논문 2009-46TC-2-10

시스템 ID를 이용한 USN의 보안 취약성 개선

(USN Security Enhancement Using System IDs)

김 현 주*, 정 종 문**

(Hyunjue Kim and Jong-Moon Chung)

요 약

군사용이나 환경 감시 등의 영역에서 응용되고 있는 유비쿼터스 센서 네트워크(Ubiquitous Sensor Network)는 센서 정보의 도청이나, 비정상적 패킷의 유통, 메시지의 재사용 등 데이터의 위·변조와 같은 외부의 공격에 쉽게 노출되는 환경에서 동작하기 때문에, 보안은 필수적으로 갖추어져야 하는 중요한 기능이다. 저전력, 초소형, 저비용의 장점을 갖는 ZigBee는 유비쿼터스 센서 네트워크를 구현하는 최적의 기술로 주목받고 있다. 그러나 ZigBee 보안 시스템에는 심각한 문제점들을 가지고 있다. 본 논문에서는 USN의 대표적인 예로 ZigBee 보안 시스템이 가지고 있는 문제점들을 자세히 분석하고, 이를 해결하여 USN에 적합한 보안 프로토콜을 새롭게 제안하고 그 효율성을 비교·분석한다.

Abstract

Security is critically important for ubiquitous sensor networks that are usually used for the military and serveillance in environments that are opened to attacks, such as, eavesdroping, replay attacks of abnormal messages, forgery of the messages to name a few. ZigBee has emerged as a strong contender for ubiquitous sensor networks. ZigBee is used for low data rate and low power wireless sensor network applications. To deploy ubiquitous sensor networks, the collected information requires protection from an adversary over the network in many cases. The security mechanism should be provided for collecting the information over the network. However, the ZigBee protocol has some security weaknesses. In this paper, these weaknesses are discussed and a method to improve security aspect of the ZigBee protocol is presented along with a comparison of the message complexity of the proposed security protocol with that of the current ZigBee protocol.

Keywords: USN, IEEE 802.15.4, ZigBee security, authentication, key management

I. 서 론

최근 홈 네트워크 및 유비쿼터스에 대한 관심이 크게 증가하면서 단거리에서 사용하는 개인 무선 네트워킹 솔루션인 WPAN(Wireless personal area network) 기술이 주목받고 있다. WPAN 기술의 대표적으로는 ZigBee, UWB(Ultra wideband)와 Blutooth 등이 있는데, 이 중 특히 ZigBee가 무선 시장의 이슈로 급부상하고 있다. ZigBee[1]는 IEEE 802.15.4[2]의 물리층(Physical layer)과 매체접근제어층(Medium access control layer)를 도입하여 네트워크 계층부터 새롭게 정의한 산업체 동맹이 작성한 표준으로, 다른 무선 통신 기술과 달리 전력소모가 적고 저가 제품의 구현이 가능하여 지능형 홈 네트워크, 빌딩 등의 근거리 통신 시장과 산업용기기 자동화, 물류, 환경 모니터링, 휴먼 인터페이스, 텔레매틱스, 군사 등의 다양한 응용에 적합한 기술이다. 또한 ZigBee 통신은 반경 100m안에서 250kbps의 속도로 데이터를 전송하고, 멀티홉(Multi-hop) 기능이 지원되어 약 65000개 이상의 노드(Node)를 연결할 수 있어 확장성 있는 네트워크를 구성하는 것이 가능하다. 다대다

* 정회원, ** 정회원-교신저자,
연세대학교 전기전자공학부
(School of Electrical & Electronic Engineering, Yonsei University)

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2009-C1090-0801-0038).

접수일자: 2008년6월9일, 수정완료일: 2009년2월17일

(N-to-M) 통신인 그물망(Mesh)으로 이루어진 확장된 네트워크에서는 공격자에 의한 데이터의 위·변조에 대응하기 위하여 노드들의 상호 인증과 데이터 암호화가 중요하며, 이때에 사용되는 키 관리도 매우 중요한 보안요소 중 하나이다.

정보유출이나 불법적인 침입자로 인한 도청 및 위·변조를 막기 위해서, ZigBee는 128비트의 AES (Advanced encryption standard) 대칭키 암호방식[3]을 이용하여 두 노드간의 키 관리(Key management), 키 설정(Key establishment), 키 전송(Key transport)과 인증(Authentication) 과정을 수행하고, 이 키를 이용하여 매체접근제어층, 네트워크층(Network layer), 응용층(Application layer)에서의 데이터 프레임에 대한 보안 기능을 제공한다.

