논문 2006-43TC-10-5

ZigBee 센서네트워크에서 효율적인 Parent - Child 키 연결 알고리즘

(Effective Parent-Child Key Establishment Algorithm used ZigBee Sensor Network)

서 대 열*, 김 진 철****, 김 경 목**, 오 영 환***

(Dae-youl Seo, Jin-chul Kim, Kyoung-Mok Kim, and Young-Hwan Oh)

요 약

ZigBee 보안에서 네트워크 키나 링크키의 전달 및 상호 인증은 ZigBee Alliance 규격에 포함되어 있으나, 마스터키를 안전하게 각 노드에 전달하기 위한 방법을 제공하지는 않는다. 마스터키를 전송하는 과정이 안전하지 않은 채널을 통해서 전달하기 때문에 마스터키가 직접적으로 노출되는 단점을 가지고 있다. 또한 ZigBee Alliance에서는 보안에서 가장 핵심인 trust center 역할을 코디네이터가 하도록 정의하고 있다. 새롭게 PAN에 조인하는 디바이스마다 코디네이터와 키 연결을 해야 하기 때문에 코디네이터는 부하가 집중되고, 악의 있는 디바이스에게 직접적으로 위험에 노출되는 단점이 있다. 몇 개의 디바이스만 키 연결을 할 때는 문제가 되지 않지만 네트워크가 거대해지면 코디네이터에서 발생하는 트래픽 양이 증가하면서 코디네이터의 부하가 증가하게 된다. 본 논문에서는 이러한 문제를 해결하기 위해서 Parent-Child 키 연결 알고리즘을 제안하였다. 제안한 알고리즘은 두 가지 구조로 되어있다. 일방향 해쉬 체인을 사용해서 안전하게 마스터키를 전송할 수 있는 마스터키 전송 알고리즘과, 새롭게 PAN에 조인하는 디바이스가 효율적으로 키 연결을 할 수 있게 child 노드와 parent 노드끼리 키 연결을 하는 Parent-Child 네트워크 키 전송 알고리즘으로 구성되어 있다. 디바이스가 마스터키를 가지고 있는 경우에는 제안한 방식이 기존 방식보다 키 연결 시간이 200~1300ms 정도 더 좋은 성능을 보였고, 디바이스가 마스터키를 가지고 있지 않은 경우에는 제안한 방식이 기존 방식보다 키 연결 시간이 400~500ms 정도 더 좋은 성능을 보였다.

Abstract

Coordinator is defining so that function as most trust center that is point in security in ZigBee Alliance. Because must do height connection with coordinator in device signing to PAN newly, coordinator has shortcoming that subordinate is revealed to danger directly to Centered and cattish device. When do height connection some device, do not become problem, but if network is huge, coordinator's subordinate shall increase as traffic quantity which happen in coordinator increases. Also, in ZigBee security to link network kina of transmission and mutually certification in ZigBee Alliance standard include, but I do not provide method to deliver master key in each node safely. Because process that transmit master key passes through channel that do not secure, master key has shortcoming that is revealed directly. In this paper, I suggested Parent-Child key establishment algorithm to solve these problem. Proposed algorithm consists of two structures. Master key establishment algorithm and device that sign to PAN newly that can use one-way Hash chain and transmit master key safely are consisted of Parent-Child network key establishment algorithm that do child node and parent node key establishment as can do key establishment efficiently. Method that device proposes in case method that propose in case have master key establishment time was shown better performance 200~1300 ms than existing method, and device does not have master key than existing method height connect time about 400~500 ms better performance see.

Keywords : ZigBee, Hash, SKKE

* 학생회원, ** 정회원, *** 종신회원, 광운대학교 전자통신공학과
(Dept. of Electronics and Communications Engineering, Kwangwoon Univ)
**** 정회원, 한전KDN(주)
(Korea Electric Power Data Network)
접수일자: 2006년6월7일, 수정완료일: 2006년10월2일

Ⅰ. 서 론

최근의 무선통신기술과 전자디바이스기술의 발전으로 저가격, 저 전력, 다기능 센서 노드로 구성된 무선 센서네트워크(Wireless Sensor Network)에 대한 관심이 급격히 고조되고 있다. 무선 센서 네트워크는 기존의 유선으로 구축된 센서네트워크를 무선네트워크로 대체 하는 기술로서, 각 센서노드는 센서에 의한 sensing, sensing된 데이터의 처리, 멀티 홉에 걸친 네트워킹 등의 기능을 가지고 있으며, 이는 기존의 전통적 의미의 센서에서 중요한 정보처리능력의 향상을 의미한다. 센서네트워크는 많은 수의 센서노드로 구성되어 있으며 이들 센서노드들은 서로 협동하며 주어진 응용 분야에서 작업을 해야 한다. 주요 응용 분야로서는 건강, 군사, 홈 네트워크, 재난방지, 환경 모니터링들을 들 수 있다[1].

센서네트워크는 기본적으로 멀티 홉 기반의 무선 Ad-hoc 네트워크(MANET) 기술을 필요로 한다. 하지만 기존에 Ad-hoc 네트워크와는 다른 다음과 같은 특징을 가지고 있다. 첫 번째로 센서 노드의 수를 Ad-hoc 네트워크에서 가정하는 노드의 수와 비교하면 몇 십 배, 몇 백배에 이를 수 있다. 두 번째로는 센서 노드는 응용에 따라 밀도가 높게 배포 될 수 있다. 세 번째로는 센서 노드는 Ad-hoc 네트워크에서의 대표적인 노드인 노트북이나 PDA등과는 다르게 배터리를 교체할 수 없고 따라서 파워소모를 줄이는 것이 가장 중요한 문제점 중의 하나이다. 네 번째로는 센서노드는 대체가 불가능하므로 고장이 났을 경우에 대비하여야 한다[2]. 따라서 센서네트워크의 설계에 있어서 가장 중요한 문제는 얼마나 에너지를 효율적으로 사용할 수 있는가 하는 것이다. 이러한 해결책으로 제시되고 있는 것이 IEEE 802.15.4 기반의 센서네트워크이다[3][4][5][6].

