ZigBee 네트워크에서 효율적인 키 분배 프로토콜

한재홍*, 김상진**, 오희국*
*한양대학교 컴퓨터공학과
**한국기술교육대학교 인터넷미디어공학부
e-mail:jhhan@infosec.hanyang.ac.kr

Effective Key Agreement Protocol on ZigBee Network

Jae-Hong Han*, Sang-Jin Kim**, Hee-Kuck Oh*
*Department of Computer Science and Engineering, Han-Yang University
**School of Internet Media Engineering, Korea University of Technology and Education

요 약

LR-WPAN의 대표적인 기술인 ZigBee는 저속 전송속도를 갖는 홈오토메이션 및 데이터 네트워크를 위해 IEEE 802.15.4 표준을 기반으로 상위 프로토콜과 응용을 규격화한 기술이다. 특히 개방된 무선 환경인 ZigBee 네트워크에서는 무엇보다 보안의 중요성이 대두되고 있으며, ZigBee Alliance 규격에도 보안 계층이 포함되어 있다. 그러나 암호화에 사용되는 링크키를 생성하기 위해 신뢰성 있는 정보(마스터키)를 평문으로 전송하기 때문에 직접적으로 노출되는 위험성과 방문자 위치 추적 등 디바이스의 이동이 빈번한 환경에서 PAN 코디네이터의 과부하가 발생할 수 있는 등의 여러 가지 문제점이 존재하고 있다. 본 논문에서는 Du 등이 제안한 사전 키 분배 기법을 이용하여 ZigBee 네트워크에서의 효율적인 키 분배 프로토콜을 제안하였다. 제안된 프로토콜은 디바이스에게 임의의 행렬 열과 행 값을 송신하여 링크키를 생성함으로서 이전의 문제점을 해결하고 더욱 빠른 통신이 가능하도록 하였다.

1. 서론

최근 홈 네트워크 및 유비쿼터스에 대한 일반인들의 관심이 고조되면서 LR-WPAN(Low Rate Wireless Personal Area Network) 기술이 주목을 받고 있다. LR-WPAN은 WPAN 기술 중 20~250kbps의 낮은 전송속도를 지원하는 저전력 무선 근거리 표준 통신 기술이다. 다른 무선 통신 기술과 비교하여 저비용, 저전력을 지향하는 LR-WPAN은 센서 네트워크에 도입되기에 적합한 통신 기술로 부각되고 있다. 향후 유비쿼터스 환경에서 자율적인 센싱, 저전력 통신기능 제공 및 대량의 노드 객체들로 센서 네트워크를 구성하여 가정 및 기업, 의료 등의 여러 주요 분야에서 다양한 서비스를 제공할 수 있을 것이라 기대되고 있다[1].

LR-WPAN의 대표적인 기술인 ZigBee는 저속 전송속도를 갖는 홈오토메이션 및 데이터 네트워크를 위해 IEEE 802.15.4 표준을 기반으로 상위 프로토콜과 응용을 규격화한 기술이다. 현재 IEEE 802.15.4의 물리 계층과 MAC 계층 표준을 바탕으로 Zigbee Alliance에서의 표준화 작업을 통해 상위 계층인 네트워크 계층과 응용 계층의 ZigBee 스택을 구성하였으며 네트워크, 보안 등의 기술적 요구사항 및 동작순서 등을 정의하고 있다[2].

특히 개방된 무선 환경인 ZigBee 네트워크에서는 무엇보다 보안의 중요성이 대두되고 있으며, ZigBee Alliance 규격에도 보안 계층이 포함되어 있다. 그러나 링크키 (link key) 생성을 유도하는 마스터키 (master key)가 PAN (Personal Area Network)에 조인한 디바이스에게 전송하는 과정이 안전하지 않은 채널을 통해 전달됨으로 인해 직접적으로 노출되는 위

험이 존재한다[3]. 또한 최초 디바이스 간의 통신 시, 양 디바이스는 PAN 코디네이터를 통해 마스터키를 분배받아 상호 간의 링크키를 생성하는데, 방문자 위치 추적 등 디바이스의 이동이 빈번하고 빠른 통신이 요구되는 상황에서는 PAN 코디네이터의 과부하가 발생할 수 있다.