그러나 ZigBee 보안 시스템은 심각한 문제들을 가지고 있다. ZigBee는 신뢰센터(Trust center)라는 개념을 이용하여 네트워크상의 노드들의 키를 분배하고 노드간의 단대단(End-to-end) 보안을 가능하게 한다. 그리고 노드 사이의 비밀키는 중간 노드들의 중계에 의하여 전달된다. 그러나 이때의 중간 통신 채널의 안전성을 ZigBee 보안 시스템에서는 완벽히 보장하지를 않는다. 이는 비밀키의 안전성의 보장이 가장 중요한 대칭키 암호기반의 ZigBee에서의 심각한 문제가 된다. 또한 대칭키 암호 시스템을 사용하는 ZigBee 시스템에서는 신뢰센터가 통신하고 하는 모든 노드들의 비밀키를 관리하도록 되어 있는 구조적인 약점을 가지고 있다.

본 논문에서는, 위에서 언급한 이외에, ZigBee 보안 시스템이 가지고 있는 여러 문제점들을 자세히 분석한다. 그리고 분석된 문제점들을 해결하는 ZigBee 보안 프로토콜을 새롭게 제안하고, 제안하는 프로토콜의 효율성을 비교·분석한다. 제안하는 프로토콜은 별도의 복잡한 키 관리를 필요로 하지 않는 공개키 암호방식[4]을 기반으로 설계한 새로운 방식이다.

본 논문의 구성은 다음과 같다. Ⅰ장의 서론에 이어 Ⅱ장에서는 ZigBee 프로토콜을 살펴보고, ZigBee가 가지고 있는 여러 가지 문제점들을 분석한다. Ⅲ장에서는 Ⅱ장에서 분석한 ZigBee의 문제점을 해결할 수 있는 새로운 프로토콜을 제안하고, Ⅳ장에서는 기존의 ZigBee 프로토콜과 본 논문에서 제안하는 프로토콜을 비교한다. 마지막 Ⅴ장에서는 결론을 맺는다.

Ⅱ. ZigBee 네트워크의 취약성 분석

1. ZigBee 보안

ZigBee는 근거리 통신을 지원하는 IEEE 802.15.4 표준 중 하나를 말한다. 가정, 사무실, 산업현장 등의 무선 네트워킹 분야에서 10~100m 내외의 근거리 통신과 유비쿼터스 컴퓨팅을 위한 기술이다. ZigBee는 휴대전화나 무선 LAN의 개념으로, 기존의 기술과 다른 특징은 전력소모를 최소화하는 대신 소량의 정보를 소통시키는 무선 센서 네트워크 표준이다. ZigBee 네트워크는 지능형 홈 네트워크, 빌딩 등의 근거리 통신 시장과 산업용 기기 자동화, 물류, 환경 모니터링, 휴먼 인터페이스, 텔레매틱스, 군사 등에 활용된다. 최근 전력 소모량이 적고 값이 싸 홈 네트워크 등 유비쿼터스 구축 솔루션으로 각광받고 있다.

2003년 IEEE는 저가격, 저전력과 간단한 네트워크 구조를 갖는 WPAN 기술을 정의하는 802.15.4를 발표하고, 2005년 ZigBee 얼라이언스(Alliance)는 IEEE 802.15.4에 네트워크·보안 계층을 추가로 정의하여 ZigBee 표준화 스펙 버전 1.0을 발표했다. ZigBee는 IEEE 802.15.4의 물리층과 매체접근제어층 위에 네트워크층과 응용지원부층(APS: Application support sublayer), 응용 프레임워크(Application framework), ZigBee디바이스객체(ZDO: ZigBee device object)를 포함하는 응용층(Application layer)으로 구성된다. ZigBee 스택 구조를 살펴보면 그림 1과 같다.

응용층은 응용 프레임워크, ZDO, APS사이의 인터페이스를 정의한다. 응용 프레임워크는 응용에 의해서 사

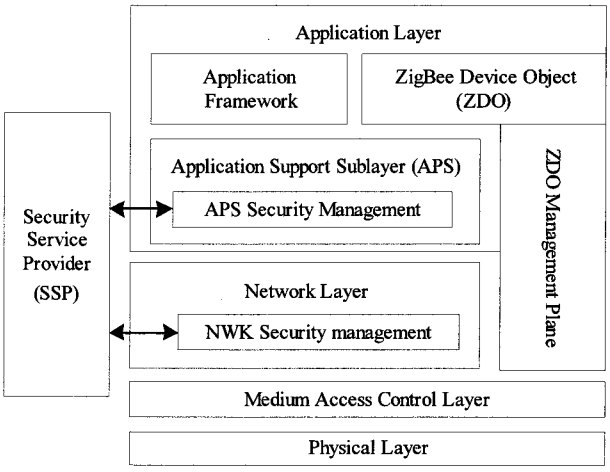

그림 1. ZigBee 스택 구조
Fig. 1. Architecture of ZigBee stack.

용되는 주소체계에 대한 내용과 응용들간의 통신 원리에 대하여 기술을 하고, ZDO는 응용 객체의 디바이스 제어와 디바이스간의 바인딩 처리 및 보안관계를 설정해주고, 응용 객체의 공용 인터페이스를 제공한다. 그리고 APS는 바인딩을 위한 테이블을 유지·관리한다.