IEEE 802.15.4 표준은 Low-Rate WPAN(Wireless Personal Area Network) 환경에서 디바이스들의 PHY 계층과 MAC 계층을 정의하고 있다. 이러한 표준 기술을 기반으로 산업화를 위한 응용서비스 개발은 ZigBee Alliance에서의 표준화 작업을 통해 진행되고 있으며 네트워크, 보안 등의 기술적 요구사항 및 동작순서 등을 정의하고 있다. ZigBee 네트워크에서 모든 부하를 코디네이터에 집중시키고 있다. 코디네이터는 디바이스들의 전송 빈도가 낮은 패킷들도 받아야 하고 처리도 해주어야 하기 때문이다[7][8][9][10][11][12]. ZigBee Alliance에서는 보안에서 가장 핵심인 trust center 역할을 코디네이터가 하도록 정의하고 있다. 새롭게 PAN에 조인하는 디바이스마다 코디네이터와 키 연결을 해야 하기 때문에 코디네이터는 부하가 집중되고, 악의 있는 디바이스에게 직접적으로 위험에 노출되는 단점이 있다. 또한 ZigBee 보안에서 네트워크 키나 링크키의 전달 및 상호인증은 ZigBee Alliance 규격에 포함되어 있으나, 마스터키를 안전하게 각 노드에 전달하기 위한 방법을 제공하지는 않는다. 마스터키를 전송하는 과정이 안전하지 않은 채널을 통해서 전달하기 때문에 마스터키가 직접적으로 노출되는 단점을 가지고 있다[13][14][15][16][17].

본 논문에서는 이러한 문제를 해결하기 위해서 Parent-Child 키 연결 알고리즘을 제안하였다. 제안한 알고리즘은 두 가지 구조로 되어있다. 일방향 해쉬 체인을 사용해서 안전하게 마스터키를 전송할 수 있는 마스터키 전송 알고리즘과, 새롭게 PAN에 조인하는 디바이스가 효율적으로 키 연결을 할 수 있게 child 노드와 parent 노드끼리 키 연결을 하는 Parent-Child 네트워크 키 전송 알고리즘으로 구성되어 있다.

본 논문은 다음과 같은 구성을 가진다. Ⅱ 장에서는 ZigBee 보안에 대해서 알아보고, Ⅲ 장에서는 본 논문에서 제안하고자 하는 Parent-Child 키 연결 알고리즘에 대해서 알아보고, Ⅳ 장에서는 본 논문이 제안하고 있는 알고리즘의 구현 및 성능평가한 후에 Ⅴ 장에서 결론을 맺기로 한다.

Ⅱ. ZigBee 보안

ZigBee에서는 정보의 처리, 전달 및 저장을 안전하게 하기 위해선 보안이 필요하다. 특히 개방된 환경에서의

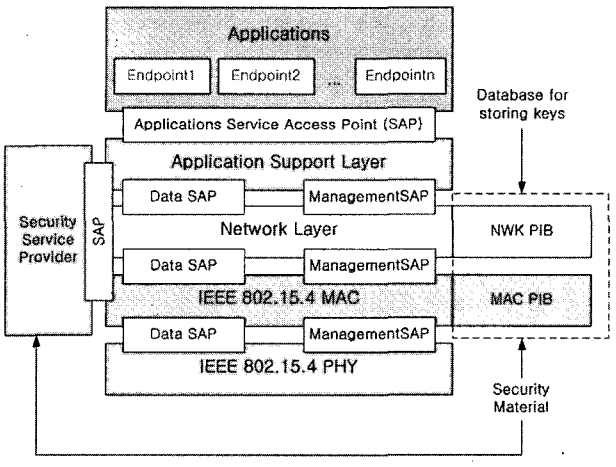


그림 1. ZigBee 보안 프로토콜 스택 구조
Fig. 1. ZigBee Security Protocol Stack Structure.

보안의 중요성은 더욱더 중요하다. 이러한 ZigBee 보안에서 필요로 하는 보안 기능으로는 암호 알고리즘, 키 관리 및 보안 프로토콜, 인증 및 secure routing, secure 데이터 등으로 암호화 하는 것이 필요하다.

1. ZigBee 보안 프로토콜 스택

그림 1은 ZigBee 보안 프로토콜 스택 구조로서, 네트워크 계층(Network Layer)과 응용 지원 하부 계층(Application Support Sublayer)에서는 보안 서비스 제공자(Security Service Provider)의 도움으로 보안 서비스를 제공하게 된다. 보안 서비스 제공자는 NWK PIB와 MAC PIB에게 보안에 관련된 Security Material 정보를 얻어온다. ZigBee 보안 서비스는 대칭키 암호 방식을 이용하여 두 노드 간의 비밀키 설정과 상호 인증 과정을 수행하고, 이 키를 이용하여 MAC 계층, 네트워크 계층, 응용 계층에서의 데이터 프레임에 대한 보안 기능을 제공한다. 이러한 구조에서 ZigBee 보안의 메커니즘은 MAC 계층, NWK 계층, 그리고 APS 계층에서 보안이 이루어진다.

2. 인증 및 키 연결 프로토콜

ZigBee 보안에서 새로운 디바이스가 조인을 하게 되면, 코디네이터와 새로운 디바이스 사이에서 SKKE 프로토콜을 사용한 인증 과정을 거친 후 코디네이터가 새로운 디바이스에게 네트워크 키를 전해준다.

그림 2는 마스터키를 가지고 있지 않은 디바이스가 코디네이터에게 조인을 할 때, 코디네이터가 디바이스를 인증한 후 네트워크 키를 전송해주는 과정을 보여주고 있다. 디바이스가 beacon 신호를 코디네이터와 주고받은 후 association response command를 받으면 인증 과정이 시작하게 된다. 디바이스는 코디네이터가 마스터키를 보내주면 코디네이터와 디바이스 사이에서 SKKE 프로토콜 과정을 진행하게 되고, SKKE 프로토콜 과정이 성공적으로 끝나면 코디네이터에게 네트워크 키를 받게 된다. 디바이스가 코디네이터에게 네트워크 키를 받게 되면 인증이 된 것이다.

그림 3은 마스터키를 가지고 있지 않은 디바이스가 라우터를 통해서 코디네이터에게 조인할 때, 코디네이터가 디바이스를 인증하는 과정을 보여주고 있다. 중간에서 라우터가 중계 역할을 해주는 것만 빼고는 그림 3-5 과 같은 과정을 통해서 인증과정이 수행되어진다. 디바이스가 코디네이터에게 인증과정이 설공하면 디바이스는 네트워크 키를 코디네이터에게 받게 된다. 여기

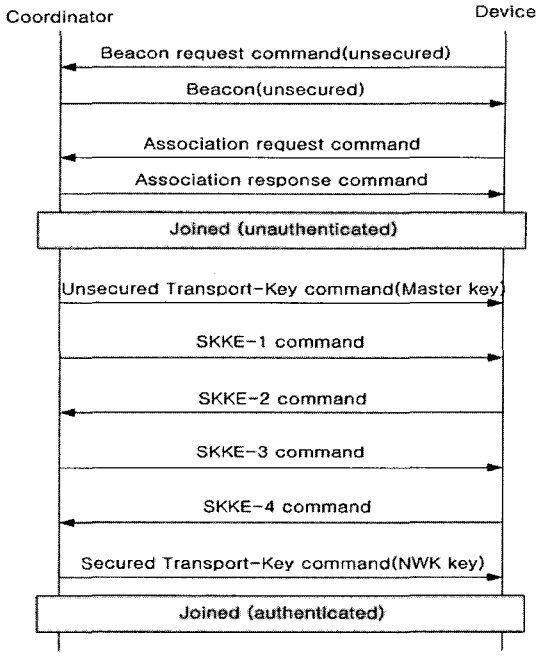


그림 2. 코디네이터와 디바이스 간의 인증 및 키 연결 과정

Fig. 2. Authentication and Key Establishment Process between Coordinator and Device.

