하나의 정보를 센싱하여 일방적으로 보고하는 단순한 센서 였으나 현재 연구되고 만들어지는 센서들은 여러 개의 센서와 액츄에이터를 가지고 있고 이것들을 운영하는 운영체제를 가지고 있기도 하며 각각이 독립적으로 운영되던 과거의 형태와 달리 센서끼리 모여 스스로 네트워크를 구성하여 서로의 정보를 교환하거나 네트워크 스스로 판단을 하여 상황에 맞는 대처를 하는 지능적, 자동설정, 자동회복등의 특성을 지닌다.

이러한 센서 네트워크의 응용 분야로는 지능형 빌딩내의 환경 제어, 생산 공정 자동 제어, 창고 물류 관리, 병원에서의 물품 정보 관리 및 환자 상태 원격 감지, 지능형 교통 시스템, 텔레매틱스 등 그 범위가 광범위하다.[1]

이와 같은 편재형 컴퓨팅 환경에서는 제한된 디바이스의 자원을 이용하여 서로 통신을 하여야 하기 때문에 저전력이어야 하고 또 작고 수많은 센서들이 결합하여 네트워크를 구성하기 때문에 능동적인 네트워크 구성과 관리가 가능한 프로토콜이 필요하다. 이에 더하여 다양한 센서 네트워크의 활용과 주고 받는 정보의 성질에 따라 접근 제한 및 보안이 필수적 요소가 되고 있다.

IEEE 802.15.4에서는 저비용, 저전력 센서를 위한 저속의 데이터 전송 프로토콜 제정 작업을 하고 있으며 표준안에 보안을 위해 필요한 요소들을 정의하고 있다. 현재는 draft18까지 나온 상태이다.

이 논문에서는 2장에서 802.15.4에서 정의하는 PHY계층과 MAC계층을 살펴보고 3장에서 MAC sublayer에서의 보안 서비스에 대해 살펴보고 편재형 센서 네트워크를 위한 요소 기술들을 살펴본다.

2. 802.15.4 LR(Low Rate)-WPAN

IEEE 802.15 의 TG4는 국제적으로 사용상 라이센스 제약이 없는 주파수 대역에서 통신을 하며 수개월에서 수년의 수명을 가지는 저 전력소모, 저 비용, 저 전송량 등의 조건을 만족시키는 무선 개인 영역 네트워크(WPAN)를 위한 표준을 제정하고 있으며 물리계층과 MAC계층을 정의하여 거의 마무리 단계에 있다.

이 표준에서의 특징을 정리하면 표 1과 같다.

표 1. IEEE 802.15.4 LR-WPAN의 특징[2]

전송률	250kb/s - 2.4GHz 40kb/s - 915MHz 20kb/s - 868MHz
Network topology	Star, peer-to-peer 네트워크당 255개 디바이스
채널 접근 메커니즘	CSMA-CA
범위	10m (1~100m 세팅가능)
채널	16채널 - 2.4GHz 10채널 - 915MHz 1채널 - 868MHz
주소할당	16bit short address 64bit IEEE address
신뢰성	Fully ACK 프로토콜
에너지관리	저전력소모, 에너지 detection

LR-WPAN 네트워크에 참가하는 디바이스는 FFD(Full function device)와 RFD(Reduced function device) 두 가지 종류로 나눌 수 있다. FFD는 PAN coordinator, coordinator, 디바이스로 동작할 수 있으며 RFD나 다른 FFD와 통신 할 수 있다. 반면 RFD는 FFD와만 통신할 수 있다. RFD는 조명스위치 같은 아주 단순한 애플리케이션을 동작시키기 위해 최소한의 자원과 메모리를 사용하여 구현되는 디바이스이다.[2]

LR-WPAN 디바이스는 저 수준의 제어 메커니즘을 가지고 있는 RF 트랜시버를 포함하는 물리계층과 모든 형태의 전송에 대해 물리적 채널에 접근을 제공해주는 MAC sublayer로 구성된다. 네트워크 구성, 메시지 라우팅 등에 관한 네트워크계층이나 디바이스에 특정 기능을 제공해주는 애플리케이션 계층등은 802.15.4에서 다루고 있지 않다.

3. 802.15.4에서의 보안 메커니즘

MAC sublayer는 상위계층에 의해 요구되어 들어오고 나가는 프레임에 대해 접근제한, 데이터 기밀성, 프레임 무결성, sequential freshness등의 보안 서비스를 제공해 준다. 또 802.15.4프로토콜은 다음과 같은 세가지 보안 모드를 가진다.

- unsecured mode: 기본 보안모드로 MAC sublayer는 어떠한 보안 서비스도 제공하지 않는다
- ACL mode: 상위계층에 대해 ACL(Access Control List)에 속해있는 디바이스로부터 온 것인지 판별하여 필터링만 하며 프레임에 대한 변형이나 보안 서비스를 제공하지는 않음
- Secured mode: MAC계층에서 ACL기능과 들어오고 나가는 프레임에 대한 보안 서비스를 제공한다

디바이스가 secured mode로 운영될 때에는 security suite를 사용한다. Security suite는 MAC프레임에 대해 수행되는 보안 서비스모임 목록이다. 이 표준에서는 보안이 구현되는 디바이드들은 AES 블록암호를 사용하도록 하며 AES-CCM-64 security suite를 반드시 지원하고 이외의 suite를 추가적으로 지원 할 수 있게 하고 있다.