네트워크층에서는 네트워크, 보안, 라우팅을 관리하고, 연결된 디바이스간의 메시지를 전달하며 APS의 보안 관리를 지원한다. ZigBee 네트워크층은 네트워크에 합류(Join) 또는 이탈(Leave)하는 등의 메커니즘, 전송 프레임에 대한 보안을 제공한다. ZigBee 보안 서비스는 네트워크층과 응용층과 직접적으로 연관되어 있다. 네트워크층과 응용층에서 생성되는 프레임은 각 층에서 데이터 암호화 및 무결성 검증을 위한 연산을 수행하도록 되어 있고, 이러한 기능을 담당하는 보안서비스 제공자 (SSP: Security service provider)가 모듈 형태로 존재한다. ZigBee의 보안 서비스는 대칭키 암호방식을 이용하여 두 노드간의 비밀키 설정과 인증 과정을 수행하고, 이 키를 이용하여 매체접근제어층, 네트워크층, 응용층에서의 데이터 프레임에 대한 보안 기능을 제공한다. ZigBee에서 보안을 위해 사용되는 키는 마스터키(Master key), 링크키(Link key), 네트워크키(Network key)의 세 종류의 키가 있다. 각 노드들은 링크키를 이용하여 일대일(Point-to-point) 비밀통신을 하고, 네트워크키를 이용하여 그룹 비밀통신을 한다. 마스터키는 링크키를 생성하기 위해 사용되는 비밀키이며, 생성된 링크키를 사용하여 네트워크키를 안전하게 전송한다.

2. ZigBee에서의 새로운 디바이스의 합류 과정

ZigBee 네트워크는 코디네이터(Coordinator), 라우터(Router), 엔드디바이스(End device)의 세 종류의 노드로 구성되어 있고, 보안에서 가장 중요한 신뢰센터의 역할을 코디네이터가 하도록 정의하고 있다[1]. 코디네이터는 암호화를 위한 키 분배 및 관리, 인증 등의 네트워크의 host 역할을 하며, 라우터는 네트워크 구성을 위한 라우팅을 수행한다. 그리고 엔드디바이스는 라우터를 통해서 또는 신뢰센터와 직접 데이터를 주고받을 수 있다. ZigBee 네트워크의 장점 중 하나는 새로운 디바이스를 쉽게 합류할 수 있다는 것이다. 새로운 디바이스는 네트워크를 제어하는 코디네이터에 간단한 요청을 통하여 합류될 수 있다. 즉, 네트워크에 진입한 디바이스는 먼저 비컨(Beacon) 메시지를 전송하여 합류를 위한 노드를 찾고, 선택한 라우터를 통하여 코디네이터와

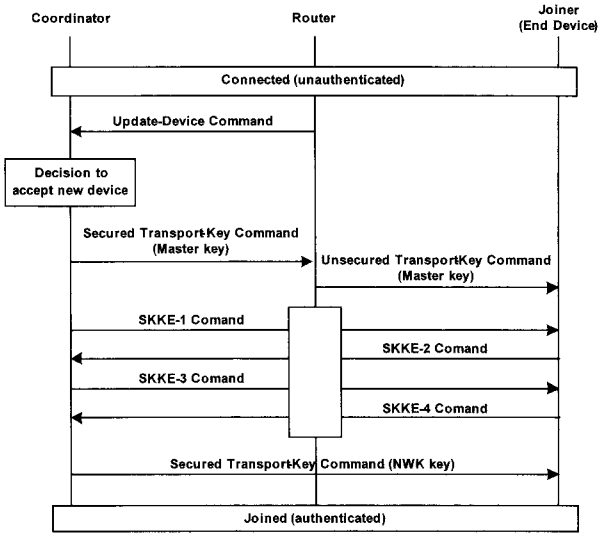

그림 2. 기존 ZigBee 네트워크에서의 새로운 디바이스의 합류 과정

Fig. 2. Key establishment process in ZigBee network.

메시지를 주고받는다. 비컨 메시지는 자신의 전파 범위 내에 존재하는 라우터 노드들에게 원홉(One-hop)으로 브로드캐스트 된다. 새로운 디바이스의 합류를 위하여, 코디네이터는 디바이스에게 마스터키를 전달하고, 이 키를 이용하여 코디네이터와 디바이스간의 새로운 링크키를 생성한다. 그리고 생성된 링크키를 이용하여 디바이스는 네트워크키를 안전하게 전송받아 네트워크에 성공적으로 합류하는 것이다. 그림 2는 새로운 디바이스가 코디네이터로부터 네트워크키를 분배 받는 과정을 나타낸 것이다. ZigBee에서는 디바이스가 네트워크키를 얻으면 합류이 된 것이다.

네트워크에 합류하고자 하는 새로운 디바이스가 네트워크키를 안전하게 전송 받는 방법을 자세히 살펴보면 다음과 같다.