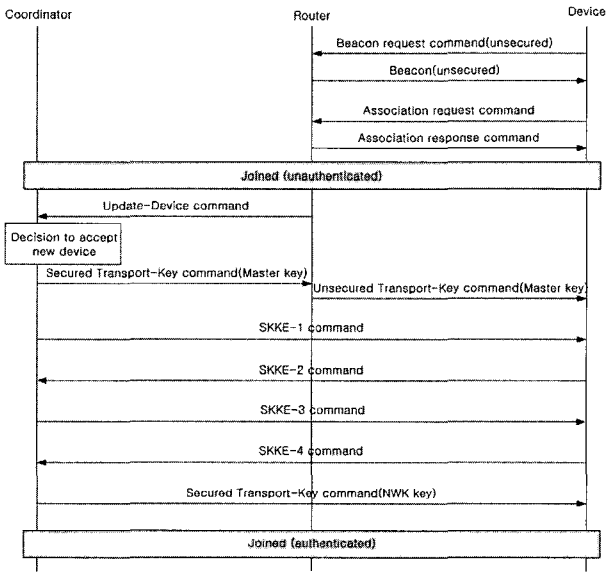


그림 3. 라우터를 통해서 조인한 디바이스와 코디네이터간의 인증 및 키 연결 과정

Fig. 3. Authentication and Key Establishment Process between Coordinator and Device through Router.

서, 앞에서 살펴본 SKKE 프로토콜 과정에서 보면 SKKE-1 command는 QEU을 보내는 command이고 SKKE-2 command는 QEV을 보내는 command이고 SKKE-3 command는 $HMAC_2$을 보내는 command이고 SKKE-4 command는 $HMAC_1$을 보내는 command를 뜻

한다. SKKE 프로토콜 과정이 성공적으로 끝나면 새로운 링크키를 서로 가지게 되고, 안전한 채널을 확보할 수 있다.

Ⅲ. 효율적인 Parent-Child 키 연결 알고리즘

ZigBee 보안에서 네트워크 키나 링크키의 전달 및 상호 인증은 ZigBee Alliance 규격에 포함되어 있으나, 마스터키를 안전하게 각 디바이스에 전달하기 위한 방법을 제공하지는 않는다. 코디네이터를 활용하여 디바이스 사이의 네트워크 키나 링크키는 중간 디바이스들의 중계에 의하여 키 전달은 가능하지만, 이 통신 채널의 안전성을 항상 보장하지는 않는다. 즉, 새롭게 조인하는 디바이스가 마스터키가 없으면 코디네이터가 디바이스에게 마스터키를 보내주어야 한다. 이러한 마스터키를 보내주는 과정은 코디네이터와 디바이스 간에 안전한 channel을 확보하는 과정이 없기 때문에 unsecured channel을 이용하게 된다.

ZigBee 키 연결 방법에서는 다음과 같은 문제점이 있다. 첫 번째로 코디네이터의 집중화라는 문제이다. 모든 디바이스들이 네트워크 키를 받기 위해서는 코디네이터와 링크키를 맺는 과정(SKKE 프로토콜)이 필요하다. 즉, 소수의 디바이스들만 있는 환경에서는 문제가 되지 않지만, 다수의 디바이스에서는 문제가 발생한다. 모든 traffic이 코디네이터로 집중되기 때문에 코디네이터로 향하는 traffic이 증가하게 된다. 이러한 traffic은 네트워크 시스템의 성능을 저하시키고 새롭게 조인하는 디바이스가 새롭게 키 연결을 하는 시간을 증가 시킨다. 두 번째로 코디네이터의 위험성이 있다. 악의적인 사용자가 코디네이터와 링크키를 맺은 디바이스를 해킹해서 코디네이터와 맺은 링크키를 알아내면 코디네이터까지 위협에 처한다. 이렇게 코디네이터가 해킹을 당하면 이러한 네트워크는 모든 디바이스가 위험해 진다. 세 번째로 사용되는 키 숫자 문제이다. 모든 디바이스들이 코디네이터와 링크키를 맺어야지만 인증이 되기 때문에 코디네이터는 모든 디바이스들의 링크키를 가지고 있어야한다. 즉, 네트워크에 디바이스들이 증가하면 코디네이터가 관리해야할 키들이 많아지는 문제가 발생한다.

상기 설명된 ZigBee 보안의 문제점을 해결하기 위해 효율적인 Parent-Child 키 연결 알고리즘을 제안하였다. 제안한 알고리즘은 두 가지 세부 알고리즘으로 구성되었다. 첫 번째 제안한 알고리즘은 새롭게 조인하는 디바이스에게 마스터키를 보내줄 때 일방향 해쉬 체인을 사용해서 Parent 노드와 Child 노드 간에 secured channel을 생성한 후 Parent 노드가 Child 노드에게 안전하게 마스터키를 보내주는 안전한 마스터키 전송 알고리즘이고, 두 번째 제안한 알고리즘은 기존의 코디네이터와 키 연결을 맺는 방식이 아니라 Parent 노드와 Child 노드가 키 연결을 맺어서 Parent 노드가 Child 노드에게 효율적으로 네트워크 키를 전송해주는 Parent-Child 네트워크 키 전송알고리즘이다.

