# ZigBee 망에서의 효율적인 단대단 키 설정 기술

김현주, 정종문*
연세대학교 전기전자공학부 통신·네트워크 연구실
e-mail : *hjkim91@yonsei.ac.kr, jmc@yonsei.ac.kr*

# Efficient End-to-End Key Establishment Scheme in ZigBee Networks

Hyunjue Kim, Jong-Moon Chung*
Communication & Networking Laboratory
School of Electrical and Electronic Engineering
Yonsei University

## Abstract

To achieve secure communication in current ZigBee networks, encrypted messages using security keys need to be shared among devices. A link key shared by two devices is used for unicast communications, where the master key is the starting point for establishing a link key. The ZigBee protocol has some limitations in end-to-end key establishment, which are discussed and an improved end-to-end key establishment scheme is presented.

## I. 서론

최근 홈 네트워크 및 유비쿼터스 통신에 대한 관심이 증가하면서 단거리에서 사용하는 WPAN(wireless personal area network) 기술이 주목받고 있다. WPAN의 대표적인 기술로는 ZigBee, UWB(ultra wideband), Bluetooth 등이 있는데, 이들 기술 중 특히 ZigBee[1]는 초저가의 무선 센서 네트워크를 구현하는 데에 최적의 방안을 제공하고 있는 기술로 주목받고 있다. 그러나 ZigBee 시스템은 코디네이터(coordinator)가 네트워크상의 디바이스들의 비밀키인 마스터키(master key)를 관리 및 분배한다. 그러므로 링크키(link key)를 생성하여 디바이스간의 단대단(end-to-end) 보안을 가능하도록 하기위해서는 코디네이터가 해당 디바이스들에게 마스터키를 직접 전송해야 하는 구조적인 약점을 가지고 있다. 본 논문에서는, ZigBee에서의 단대단 키 설정 방법을 소개 및 분석하고, 분석한 문제점들을 개선한 새로운 단대단 키 설정 방법을 제안한다.

## II. ZigBee 키 설정 분석

그림 1은 initiator 디바이스와 responder 디바이스가 마스터키를 사용하여 링크키를 유도하는 과정을 나타낸 것이다. 이 때, 링크키를 생성하기 위해, ZigBee는 SKKE 프로토콜을 사용한다.

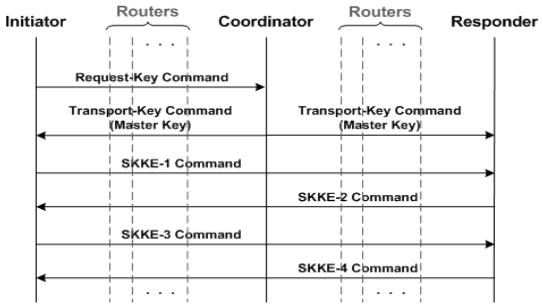


그림 1. ZigBee에서의 단대단 키 설정 과정

그러나 ZigBee는 그림 1에서와 같이 initiator 디바이

* 교신저자, 연세대학교 전기전자공학부 부교수
본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-C1090-0801-0038)

스는 responder 디바이스와의 링크키를 생성하기에 앞서, 두 디바이스간의 마스터키 분배과정이 먼저 수행되어야 한다. 즉, 코디네이터에게 두 디바이스간의 마스터키를 요청해야 하고 요청을 받은 코디네이터는 해당 디바이스들(initiator 디바이스와 responder 디바이스)에게 사전에 생성된 각 디바이스와의 링크키를 사용하여 마스터키를 안전하게 전송해야하는 과정이 추가로 수행되어야 하는데, 이는 네트워크 성능의 심각한 문제점들을 야기한다. 만약 마스터키를 요청하는 디바이스 수가 많아진다면 코디네이터에 부하가 치중되어 통신시간이 지연되고, 만약 홉(hop)수가 많다면 여러 라우터를 지나야 하기 때문에 통신시간이 길어져 네트워크 시스템의 성능이 저하되는 문제점이 있다.

또한 ZigBee 시스템에서는 코디네이터가 네트워크상의 모든 디바이스와의 마스터키와 링크키뿐만 아니라, 단대단 통신을 하는 각 디바이스간의 마스터키까지 전부 가지고 있어야만 한다. 그렇게 때문에 네트워크상의 디바이스 수가 증가할수록 이에 비례하여 더 많은 저장 공간이 요구되는 키 관리상의 구조적 단점이 존재한다.