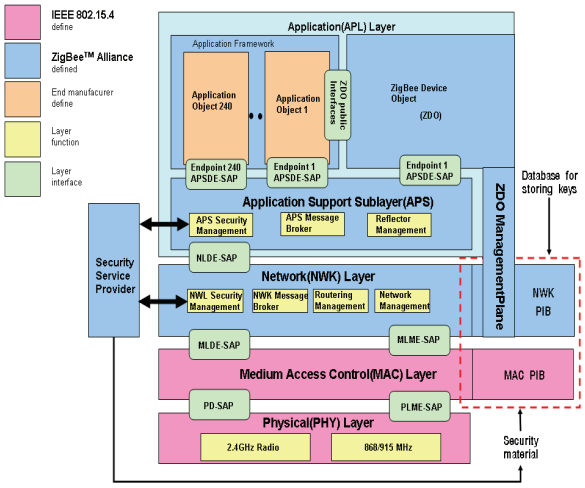
이러한 문제점을 해결하기 위하여 본 논문에서는 Du 등이 제안한 사전 키 분배 기법[4]을 이용하여 ZigBee 네트워크에서의 효율적인 키 분배 프로토콜을 제안하였다. 제안한 프로토콜은 생성을 유도하는 마스터키를 디바이스에게 직접 전송할 필요 없이 손쉽게 링크키를 생성할 수 있으며, 하나의 키로 인접된 디바이스와 모든 통신이 가능하다는 장점을 가지고 있다.

본 논문은 다음과 같다. 2장에서는 ZigBee 보안 표준화에 대한 관련연구를 알아보고, 3장에서는 본 논문에서 제안하는 프로토콜을 설명한다. 4장에서는 제안한 프로토콜을 분석하고 마지막 5장에서는 결론 및 향후과제를 정리한다.

2. 관련연구

2.1. ZigBee 보안 프로토콜 스택

ZigBee Alliance에서는 그림 1과 같이 보안 프로토콜 스택을 구성하였다.

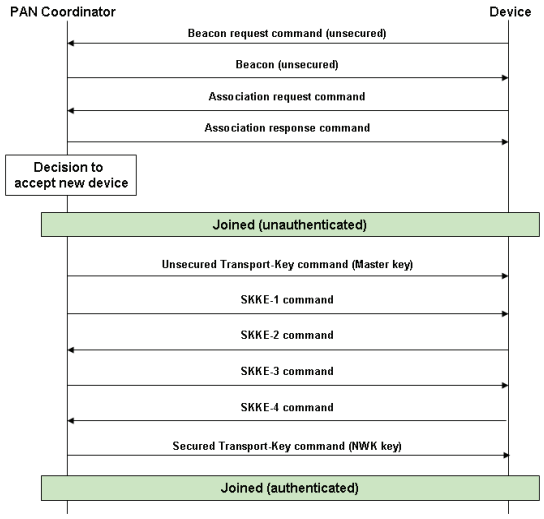


(그림 1) ZigBee 보안 프로토콜 스택 구조

보안 서비스 제공자 (Security Service Provider)는 NWK PIB (PAN Information Base)와 MAC PIB에게 Security Material 정보를 얻어와 네트워크 계층과 응용 지원 하부 계층에 보안 서비스를 제공한다. ZigBee 보안 서비스는 128-bit AES의 대칭키 암호 알고리즘을 이용하여 두 노드 간의 비밀키 설정과 상호 인증을 수행한다. 각 비밀키는 MAC 계층, 네트워크 계층, 응용 계층에서의 데이터 프레임에 대한 보안 기능을 제공하여 ZigBee 보안 메카니즘을 구성하게 된다. ZigBee는 네트워크키 (network key)와 링크키, 그리고 마스터키를 이용하여 인증 및 암호화를 수행하는데 네트워크키는 네트워크 레벨에서의 인증 및 암호화에, 링크키는 디바이스 레벨에서의 인증 및 암호화에 사용된다. 그리고 마스터키는 디바이스 간에 링크키를 유도하기 위한 신뢰성 있는 정보로, SKKE 프로토콜에서는 마스터키를 이용하여 디바이스 상호 간에 링크키를 생성하게 된다[5].