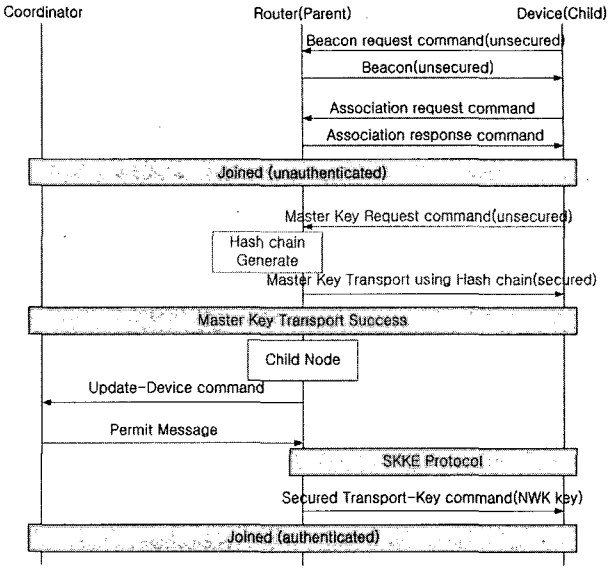


그림 4. 제안한 Parent-Child 키 연결 알고리즘
Fig. 4. Proposed Parent-Child Key Establishment Algorithm.

그림 4는 라우터를 통해서 디바이스와 코디네이터 간의 인증 및 키 연결을 수행할 때 제안한 효율적인 Parent-Child 키 연결 알고리즘을 적용한 과정을 보여주고 있다. 조인하는 디바이스(Child 노드)가 마스터키를 가지고 있지 않기 때문에 라우터(Parent 노드)에게 안전하게 마스터키를 전송 받고 라우터와 디바이스 간에 효율적으로 SKKE 프로토콜을 성공적으로 수행하면 라우터에게 네트워크 키를 전송 받는다.

1. 안전한 마스터키 전송 알고리즘

조인하는 디바이스가 마스터키를 가지고 있지 않으면 안전한 마스터키 전송 알고리즘이 수행되고, Parent 노드는 그림 5와 같이 Child 노드는 그림 6과 같은 과정으로 수행된다.

다음은 안전한 마스터키 전송 알고리즘이 수행되어질 때 Parent 노드에서 이루어지는 세부단계를 보여주고 있다.

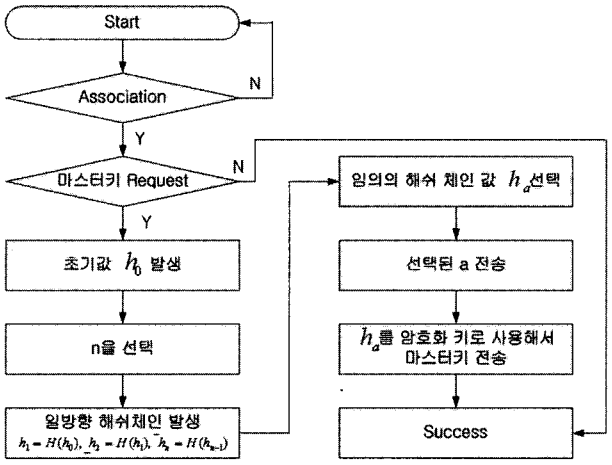


그림 5. 안전한 마스터키 전송 알고리즘 (Parent 노드)
Fig. 5. Secured Master Key Transport Algorithm (Parent Node).

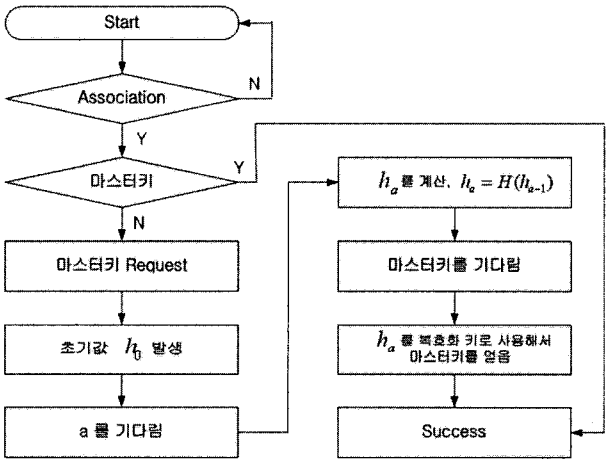


그림 6. 안전한 마스터키 전송 알고리즘 (Child 노드)
Fig. 6. Secured Master Key Transport Algorithm (Child Node).

[가정] 초기치 h_0은 Parent 노드와 Child 노드가 알고 있어야 한다.

[단계 1] Association 발생

[단계 2] 마스터키 Request 발생

마스터키 Request가 발생하면 단계 3을 수행하고 발생하지 않으면 알고리즘을 종료한다.

[단계 3] 초기치 h_0 발생

[단계 4] n을 선택

[단계 5] 일방향 해쉬 체인을 발생

$$h_1 = H(h_0),\ h_2 = H(h_1),\ldots,\ h_n = H(h_{n-1})$$

[단계 6] 임의의 해쉬 체인 값 h_a 선택

[단계 7] 선택된 a를 Child 노드에게 전송

[단계 8] h_a로 암호화키로 사용해서 마스터키를 Child 노드에게 암호화 하여 전송

[단계 9] 끝냄

다음은 안전한 마스터키 전송 알고리즘이 수행되어질 때 Child 노드에서 이루어지는 세부단계를 보여주고 있다.

[가정] 초기치 h_0은 Parent 노드와 Child 노드가 알고 있어야 한다.

[단계 1] Association 발생

[단계 2] 마스터키 유무 확인

마스터키가 있으면 단계 3을 수행하고 마스터키가 없으면 알고리즘을 종료한다.

[단계 3] Parent 노드에게 마스터키 Request를 보냄

[단계 4] 초기치 h_0 발생

[단계 5] a를 기다림

[단계 6] h_a 을 계산

$$h_1 = H(h_0),\ h_2 = H(h_1),\ \ldots,\ h_a = H(h_{a-1})$$

[단계 7] 마스터키를 기다림

[단계 8] h_a을 복호화 키로 사용해서 마스터키를 얻음

[단계 9] 끝냄

2. Parent-Child 네트워크 키 전송 알고리즘

마스터키를 가지고 있거나 안전한 마스터키 전송 알고리즘이 성공적으로 수행되면 Parent 노드와 Child 노드 간에 Parent-Child 네트워크 키 전송 알고리즘이 수행된다. 그림 7은 Parent-Child 네트워크 키 전송 알고리즘의 과정을 보여주고 있다.