1. 디바이스가 네트워크에 연결되면, 라우터는 코디네이터에게 업데이트 디바이스 명령을 보낸다.
2. 업데이트 디바이스 메시지를 받은 코디네이터는 새로운 디바이스가 네트워크에 참여되어도 되는지의 합류여부를 판단한 후, 디바이스에게 네트워크키를 분배하는 과정을 다음과 같이 진행한다. 이때, 라우터는 중간에서 중계역할을 한다.
   i) 코디네이터는 마스터키를 디바이스에게 전송한다.
   ii) 코디네이터와 디바이스는 마스터키를 이용하여 SKKE (Symmetric-key key establishment) 프

로토콜을 수행하여 링크키를 생성한다.

iii) 코디네이터는 링크키를 이용하여 네트워크키를 암호화한 값을 디바이스에게 전송한다.

iv) 디바이스는 링크키를 이용하여 코디네이터에게 전송받은 데이터로부터 네트워크키를 획득한다.

3. ZigBee 네트워크의 취약성 분석

저전력, 초소형, 저비용의 장점과 함께 ZigBee는 유비쿼터스 센서 네트워크를 구현하는 최적의 기술로 주목받고 있다. 그러나 현존하는 ZigBee 네트워크는 다음과 같은 문제점들을 가지고 있다.

1. 코디네이터는 네트워크키는 물론 네트워크에 합류한 모든 노드들의 개수만큼의 마스터키와 링크키를 다 가지고 있어야 할 뿐만 아니라 앞으로 통신하게 될 모든 노드들의 마스터키까지 전부 가지고 있어야 한다. 그렇기 때문에 네트워크상의 노드 수가 증가할수록 이에 비례하여 더 많은 저장 공간이 요구되는 키 관리상의 구조적 단점이 존재한다.
2. 코디네이터는 네트워크에 최초로 합류하는 디바이스들의 정당성에 대하여 확인을 해야 한다. 그러나 코디네이터에게는 그들의 정당성 유무에 대해 판별할 아무런 근거가 존재하지 않기 때문에, 외부의 부정한 디바이스가 네트워크에 합류하게 될 여지가 된다. 최초로 합류하는 디바이스에 관련된 인증의 부재는 ZigBee 보안 시스템의 심각한 문제점이다.
3. 만약 새롭게 합류하는 디바이스가 마스터키를 가지고 있지 않다면, 그림 2에서와 같이 코디네이터는 마스터키를 디바이스에게 전송해야 하는데, 이 과정에서 중계역할을 하는 라우터와 디바이스사이에 안전한 채널이 확보가 되어 있지 않기 때문에 마스터키는 그대로 외부로 노출이 되어버린다. 마스터키가 노출이 되면, 이후에 수행될 통신 채널의 안전성 여부와는 상관없이 누구든지 생성되는 링크키뿐만 아니라 네트워크키까지도 알 수 있게 되어버리기 때문에 네트워크 전체 보안이 무력화되어 버린다. 그러므로 마스터키의 노출 또한 ZigBee 보안 시스템의 심각한 문제점이 된다.
4. 새롭게 네트워크에 합류하려는 모든 디바이스마다 코디네이터와 연결하여 마스터키, 링크키와 네트워크키를 전송 받도록 함으로써 모든 트래픽이 코디네이터로 집중된다. 그렇게 때문에 만약 네트워크에 합류하려는 노드 수가 많아진다면 코디네이터에 부하가 치중되어 통신시간이 길어져 네트워크 시스템의 성능이 저하되는 문제점이 있다.

III. 제안하는 방식

이 장에서는 II장에서 분석한 ZigBee 네트워크의 문제점들을 개선한 새로운 ZigBee 프로토콜을 제안한다. 제안하는 프로토콜은 코디네이터의 키 관리를 간단히 하기 위하여, 시스템 ID 자체를 공개키로 이용할 수 있는 개인식별방식의 공개키 암호방식[4]을 적용하였다. ZigBee에서 각 노드들은 네트워크 내에서 유일한 주소를 부여받으며, 자신만의 주소를 부여받은 노드들은 이 주소를 통해 네트워크 내에서 독립적인 개체로 존재한다. 그리고 제안하는 프로토콜은 공개키 암호방식이 기지고 있는 계산량의 문제를 해결하기 위하여 타원 곡선 암호[5~9]를 기반으로 하여 설계한다. 타원 곡선 암호는 유한체에서 설계된 기존의 암호방식[10~12]과 비슷한 레벨의 보안성을 제공하면서도 훨씬 적은 키 사이즈를 요구하기 때문에, 센서 네트워크에 충분히 적용 가능한 공개키 암호방식으로 알려져 있다[13].