2.2. ZigBee 인증 및 키 생성 프로토콜

ZigBee 보안에서 새로운 디바이스가 PAN에게 조인하게 되면 PAN 코디네이터는 디바이스와 링크키를 생성하게 된 후, 마지막으로 네트워크키를 전송하여 디바이스를 인증하게 된다. 링크키를 생성하기 위한 마스터키는 각 디바이스에게 사전 분배하거나 네트워크에 조인한 디바이스에게 직접 전송하는 2가지 방법이 존재한다. 그림 2는 마스터키를 가지지 않은 새로운 디바이스가 PAN 코디네이터와 통신하여 PAN에 조인하는 과정을 보여준다.



(그림 2) PAN 코디네이터와 디바이스 간의 인증 및 키 생성 프로토콜

디바이스와 PAN 코디네이터가 비컨 (beacon) 신호를 주고받은 후, 디바이스는 Association request command를 보내어 PAN에 조인을 요청한다. PAN

코디네이터가 Association response command를 보내 디바이스의 조인을 허가하면 PAN 코디네이터와 디바이스 간의 인증 및 키 생성 과정을 수행하게 된다. PAN 코디네이터는 디바이스에게 마스터키를 보내주고 SKKE 프로토콜을 진행하여 링크키를 생성한 후, 마지막으로 네트워크키를 보내어 디바이스를 인증한다.

2.3. SKKE 프로토콜

SKKE 프로토콜은 initiator 디바이스와 responder 디바이스가 신뢰성 있는 정보(마스터키)를 사용하여 서로 신뢰할 수 있는 비밀키(링크키)를 유도하는 과정을 의미한다. SKKE 프로토콜은 디바이스 간에 마스터키를 공유하고 있는 상황에서 진행된다. 프로토콜의 과정은 다음과 같다.

단계 1. initiator 디바이스는 임의의 비트 스트링 SB_i를 생성하여 responder 디바이스에게 송신한다.

단계 2. responder 디바이스도 임의의 비트 스트링 SB_r을 생성하여 initiator 디바이스에게 송신한다.

단계 3. 각 디바이스는 서로 주고받은 비트 스트링과 마스터키 K_m를 이용하여 $HMAC$ 값을 산출한다. (i와 r은 각각 initiator 디바이스와 responder 디바이스의 식별자)

$$HMAC = H_{K_m}(i \| r \| SB_i \| SB_r)$$

단계 4. 산출된 $HMAC$ 값에 16진수 x_{16}을 이용하여 2개의 해쉬 값을 만든다. 각 디바이스가 만든 해쉬 값은 동일하다.

$$H_1 = H(HMAC \| 01_{16})$$

$$H_2 = H(HMAC \| 02_{16})$$

각 디바이스가 산출한 해쉬 값 중 H_2은 링크키로, H_1은 서로 간에 동일한 링크키가 생성되었는지를 확인하기 위해 사용된다.

단계 5. 각 디바이스는 다음과 같이 2개의 $MACData$ 값을 산출한다.

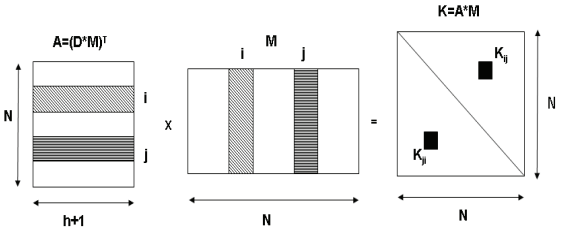
$$MACData_1 = H_{K_{H_1}}(i \| r \| SB_i \| SB_r \| 02_{16})$$

$$MACData_2 = H_{K_{H_1}}(i \| r \| SB_i \| SB_r \| 03_{16})$$

단계 6. response 디바이스는 $MACData_1$을, initiator 디바이스는 $MACData_2$을 서로 송신하여 각각의 값이 일치하면 서로 동일한 링크키를 생성한 것으로 인증하게 된다.