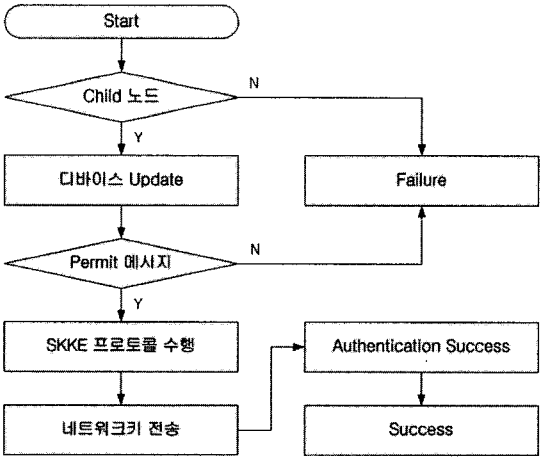


그림 7. 제안한 Parent-Child 네트워크 키 전송 알고리즘
Fig. 7. Proposed Parent-Child Network Key Transport Algorithm.

제안한 Parent-Child 네트워크 키 전송 알고리즘 세부단계는 다음과 같다.

[가정] Parent 노드와 Child 노드가 마스터키를 가지고 있어야 한다.

[단계 1] 조인하는 디바이스 확인

조인하는 디바이스의 주소가 Child 노드이면 단계 2를 수행하고 Child 노드가 아니면 알고리즘은 실패하게 된다.

[단계 2] 디바이스 업데이트 수행

코디네이터에게 조인한 디바이스에 대한 업데이트를 수행한다.

[단계 3] permit message를 기다림

코디네이터에서 permit message가 오면 단계 4를 수행한다. 하지만 permit message가 오지 않으면 이 디바이스의 인증과정은 실패하게 된다.

[단계 4] SKKE 프로토콜을 수행

Parent 노드와 Child 노드 간에 SKKE 프로토콜을 수행한다.

[단계 5] 네트워크 키 전송

단계 4가 성공하면 Parent노드가 Child 노드에게 네트워크 키를 전송한다.

[단계 6] [끝냄]

Ⅳ. 구현 및 성능평가

제안한 방식을 구현 및 성능평가를 수행하기 위해서 RadioPulse, Inc에서 개발한 MG2400 Evaluation Kit (MG2400-EVK)를 사용하였다. MG2400-EVK는 IEEE 802.15.4기반의 ZigBee지원 Single Chip인 Kit이다. MG2400-EVK는 다음과 같이 구성되어 있다. MG2400-EVM인 ZigBee 모듈과 MG2400-PCIB인 PC Interface 보드로 구성되어 있다. MG2400-EVM은 외장형 SMA Antenna를 장착할 수 있는 ZigBee 모듈이다. MG2400-PCIB은 MG2400-EVM을 사용하기 위하여, PC와의 연결 및 MG2400에서 구현되어 있는 기능을 동작시킬 수 있도록, MG2400-EVM과 연동하여 사용할 수 있는 응용 B/D이다.

제안한 알고리즘을 구현하기 위해서 각각 State Machine 방식으로 C 언어를 통해서 구현하였다. 구현된 소스는 ANSI 표준규격을 만족한다. 이렇게 구현된 소스를 Keil 8051 C Compiler를 통해서 컴파일러 한 후 컴파일 된 소스 파일을 Hex 파일로 바꾸어준다. 이 Hex 파일을 Device-Programmer를 사용해서 MG2400-EVK

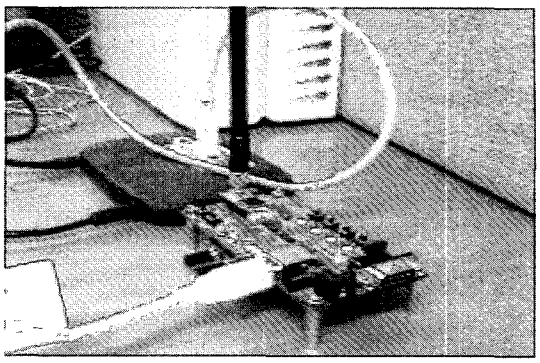


그림 8. MG2400-EVK에 다운로드를 하는 과정
Fig. 8. Process MG2400-EVK Download.

에 다운로드를 한다. MG2400-EVK 모듈을 기반으로 하여 제안 알고리즘을 소프트웨어로 구현한 후, 이 모듈을 PC 또는 노트북에 RS-232로 연결하여 무선으로 데이터 통신을 실험하였다. 실험 결과는 PC 또는 노트북에서 모니터링 할 수 있는 펌웨어인 CatTerm 2.0을 사용하여 측정하였다.

그림 8은 Hex 파일을 Device-Programer를 사용해서 MG2400-EVK에 다운로드를 하는 과정을 보여주고 있다.

제안한 알고리즘의 성능평가를 하기 위해서 기존 SKKE 키 연결 알고리즘과 제안한 Parent-Child 키 연결 알고리즘을 적용하여 각각의 키 연결 시간을 측정하였다. 성능평가는 각각의 디바이스가 마스터키를 가지고 있는 경우와 마스터키를 가지고 있지 않는 경우에 대해서 실험하였다. 마스터키가 있는 경우에는 Parent-Child 키 연결 알고리즘 중에서 Parent-Child 네트워크 키 연결 알고리즘만 수행되고, 마스터키가 없는 경우에는 Parent-Child 키 연결 알고리즘 중에서 Parent-Child 네트워크 키 연결 알고리즘과 안전한 마스터키 전송알고리즘이 수행된다. 성능평가는 1홉에서 4홉까지 홉 수를 변화 시켜서 홉 수에 따른 키 연결 시간을 기존 방식과 제안 방식을 비교해봤다. 측정한 키 연결 시간은 디바이스가 조인부터 디바이스가 네트워크 키를 받을 때까지이고, 1홉에서는 한 개의 디바이스가 키 연결을 수행할 때까지 걸리는 키 연결시간이고 2홉에서는 두 개의 디바이스가 키 연결을 수행할 때까지 걸리는 키 연결시간이고 3홉에서는 세 개의 디바이스가 키 연결을 수행할 때까지 걸리는 키 연결시간이고 4홉에서는 네 개의 디바이스가 키 연결을 수행할 때까지 걸리는 키 연결 시간을 각각 측정하였다.

제안한 알고리즘의 성능평가를 하기위한 환경은 다음과 같다.

▶ 성능평가 장소 : 실내 20m 이내
▶ 전송속도 : 250Kbps
▶ 디바이스 수 : 코디네이터 1, 디바이스 4개
▶ Payload Size : 20Byte
▶ 동작전원 : 배터리 전원 3V
▶ 성능평가 항목 : 각 홉 수에 따른 키 연결 시간

제안한 알고리즘의 성능평가 방법은 다음과 같다. 조인하는 디바이스가 마스터키를 가지고 있는 경우와 마스터키를 가지고 있지 않은 경우로 나누어서 성능평가를 진행하였다. 성능평가는 키 연결을 이벤트 방식으로 100번 수행시켜서 키 연결을 하는데 걸리는 시간을 측정하였다. 디바이스가 코디네이터에게 조인을 하는 시간부터 코디네이터에게 네트워크 키를 받는 시간까지를 측정하였다. 만약 2홉일 경우에 라우터가 코디네이터에게 네트워크 키를 받고 라우터를 통해서 조인하는 디바이스가 네트워크 키를 받는 시간까지 시간을 측정하였다.