## Ⅲ. 제안하는 ZigBee 키 설정

그림 2는 2장에서 분석한 ZigBee 네트워크의 문제점들을 개선한 새로운 단대단 키 설정 과정을 나타낸 것이다. 프로토콜의 초기화에서, 코디네이터 $C$는 자신의 비밀키 $s \in Z_p$와 IP주소와 같은 디바이스의 고유주소나 고유번호를 이용하여 각 디바이스 $i$의 비밀키 $K_{S_i} = sH_1(IP_i) \in G_1$를 계산한다. 이때, 각 디바이스의 비밀키는 제작 단계에서 저장되거나 사용자가 직접 입력하는 등의 안전한 방법을 이용해 저장되고, 각 디바이스 $i$의 공개키는 $K_{P_i} = H_1(IP_i) \in G_1$이다. 시스템 파라미터는 $param = < G_1, G_2, e, p, P, H_1, H_2 >$이다. 여기서 $G_1$과 $G_2$는 각각 소수 $p$를 위수로 갖는 덧셈군과 곱셈군이고, $P \in G_1$는 $G_1$의 생성원(generator), $e : G_1 \times G_1 \rightarrow G_2$는 겹선형 함수, $H_1 : \{0,1\}^* \rightarrow G_1$과 $H_2 : G_2 \rightarrow Z_p$는 암호학적 해쉬함수들이다[2~4].

제안하는 방법에서는 SKKE 프로토콜 실행 전에 먼저 수행되어야 했었던 추가 과정, 즉, initiator 디바이스가 코디네이터에게 responder 디바이스와의 마스터키를 요청하고 요청을 받은 코디네이터는 해당 디바이스들(initiator 디바이스와 responder 디바이스)에게 사전에 생성된 각 디바이스와의 링크키를 사용하여 마스터키를 안전하게 전송하는 과정을 제거하여 단대단 키 설정과정을 간단히 하였다. 제안하는 방법은 코디네이터로 부터의 별도의 마스터키 전송과정이 필요 없이 initiator 디바이스 $I$와 responder 디바이스 $R$은 각각 그들 사이의 마스터키 $MK_{IR} \in Z_p$를 (1)과 (2)와 같이 직접 생성할 수 있는 새롭고 효율적인 방법이다.

$$I : MK_{IR} = H_2(e(K_{S_I}, K_{P_R})) = H_2(e(K_{P_I}, K_{P_R})^s) \quad (1)$$

$$R : MK_{IR} = H_2(e(K_{P_I}, K_{S_R})) = H_2(e(K_{P_I}, K_{P_R})^s) \quad (2)$$

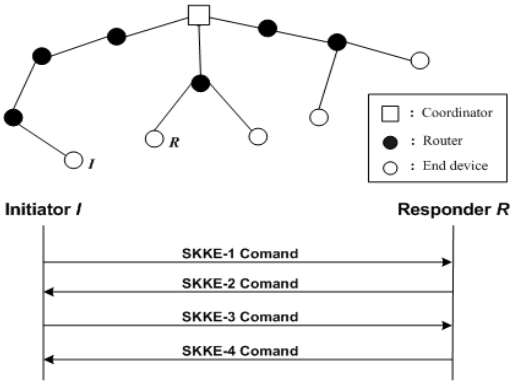


그림 2. 제안하는 단대단 키 설정 과정

## Ⅳ. 결론 및 향후 연구 방향

제안한 방법은 마스터키의 요청 및 전송과정을 제거하여 통신횟수를 감소시키고 코디네이터로 집중되었던 트래픽을 분산시킴으로써 네트워크의 부하를 해결하고 네트워크의 효율성을 향상시켰다. 또한 코디네이터가 자신의 비밀키와 자신과 직접 연결된 노드간의 링크키만 관리하도록 함으로써 코디네이터의 키 관리를 간편화하였다. 따라서 제안하는 방식은 멀티홉(multi-hop) 환경에 적용될 경우에 더욱 더 효율적인 방식이다.

## 참고문헌

[1] ZigBee Alliance, "ZigBee Specification," Technical Report Document 053474r06, Version 1.0, ZigBee Alliance, 2005.

[2] A. Shamir, "Identity-based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology, Crypto'84, Springer-Verlag, LNCS 196, pp. 47~53, 1985.

[3] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Advances in Cryptology, Crypto 2001, Springer-Verlag, LNCS 2139, pp. 213~229, Aug. 2001.

[4] M. C. Gorantla, R. Gangishetti, and A. Saxena, "A Survey on ID-Based Cryptographic Primitives," Cryptology ePrint Archive, Report 2004/131, available at iacr.org/2005/094/.