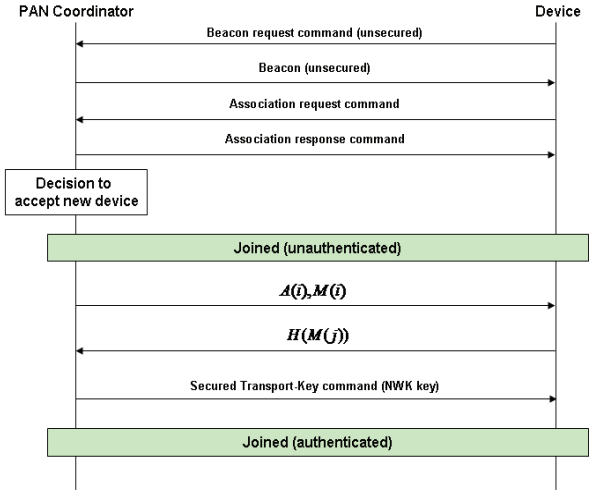
3. 제안하는 프로토콜

제안한 프로토콜은 Du 등이 제안한 사전 키 분배 기법을 ZigBee 네트워크에 적용하여 더욱 안전하고 빠른 통신환경을 제공한다. 그림 3에는 Du 등이 제안한 대칭키 생성 방식을 보여주고 있다.



(그림 3) Du 등이 제안한 대칭키 생성 방식

디바이스 간의 통신을 위해서는 PAN 코디네이터가 새롭게 조인하는 디바이스에게 키를 분배하는 과정이 필요하다. 그림 4는 PAN 코디네이터가 새롭게 조인한 디바이스에게 임의의 행렬의 열과 행 값을 송신함으로서 통신 시 링크키를 생성할 수 있도록 하는 과정을 보여주고 있다.



(그림 4) PAN 코디네이터와 디바이스의 사전 키 분배 과정

단계 1. PAN 코디네이터는 유한군 $GF(q)$에서 $(h+1)\times(h+1)$의 크기를 가진 행렬 D와 $(h+1)\times N$의 크기를 가진 또 하나의 행렬 M을 생성한다. (여기서 h는 한 네트워크에서 h개의 키 쌍이 노출되어도 그 네트워크는 안전하다는 특징을 가진다[6].) 그리고 D와 M을 곱한 후 그 결과값의 행과 열을 바꾸어 새로운 행렬 A를 계산한다.

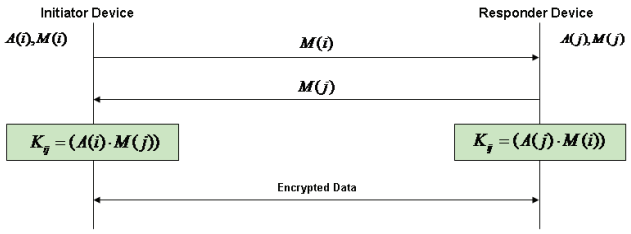
단계 2. PAN 코디네이터는 조인을 요청한 디바이스에게 임의의 행렬의 열과 행 값 $A(j), M(j)$를

송신한다.

단계 3. 디바이스는 $M(j)$를 해쉬한 $H(M(j))$ 값을 PAN 코디네이터에게 보낸다.

단계 4. PAN 코디네이터는 $H(M(j))$를 확인하여 값이 일치하면 디바이스가 정상적으로 수신했다고 인정하고 네트워크키를 보내어 디바이스를 인증하게 된다.