제안하는 프로토콜은 초기화 단계와 네트워크 합류 단계로 구성된다. 그림 3은 본 논문에서 제안하는 방식, 즉 새로운 디바이스가 라우터로부터 네트워크키를 분배받는 과정을 나타낸 것이다.

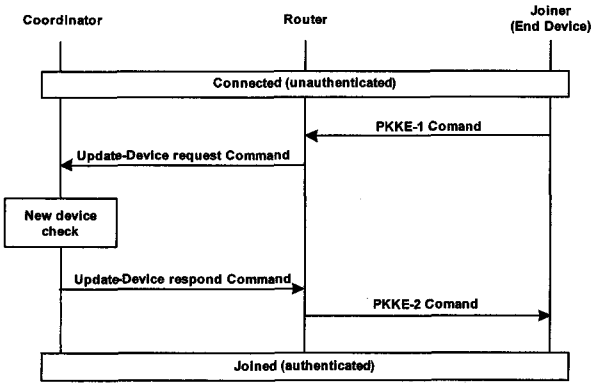

그림 3. 제안하는 ZigBee 네트워크에서의 새로운 디바이스의 합류 과정

Fig. 3. Proposed key establishment process in ZigBee network.

먼저, 본 논문에서 사용되는 파라미터들을 요약하면 다음과 같다.

- G_1 : 소수 p를 위수로 갖는 덧셈 군
- G_2 : 소수 p를 위수로 갖는 곱셈 군
- $P \in G_1$: G_1의 생성원
- $e : G_1 \times G_1 \rightarrow G_2$: 겹선형 함수*
- C : 코디네이터
- R : 라우터
- J : 디바이스
- $K_{S_C} = s \in Z_p$: 코디네이터의 비밀키
- $K_{P_C} = sP \in G_1$: 코디네이터의 공개키
- ID_i : 노드 i의 시스템 ID
- $K_{P_i} = H_1(ID_i) \in G_1$: 노드 i의 공개키
- $K_{S_i} = sK_{P_i} \in G_1$: 노드 i의 비밀키
- $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : G_1 \rightarrow Z_p$, : 해쉬함수
- $NK_N \in Z_p$: 네트워크키
- $MK_{AB} \in Z_p$: A와 B의 MAC(Message authentication code)키
- $L_{AB} \in G_1$: A와 B의 공유정보
- $LK_{AB} \in Z_p$: A와 B의 링크키
- $E_K(M)$: 키 K를 이용하여 메시지 M을 암호화
- $D_K(M)$: 키 K를 이용하여 메시지 M을 복호화

네트워크에 합류된 모든 노드들은 링크키를 이용하여 일대일 통신을 하고 네트워크키 NK_N를 이용하여 그룹통신을 한다.

[초기화 단계]

코디네이터 C는 자신의 비밀키 $s \in Z_p$와 공개키 $K_{P_C} = sP$를 생성하고, 노드의 시스템 ID (또는 노드의 고유번호나 고유주소)를 이용하여 각 노드들의 비밀키 $K_{S_i} = sH_1(ID_i)$를 계산하고 시스템 파라미터 $param = < G_1, G_2, p, P, H_1, H_2, K_{P_C} >$를 공개한다. 이때, 각 노드의 비밀키는 제작 단계에서 저장되거나 사용자가 직접 입력하는 등의 안전한 방법을 이용해 저장되고, 각 노드의 공개키는 그들의 식별정보인 시스템 ID가 된다.

그리고 부정한 디바이스가 네트워크에 참여하는 것을 방지하기 위하여, 코디네이터 C는 노드들의 주소 목록을 기록하여 저장하고, 네트워크가 설정되어 노드가 연결되면 네트워크에 합류한 노드들의 목록을 관리하는 동시에 손상되거나 취소된 노드들의 목록도 같이 관리한다. 취소목록에는 악의적인 노드, 손상된 노드, 네트워크를 탈퇴한 노드 등이 포함된다. 각 노드들은 네트워크에서 탈퇴하거나 자신의 키에 대한 손상을 감지하였을 경우, 이러한 상태를 C에게 알려주어 취소목록의 업데이트를 통보한다. 뿐만 아니라 노드들은 자신의 주변 노드들의 상태를 감시하면서 특정 노드의 부정이나 공격으로 인한 손상을 감지하는 경우, 이를 C에게 통보한다.