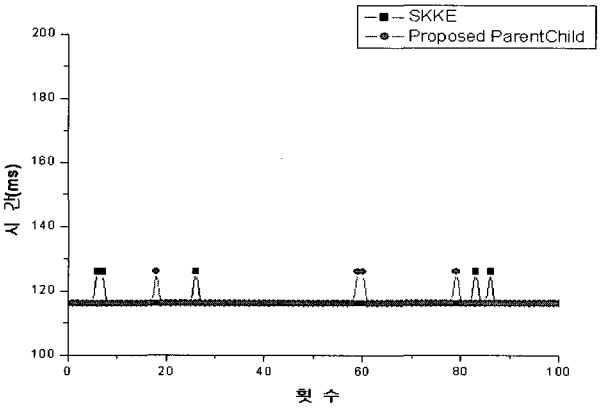


그림 9. 1 홉일 때 키 연결 시간
Fig. 9. Key establishment time in 1 hop.

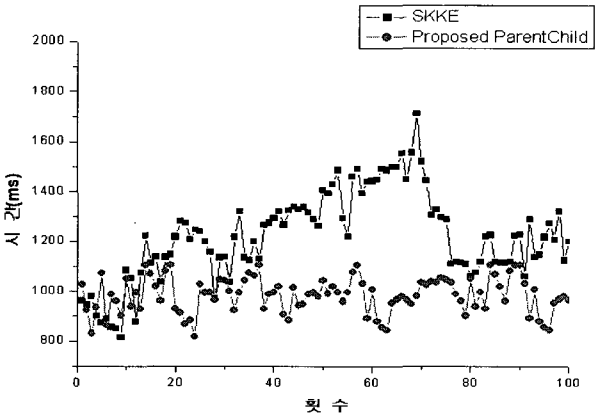


그림 10. 2 홉일 때 키 연결 시간
Fig. 10. Key establishment time in 2 hop.

마스터키가 있는 경우에 성능평가 결과는 다음과 같다. 그림 9는 1 홉일 때 키 연결 시간의 결과이고, 그림 10은 2 홉일 때 키 연결 시간의 결과이고, 그림 11은 3 홉일 때 키 연결 시간의 결과이고, 그림 12는 4 홉일 때 키 연결의 시간의 결과이다. 그림 13은 각 홉 수에 따른

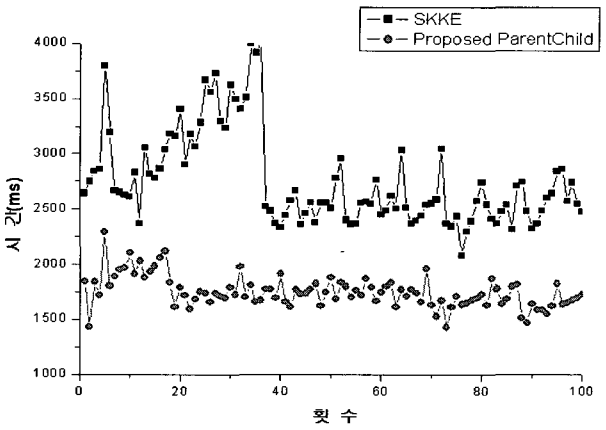


그림 11. 3 홉일 때 키 연결 시간
Fig. 11. Key establishment time in 3 hop.

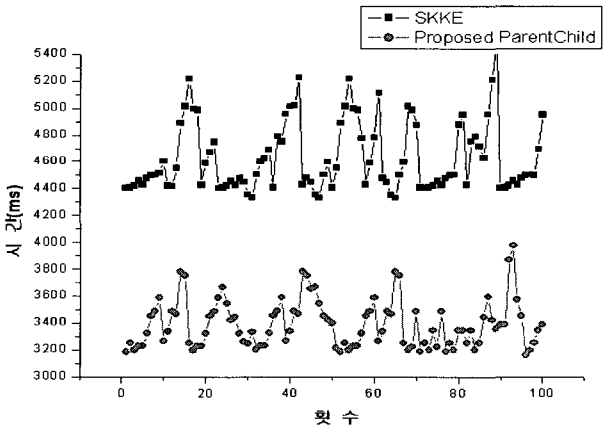


그림 12. 4 홉일 때 키 연결 시간
Fig. 12. Key establishment time in 4 hop.

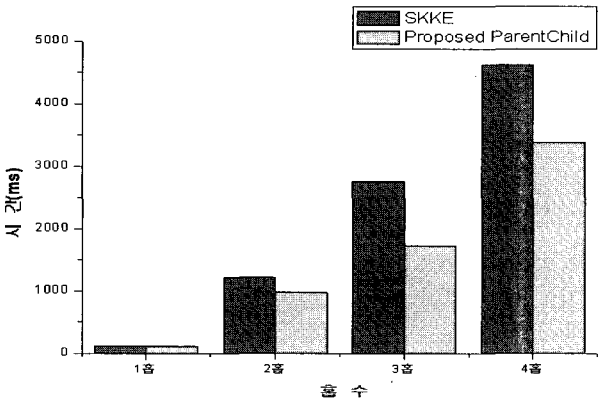


그림 13. 홉 수에 따른 평균 키 연결 시간
Fig. 13. Average key establishment time by unit of hop number.

평균 키 연결 시간을 그래프로 표현한 것이다.

디바이스들이 마스터키를 가지고 있는 경우 키 연결 시간은 성능평가에서 알 수 있듯이 1홉에서는 제안 방식과 기존 방식이 비슷한 성능을 보였지만 홉 수가 증가할수록 제안한 방식이 더 좋은 성능을 보였다. 2홉에서는 제안한 방식이 기존 방식보다 250ms 정도 더 좋은 성능을 보여 주었고 3홉에서는 제안한 방식이 기존 방식보다 1000ms 정도 더 좋은 성능을 보여 주었고 4홉에서는 제안한 방식이 기존 방식보다 1300ms 정도 더 좋은 성능을 보여 주었다. 홉 수가 증가할수록 조인하는 디바이스들이 코디네이터와 키 연결을 맺는 방식보다는 제안한 Parent 노드와 Child 노드끼리 맺는 방식이 더 효율적으로 키 연결을 할 수가 있다.