PAN 코디네이터에게 인증된 디바이스는 네트워크의 다른 디바이스와 링크키를 이용하여 상호 통신이 가능하게 된다. 그림 5는 initiator 디바이스와 responder 디바이스 간에 링크키를 생성하여 통신하는 과정을 보여주고 있다. initiator 디바이스와 responder 디바이스는 각각 PAN 코디네이터가 송신한 $A(i), M(i)$와 $A(j), M(j)$을 가지고 있다고 가정한다.



(그림 5) 디바이스 상호 간의 링크키 생성 과정

단계 1. initiator 디바이스는 $M(i)$을, responder 디바이스는 $M(j)$을 서로에게 송신하여 값을 교환한다.

단계 2. initiator 디바이스와 responder 디바이스는 각각 다음과 같은 방식으로 링크키를 생성한다.

$$K_{ij} = (A(i) \bullet M(j)) \text{ (initiator 디바이스)}$$

$$K_{ji} = (A(j) \bullet M(i)) \text{ (responder 디바이스)}$$

K_{ij}와 K_{ji}는 같은 값을 가지게 됨으로 initiator 디바이스와 responder 디바이스는 동일한 링크키를 이용하여 데이터를 암호화하여 통신할 수 있다.

4. 프로토콜 분석

ZigBee 인증 및 키 생성 프로토콜은 링크키를 생성하기 위한 마스터키를 평문으로 전송하여 직접적으로 노출되는 위험성이 존재하지만, 제안한 프로토콜은 임의의 행렬의 열과 행 값을 전송함으로써 디바이스 상호간에 링크키를 생성할 수 있도록 한다.

또한 제안한 프로토콜은 네트워크에 참여한 디바이스 간의 최초 통신 시 PAN 코디네이터를 통하지 않고도 링크키 생성이 가능하기 때문에, 디바이스의 이동이 빈번한 상황에서도 빠른 통신이 가능하다.

5. 결론 및 향후 과제

개방된 무선 환경인 ZigBee 네트워크에서는 무엇보다 보안이 중요한 이슈로 떠오르고 있으며, ZigBee Alliance 규격에도 보안 계층이 포함되어 있다. 하지만 링크키를 생성하기 위한 마스터키를 평문으로 전송하여 직접적으로 노출되는 위험성과 방문자 위치 추적 등 디바이스의 이동이 빈번한 환경에서는 PAN 코디네이터의 과부하가 발생할 수 있는 등의 여러 가지 문제점이 존재하고 있다. 본 논문에서는 Du 등이 제안한 사전 키 분배 기법을 이용하여 ZigBee 네트워크에서의 효율적인 키 분배 프로토콜을 제안하였다. 제안된 프로토콜은 디바이스에게 임의의 행렬의 열과 행 값을 송신하여 링크키를 생성함으로서 이전의 문제점을 해결하고 더욱 빠른 통신이 가능하도록 하였다.

하지만, 이전 프로토콜이 가지고 있는 중간자 공격의 위험성, 그리고 PAN 코디네이터와 디바이스 간의 인증문제는 아직까지 해결해야할 부분으로 남아있기 때문에, 앞으로 ZigBee 보안에 대한 연구가 더욱 필요할 것이라 생각된다.

참고문헌

[1] 김진태, 이훈, 황대환, 김봉태, “저속, 저가, 저전력 무선 PAN 표준 개발동향,” 전자통신동향분석, 제 18권, 제 2호, pp. 37-44, 2003년 4월.

[2] B. Heile, "ZigBee Alliance Tutorial", Nov. 2005.

[3] 김신효, 강유성, 정병호, 정교일, “u-센서 네트워크 보안 기술 동향,” 전자통신동향분석, 제 20권, 제 1호, pp. 93-99, 2005년 2월.

[4] W. Du, J. Deng, Y. S. Han, P. K. Varshney, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks," CCS '03, pp. 42-51, Oct. 2003.

[5] Zigbee Alliance, "ZigBee 1.0 Security Specification," Dec. 2004.

[6] R. Blom, "An Optimal Class of Symmetric Key Generation Systems," Advances in Cryptology: Proceedings of EUROCRYPT 84, Lecture Notes in Computer Science, pp. 335-338, 1985.