[네트워크 합류 단계]

1. 네트워크에 연결이 되면, 디바이스 J는 임의의 정수 $d \in Z_p$를 선택하고 $J_1 = dP$, $MK_{RJ} = e(K_{S_R}, K_{P_J}) = e(K_{P_R}, K_{P_J})^s$와 $J_2 = MAC_{MK_{RJ}}(R, J, J_1, t_1)$를 계산하여 라우터 R에게 $m_1 = (J_1, J_2)$를 전송한다. 이때, t_1는 시간정보이고, 전송되는 메시지 m_1은 그림 2에서의 PKKE-1 (Public-key key establishment-1)을 나타낸다.
2. 라우터 R은 $MK_{RJ} = e(K_{P_R}, K_{S_J}) = e(K_{P_R}, K_{P_J})^s$와 $J_2' = MAC_{MK_{RJ}}(R, J, J_1, t_1)$을 계산하여 $J_2 = J_2'$의 성립여부를 체크한다. 방정식이 성립하면 R은 C에게 J의 업데이트 요청 메시지를 전송한다. (필요하다면, C와 R은 그들의 링크키 LK_{CR}를 사용하여 안전하게 통신을 수행한다.) 만약 방정식이 성립하지 않을 경우에는 네트워크 연결과정을 종료한다.
3. C는 J가 취소목록에 등록된 디바이스인지의 여부를 검사하여 J의 정당성을 확인한 후 R에게 J의 업데이트 완료 메시지를 보낸다. 만약 J가 취소목록에 등록되어 있는 경우에는 업데이트 실패 메시지를 라우터에게 보내어 네트워크 연결과정을 종료시킨다. (이때에도 필요하다면, C와 R은 링크키 LK_{CR}를 사용하여 안전하게 통신을 수행한다.)
4. J가 업데이트되면, R은 임의의 정수 $r \in Z_p$를 선택하여 $L_{RJ} = rJ_1 = rdP$를 계산하여 J와의 링크키 $LK_{RJ} = H_2(L_{RJ})$를 생성하고, 생성된 링크키 LK_{RJ}를 이용하여 네트워크키 NK_N를 암호화 $E = E_{LK_{RJ}}(NK_N)$한다. 그리고 $R_1 = rP$과 $R_2 =$

* 겹선형 함수 $e : G_1 \times G_1 \rightarrow G_2$는 i) 모든 $P, Q \in G_1$와 $a, b \in Z_p$에 대하여 $e(aP, bQ) = e(P, Q)^{ab}$를 만족하는 겹선형성, ii) $e(P, Q) \neq 1$를 만족하는 $P, Q \in G_1$의 존재성, iii) 모든 $P, Q \in G_1$에 대한 $e(P, Q)$ 계산의 효율성을 만족하는 함수이다.

$MAC_{MK_{RJ}}(R,J,R_1,t_2)$를 계산하여 디바이스 J에게 $m_2=(R_1,R_2,E)$를 전송한다. 이때, t_2는 시간정보이고, 전송되는 메시지 m_2은 그림 2에서의 PKKE-2 (Public-key key establishment-2)를 나타낸다.

5. J는 $R_2'=MAC_{MK_{RJ}}(R,J,J_1,t_1)$을 계산하여 $R_2=R_2'$의 성립여부를 체크하고, $L_{RJ}=dR_1=rdP$를 계산하여 R과의 링크키 $LK_{RJ}=H_2(L_{RJ})$를 생성한다. 그리고 생성된 링크키 LK_{RJ}를 이용하여 암호문 E를 복호화 $D_{LK_{RJ}}(E)=NK_N$하여 네트워크키 NK_N를 획득한다. J가 네트워크키를 획득하면 J는 네트워크 합류에 성공한 것이다.

Ⅳ. 제안하는 방식의 안전성과 효율성

제안하는 프로토콜은 기존에 사용하였던 마스터키를 없애, 비밀키 개수와 통신횟수를 감소시킴으로써 효율성은 물론 안전성까지 개선시켰다. 또한 코디네이터가 노드에 관련된 여러 정보들의 목록을 관리함으로써 부정한 디바이스가 네트워크에 참여하는 것을 방지하여 네트워크의 안전성을 더욱 증가시켰다, 이 외에도, 제안한 프로토콜에서는 MAC에 시간정보를 포함하여 재전송 공격에 대비할 수 있도록 설계하였다.

그리고 제안하는 프로토콜에서는 코디네이터가 자신의 비밀키와 네트워크키, 그리고 자신과 직접 연결된 노드간의 링크키만 관리하도록 함으로써 코디네이터의 키 관리를 간편화하였고, 네트워크에 합류하려는 새로운 디바이스는 가까운 위치에 있는 라우터로부터 직접 네트워크키를 전송 받을 수 있도록 설계하여 기존의 코디네이터로 집중되었던 트래픽을 여러 라우터에게 분산시킴으로써 네트워크의 부하를 해결하고 디바이스의 네트워크 합류시간을 감소시켜 네트워크의 효율성을 향상시켰다.