마스터키가 없는 경우에 성능평가 결과는 다음과 같다. 그림 14는 1 홉일 때 키 연결 시간의 결과이고, 그림 15는 2 홉일 때 키 연결 시간의 결과이고, 그림 16은 3 홉일 때 키 연결 시간의 결과이고, 17은 4 홉일 때 키 연결의 시간의 결과이다. 그림 18은 각 홉 수에 따른 평균 키 연결 시간을 그래프로 표현한 것이다.

디바이스들이 마스터키를 가지고 있지 않은 경우 키 연결 시간은 성능평가에서 알 수 있듯이 1홉에서는 기존 방식이 제안 방식보다 200ms 정도 좋은 성능을 보였고 2홉에서는 기존 방식이 제안 방식보다 130ms 정

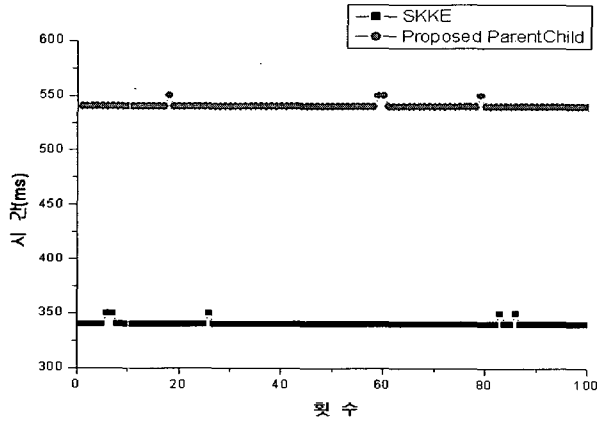


그림 14. 1 홉일 때 키 연결 시간
Fig. 14. Key establishment time in 1 hop.

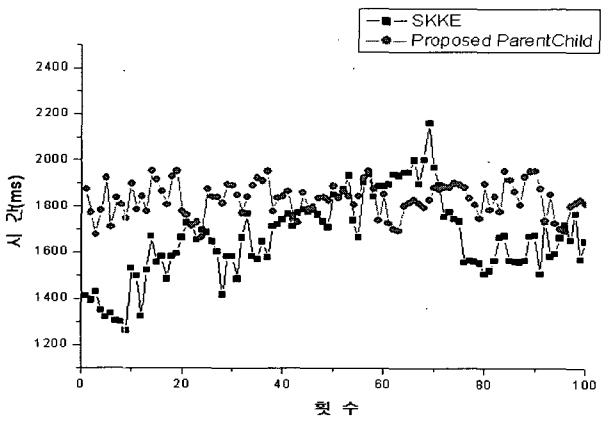


그림 15. 2 홉일 때 키 연결 시간
Fig. 15. Key establishment time in 2 hop.

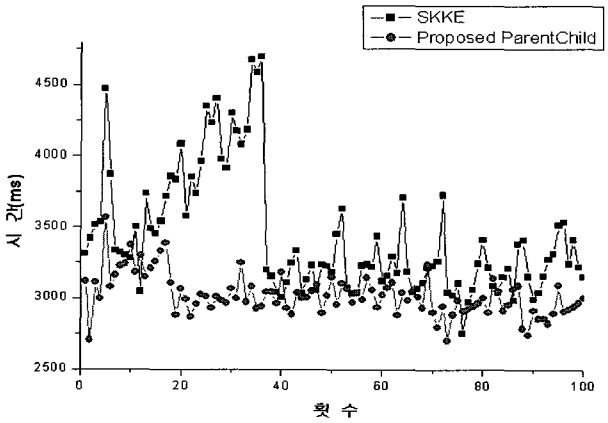


그림 16. 3 홉일 때 키 연결 시간
Fig. 16. Key establishment time in 3 hop.

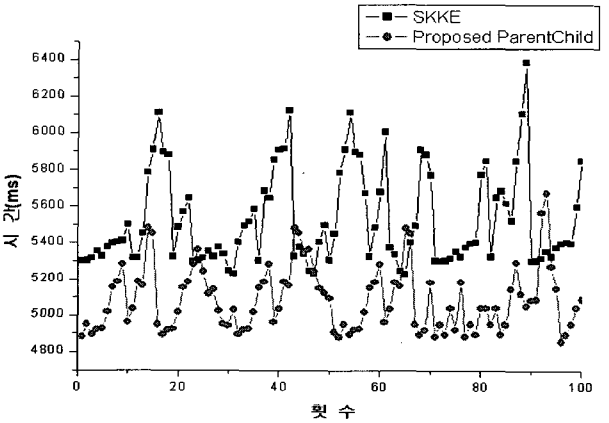


그림 17. 4 홉일 때 키 연결 시간
Fig. 17. Key establishment time in 4 hop.

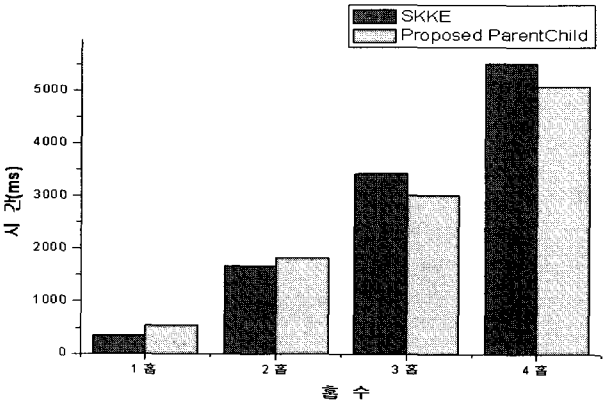


그림 18. 홉 수에 따른 평균 키 연결 시간
Fig. 18. Average key establishment time by unit of hop number.

도 좋은 성능을 보였다. 하지만 3홉에서는 제안한 방식이 기존 방식보다 400ms 정도 좋은 성능을 보였고 4홉에서는 제안한 방식이 기존 방식보다 500ms 정도 좋은 성능을 보였다. 3홉 이상일 때 기존방식보다 제안 방식이 더 우수한 성능을 보여주었다.

제안한 방식에서 마스터키를 가지고 있지 않은 디바이스가 조인하게 되면 안전한 채널을 통해서 마스터키를 전송한다. 이러한 이유 때문에 2홉 이하에서는 기존 방식의 키 연결 시간이 빠르지만 3홉 이상에서는 제안한 방식이 더 효율적으로 키 연결을 할 수 있는 것을 보여주었다.