표 2. Security suite 리스트[2]

ID	명칭	보안 서비스			
		접근제한	데이터 기밀성	프레임 무결성	Sequential freshness
0x01	AES-CTR	O	O		O
0x02	AES-CCM-128	O	O	O	O
0x03	AES-CCM-64	O	O	O	O
0x04	AES-CCM-32	O	O	O	O
0x05	AES-CBC-MAC-128	O		O	
0x06	AES-CBC-MAC-64	O		O	
0x07	AES-CBC-MAC-32	O		O	

기본으로 지원해야할 CCM모드는 CTR모드의 암호화와 CBC모드의 인증을 둘 다 수행하여 기밀성과 무결성 서비스를 제공해 준다.

CTR모드는 카운터라 불리는 입력 블록의 셋을 써서 암호문을 생성하기 위해 평문과 출력블록을 XOR하는 기밀성 모드이다. 연속된 카운터들은 각각의 입력되는 블록에서 다른 값을 가져야 한다. 이것은 하나의 메시지에 한정되지 않고 주어진 키에 대해 암호화되는 모든 메시지에 대하여 다른 카운터 값을 가져야 한다. 이 주어진 카운터들에 대해 CTR모드는 다음 그림 1과 같이 수행된다.

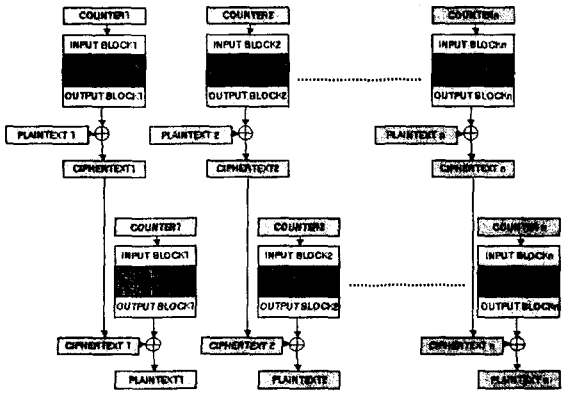

그림 1. CTR 모드[2]

그림 2에서는 위의 그림 1에 CCM모드에서 CTR모드를 사용하여 동작하는 암호화에 사용되는 입력 블록 구성과 인증을 위해 사용되는 CBC-MAC에서의 첫번째 입력 블록에 사용되는 플래그와 Nonce의 구성의 예를 보여준다.

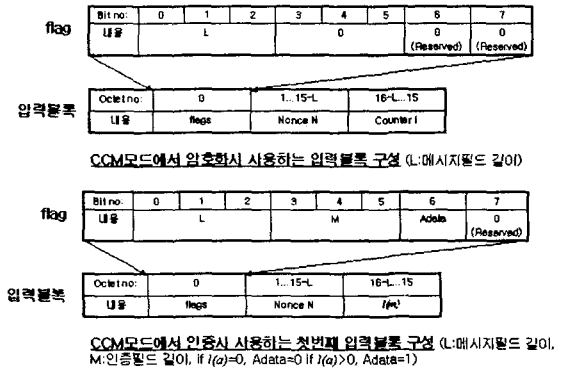

그림 2. CTR모드와 CBC-MAC을 위한 입력 블록 구성 [2]

그림 1의 CTR모드 암호화에는 카운터와 평문이 사용되는데 사용하는 카운터는 플래그와 Nonce 그리고 카운터를 연접시켜 사용한다. 인증에는 첫번째 입력 블록과 인증할 메시지가 필요한데 첫번째 입력 블록은 플래그, Nonce와 메시지 길이를 연접시켜 첫번째 입력 블록으로 사용한다.

4. 결 론

본 논문에서는 현재 편재형 환경에서의 센서 네트워크를 위한 무선 통신 인터페이스로 채택될 가능성이 큰 IEEE 802.15.4에서의 보안 사항을 살펴 보았다. IEEE 802.15.4에서는 물리계층과 MAC계층만을 정의하고 있기 때문에 보안요구 사항도 사용알고리즘과 운영모드 그리고 입력값들에 대해서만 정의하고 있다. 하지만 온전한 보안메커니즘을 위해서는 센서네트워크에서의 키분배와 관리를 포함하는 보안 프로토콜이 있어야 하나 이 부분은 ZigBee Alliance라는 단체에서 네트워크계층, 응용계층 인터페이스를 만들며 고려하고 있다.[3]

편재형 혹은 유비쿼터스 환경에서는 언제 어디서나 모든 기기들이 정보를 수집하고 제공하기 때문에 느끼지 못하는 새에 자신의 정보가 새어 나가거나 위변조,위해코드 등의 공격을 받을 수 있다. 따라서 이러한 위험으로부터 안전한 편재형 환경을 구축하기 위해서 인증과 기밀성, 무결성 서비스가 이루어져야 하고 연산능력이 적은 센서의 경우 하드웨어적 지원을 받아 이루어져야 할 것이다.

앞으로는 현재 진행된 무선센서기기를 위한 보안 기능에 덧붙여 상위계층에서 지원 되야 할 키 생성과 분배에 대한 연구를 보완하여 다른 기능의 센서망간의 통합 메커니즘 연구를 진행하려 한다.

참고 문헌

[1] 이대성 "스마트 센서의 기술 동향",전자부품,8월호, 2003

[2] IEEE 802.15.4, "Draft Standard for Part 15.4:Wireless Medium Access Control(MAC) and Physical Layer(PHY) specifications for Low Rate Wireless Personal Area Networks(LR-WPANs)" Feb. 2003

[3] http://www.zigbee.org