또한 디바이스가 가까운 위치에 있는 라우터로부터 직접 네트워크키를 전송 받을 수 있도록 설계하였기 때문에, 제안하는 방식은 멀티홉(Multi-hop) 환경에 적용될 경우에 더욱 더 효율적인 프로토콜이다. 코디네이터와 디바이스 사이에 이루어지는 기존의 ZigBee의 키 분배 방식에서는 메시지 개수는 코디네이터와 디바이스 사이의 홉 수에 비례한다. 그러므로 기존 ZigBee에서 링크키와 네트워크키의 분배를 위해서 h홉 떨어져 있는 코디네이터와 디바이스 사이에 주고받는 메시지 개수는

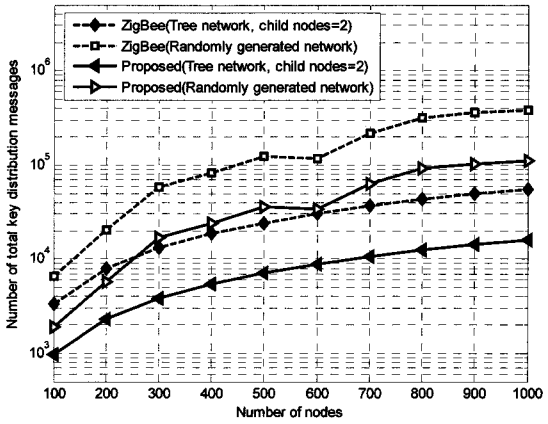

그림 4. 제안하는 ZigBee 네트워크와 기존의 ZigBee 네트워크에서 키분배를 하기 위한 메시지 개수 비교

Fig. 4. The number of the key distribution messages of the proposed ZigBee network protocol and typical ZigBee protocol.

$O(7h-1)$개가 된다. 이에 비하여 제안한 프로토콜은, 코디네이터를 통해서만 키분배 과정을 수행할 수 있는 기존 방식과는 달리, 라우터와 디바이스 사이에서 직접 키가 분배되므로 메시지의 개수가 $O(2h)$로 급격하게 줄어든다. 그림 4는 기존의 ZigBee 프로토콜과 제안한 프로토콜의 키 분배 방식에 대한 메시지 복잡도를 비교한 것이다.

ZigBee 네트워크는 스타, 트리, 메쉬 토폴로지를 지원한다. 본 논문에서는 메시지의 복잡도를 비교하기 위해서 자식노드가 2개인 2진 트리 구조의 네트워크와, 임의의 위치에 노드를 생성하고 이에 따라 임의로 생성된 네트워크에서, 키 분배를 위한 메시지 개수를 비교한다. 임의로 네트워크를 형성할 때, 일정한 영역의 중심에 코디네이터 노드를 두고, 코디네이터에서 가까운 노드가 첫 번째로 네트워크에 연결된다. 네트워크에 연결되지 않은 노드 중에서 네트워크에 가까운 노드의 순서로 네트워크에 연결된다. 프로토콜의 성능을 측정하기 위해서 메시지 복잡도[14]를 이용하였다. 그림 5는 위의 방법으로 만들어진 트리 구조에서 신뢰센터와 각 노드 사이에 교환되는 메시지 개수를 나타낸다. 제안한 방법은 초기 네트워크를 구성할 때 보안 키 분배를 위해 사용되는 메시지 개수를 기존의 29% 수준으로 줄일 수 있다. 또한 그림 5와 같이 신뢰센터에서 전송하는 메시지의 개수도 25% 감소하며, 그림 6에서처럼 각각의 노드에서 전송되는 메시지도 29%이하 수준으로 감

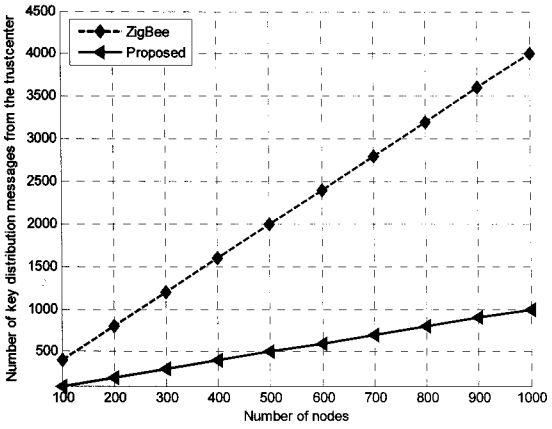

그림 5. 제안하는 방식과 기존 ZigBee 방식에 따라 키 분배를 위해 신뢰센터에서 전송하는 메시지 개수 비교

Fig. 5. The number of the key distribution message that transmitted from turstcenter.

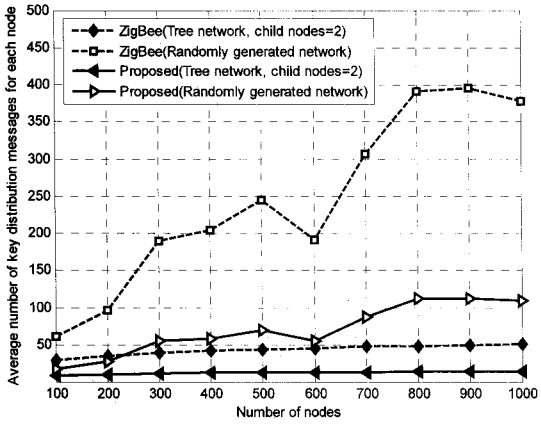

그림 6. 제안하는 방식과 기존 ZigBee 방식에 따라 신뢰센터를 제외한 노드에서 키분배를 위해 전송하는 메시지의 평균 개수 비교

Fig. 6. The average number of the transmitted key distribution message per node.