V. 결 론

센서네트워크의 설계에 있어서 에너지 효율성 및 배터리를 고려했을 때 IEEE 802.15.4 기반의 센서네트워크가 가장 각광받고 있다. 이러한 표준 기술을 기반으로 산업화를 위한 응용서비스 개발은 ZigBee Alliance에서의 표준화 작업을 통해 진행되고 있다.

ZigBee 센서네트워크에서 디바이스가 새롭게 조인을 하게 되면 코디네이터와 디바이스 간에 키 연결과정을 수행하게 된다. 이러한 과정을 통해서 디바이스는 인증을 수행하게 되고 링크키와 네트워크 키를 코디네이터에게 얻게 된다. 하지만 조인하는 디바이스가 많아지게 되면 코디네이터는 각각의 디바이스마다 키 연결을 수행해야하기 때문에 코디네이터와 디바이스간의 키 연결 시간 증가와 네트워크 traffic이 증가하게 되고 악의 있는 디바이스에게 코디네이터의 전복의 위험이 존재한다. 또한 ZigBee Alliance에서 제시한 ZigBee Security Specification에서는 안전한 마스터키 분배에 대해서 제시하지 않고 있기 때문에 마스터키의 노출 문제점을 가지고 있다.

이러한 문제를 해결하기 위해서 ZigBee 센서네트워크에서 효율적으로 키 연결을 수행하는 Parent-Child 키 연결 알고리즘을 제안하였다. 성능평가 결과 디바이스가 마스터키를 가지고 있는 경우에는 제안한 방식이 기존 방식보다 키 연결 시간이 200~1300ms 정도 더 좋은 성능을 보였고, 디바이스가 마스터키를 가지고 있지 않은 경우에는 제안한 방식이 기존 방식보다 키 연결 시간이 400~500ms 정도 더 좋은 성능을 보였다.

제안 방식은 마스터키를 디바이스에게 안전하게 전송해줄 수 있고, 코디네이터에게 치중되는 부하를 줄임으로써 네트워크 traffic을 분산시켜주고 키 연결시간을 감소시켜준다. 또한 네트워크상에서 사용되는 키 숫자를 절감할 수 있고 디바이스가 악의 있는 사용자에게 전복되어도 코디네이터는 안전하기 때문에 전체적인 네트워크 안전성을 증가한다.

무선 센서네트워크에서는 에너지 효율성과 배터리 수명이 가장 중요하다. 이러한 점을 고려했을 때 가장 각광 받고 있는 것이 ZigBee 기술이다. ZigBee 에서 보안을 적용할 때도 에너지 효율성과 배터리 수명을 고려해야한다. 많은 디바이스들이 키 연결을 수행할 때 에너지 효율성 부분에서 SKKE 키 연결 알고리즘보다 제안한 Parent-Child 키 연결알고리즘이 효과적인 것을 성능평가를 통해서 확인해보았다.

참 고 문 헌

[1] 김대영, 도윤미, 박노성, 이상수, 팜민롱, 뒤뷔백, 파티오즈투르크 "센서네트워크 기술", 정보처리학회지, 제 10권, 제 4호, pp. 85~96, 2003년 7월

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

[3] 전호인 "IEEE 802.15.4 WPAN 기술", 전자공학회지, 제 32권, 제 4 호, pp. 87~104, 2005년 4월.

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

[5] 김기형, 정원도, 박준성, 서현곤, 박승민, 김홍남 "IEEE 802.15.4기반의 유비쿼터스 센서네트워크 기술", 전자공학회지, 제 31권, 제 12호, pp. 74~84, 2004년 12월.

[6] 정성훈, 전호인 "IEEE 802.154 and ZigBee Protocol : 유비쿼터스 센서 네트워킹을 위한 Active RFID 기술", 한국통신학회지(정보통신), 21권, 6호, pp. 693~714, 2003년 6월.

[7] IEEE 802.15.4-2003 IEEE Standard for Information Technology-Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specification for Low Rate Wireless Personal Area Networks (LR-WPANs), 2003.

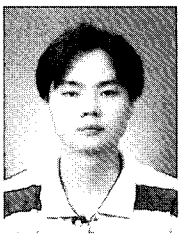
[8] J.A Gutierrez et al, "IEEE 802.15.4: A Developing Standard for Low-Power Low-Cost Wireless Personal Area Networks." IEEE Network Vol. 15, No 5, Sep/Oct. 2001, pp. 12-19.

[9] Ed Callaway, Paul Gorday and Lance Hester, "Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal AreaNetworks", in IEEE Communications Magazine, August 2002.

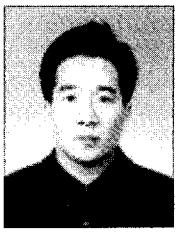
[10] Jose A. Gutierresz, Edgar H. Callaway, Jr., and

Raymond L., Barrett, Jr., "Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensors with IEEE 802.15.4", IEEE Press, 2003.
[11] IEEE 802.15.1-2002 IEEE Standard for Information Technology - TeleCommunication and Information Exchage between Systems - LAN/MAN - Part 15.1: Wireless Medium Access Control MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks(WPANs), 2002.
[12] IEEE 802.11-1999 IEEE Standard for Information Technology - LAN/MAN - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.
[13] 김원수, 장기수 "ZigBee 기술 동향 및 시장 전망 분석", 삼성 종합 기술원, 2004년 4월.
[14] ZigBee Alliance home page, http://www.zigbee.org
[15] ZigBee Alliance Document 02130 : Network Layer Specification, July 2004.
[16] ZigBee Alliance Document 03525 : ZigBee Apllication Framework, March 2004.
[17] ZigBee Alliance Document 03522 : Security Service Specification, Dec 2004.

저 자 소 개



서 대 열(학생회원)
2004년 서울산업대학교 전자정보 공학과 학사 졸업
2006년~현재 광운대학교 전자통신공학과 석사 재학중
<주관심분야 : IEEE 802.15.4, Ad-hoc Security, Sensor Security, ZigBee Security>



김 진 철(정회원)
1995년 광운대학교 전자공학과 학사 졸업
1997년 광운대학교 전자공학과 석사 졸업
2006년 광운대학교 대학원 전자통신공학과 박사졸업
2006년 현재 한전 KDN(주)
<주관심분야 : PKI, WPKI, Mobile Ad-hoc Network>

김 경 목(정회원)
1996년 서울산업대학교 전자공학과 학사 졸업.
2002년 광운대학교 전자통신공학과 석사졸업.
2006년 광운대학교 대학원 전자통신공학과 박사 졸업.
<주관심분야 : Optical Internet, MPλS, GMPLS>

오 영 환(종신회원)
2006년 현재 광운대학교 전자통신공학과 교수
<주관심분야 : Network and Device Reliability>