소한다. 배터리 전원을 이용하여 동작하는 센서네트워크의 경우에 키 분배과정에서 1/3 수준 이하로 전력소비를 줄일 수 있다. 각각의 노드를 통해서 교환되는 메시지의 개수는 홉 수가 증가할수록 늘어나므로, 네트워크에 참여하고자 하는 노드의 개수가 늘어날수록 필요한 메시지 수도 증가하게 된다. 그러므로 제안된 프로토콜은 노드의 개수가 많은 센서 네트워크에서 더욱 효과적이다. 그림 6에서처럼 네트워크의 구성에 따라서 노드 개수가 증가할 경우에 평균 노드의 메시지 전송수는 오히려 줄어들 수는 있다. 하지만 이러한 경우에도 신뢰센터 주변에서 중계역할을 하는 노드는 노드 수가 늘어남에 따라 많은 메시지를 전송하기 때문에, 네트워크의 동작 시간은 노드 수가 증가할수록 짧아진다.

V. 결 론

ZigBee는 저전력, 초소형, 저비용으로 제어와 모니터링을 가능하게 하는 전 세계적으로 유일한 무선통신표준으로 주목받고 있다. 그러나 본 논문에서는 복잡한 키관리와 인증 등의 부재로 ZigBee 보안 시스템에 심각한 취약성이 있음을 밝히고, 이를 해결하는 새로운 프로토콜을 제안하였다. 제안한 방식은 별도의 복잡한 키 관리를 필요로 하지 않는 공개키 암호방식을 기반으로 설계한 새로운 프로토콜로써, 기존 ZigBee 시스템의 보안을 강화시키고 네트워크의 성능을 향상시킨 개선된 프로토콜이다. 본 논문에서는 시뮬레이션을 통해 제안한 프로토콜의 우수성을 검증하였다.

참 고 문 헌

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

[2] "Standard for part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (LR-WPAN)," IEEE Std 802.15.4, 2003.

[3] NIST, "Announcing the Advanced Encryption Standard(AES)," FIPS PUB ZZZ, 2001, available at http://www.nist.gov/aes.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes," Proc. Advances in Cryptology, Crypto'84, Springer-Verlag, LNCS 196, pp. 47~53, 1985.

[5] V. Miller, "Use of elliptic curves in cryptography," Proc. Advances in Cryptology, CRYPTO'85, Springer-Verlag, LNCS 218, pp. 417~426, 1986.

[6] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203{209, Jan. 1987.

[7] D. Bonech, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," Proc. Advances in Cryptology, Asiacrypt 2001, Springer-Verlag, LNCS 2248, pp. 514~532, Dec. 2001.

[8] 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.
[9] 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/.
[10] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, vol. 22, no. 6, pp. 644~654, Nov. 1976.
[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method of obtaining digital signature and public key cryptosystem," ACM Communication, vol. 21, no. 2, pp. 120~126, Feb. 1978.
[12] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Inform. Theory, vol. IT-31, no. 4, pp. 469~472, July 1985.
[13] N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," Proc. Cryptographic Hardware and Embedded Systems (CHES 2004), Springer-Verlag, LNCS 3156, pp. 119~132, Aug. 2004.
[14] C. C. Shen, C. Srisathapornphat, R. L. Z. Huang, C. Jaikaeo, and E. L. Lloyd, "CLTC: A cluseter-based topology control framework for ad hoc networks," IEEE Trans. Mobile Computing, vol. 3, no. 1, pp. 18~32, Jan.~Mar. 2004.

저 자 소 개

김 현 주(정회원)
1995년 세명대학교 수학과 학사 졸업.
1997년 서강대학교 수학과 석사 졸업.
2005년 성균관대학교 전기전자및 컴퓨터공학과 박사 졸업.
2005년~2007년 성균관대학교 정보통신공학부 연구교수.
2007년~현재 연세대학교 전기전자공학부 연구교수.
<주관심분야 : 통신네트워크보안, 암호이론>

정 종 문(정회원)
1992년 연세대학교 전자공학과 학사 졸업.
1994년 연세대학교 전자공학과 석사 졸업.
1999년 Pennsylvania State University, Electrical Engineering 박사 졸업.
1997년~1999년 Pennsylvania State University, Electrical Engineering, Faculty Instructor 및 조교수
2000년~2005년 Oklahoma State University, Electrical and Computer Engineering 부교수(정년보장)
2005년~현재 연세대학교 전기전자공학과 부교수
<주관심분야 : 무선통신, 이동통신망, Ad Hoc 망, 정보이론, 통신보안>