논문 2006-43TC-11-7

공개키 방식의 LR-WPAN 보안 알고리즘

(Public Key based LR-WPAN Security Algorithm)

김 진 철*, 오 영 환**

(Jin-cheol Kim and Young-Hwan Oh)

요 약

센서 노드의 저전력, 저가격을 지향하는 Low Rate WPAN (Wireless Personal Area Network)은 유비쿼터스 환경을 실현하는 중요한 기술이다. LR WPAN의 표준화를 담당하고 있는 IEEE 802.15.4와 ZigBee Alliance에서는 대칭키 방식의 키 설정 및 관리 프로토콜인 SKKE (Symmetric -Key Key Establishment)를 권고하고 있으나, 키의 생성과 교환에서 전자서명과 같은 인증과정이나 보안 알고리즘의 부재로 보안에 취약성이 있다. 본 논문에서는 위에서 서술한 LR WPAN의 보안적인 문제점들을 해결하기 위하여 공개키 기반의 키 교환 및 보안 알고리즘을 제안하였다. 또한 통신 신뢰성 및 보안에 대한 취약성을 가지는 전력선 통신 기반의 원격검침시스템의 단점을 보완할 수 있는 IEEE 802.15.4 WPAN 기반의 원격검침 모델을 제시하고, 원격검침 프로파일에 제안한 보안 알고리즘을 적용함으로써 보안성을 향상시키도록 하였다.

Abstract

Low Rate WPAN (Wireless Personal Area Network) designed for low power and low cost wireless communication is an important technology to realize ubiquitous environment. IEEE 802.15.4 and ZigBee Alliance recommend the SKKE (Symmetric-Key Key Establishment) protocol for key establishment and management. The SKKE algorithm has security weakness such as the absence of authentication process or electric signature in key generation and exchange when devices join the role of coordinators. In this paper, we propose new key establishment and security algorithm based on public key encryption to solve low rate WPAN security problems. Also, to improve PLC AMR system's weaknesses in communication reliability and security, we propose a new AMR system model based on IEEE 802.15.4 and we apply our security algorithm to AMR profile for security enhancement.

Keywords: IEEE 802.15.4, ZigBee, 공개키 보안 알고리즘, 원격검침

I. 서 론

센서 노드의 저전력, 저가격을 지향하는 Low Rate WPAN (Wireless Personal Area Network)은 유비쿼터스 환경을 실현하는 중요한 기술이다. 다수의 센서 노드간 통신방식은 통신 인프라가 없는 환경에서 이동 노드들만으로 구성된 자율적이고 수평적인 통신을 할 수 있는 MANET (Mobile Ad-hoc Network)과 네트워크 패러다임 측면에서 유사하다.

Stajano 등이 거의 처음으로 Ad hoc 네트워크에서 보안의 중요성을 언급하였고, 보안에 대한 이슈가 가장 중요한 것이 될 것이며, 실생활에서의 예를 들어 문제제기를 하였다.[1] 그 이후의 연구들에서도 같은 결론에 도달하였다.[2],[3] 최근 Ad hoc 네트워크 보안에 대한 연구들은 네트워크에서 일부의 또는 모든 디바이스들에게 인증 권한 역할을 분산하는 연구들을 진행하였는데, 주요 접근 방법은 "Threshold Cryptograghy" 기반이다. 하지만 대부분의 이러한 접근 방법들은 그다지 효율적이지 못하다는 단점이 있다.[4~8] Yih-Chun Hu 등은 Ad hoc 네트워크 라우팅 보안 알고리즘인 Ariadne (A Secure On-Demand Routing Protocol for Ad Hoc Networks)을 제안하였다. 이들은 DSR (Dynamic Source Routing) 경로설정 프로토콜에 TESLA (Timed

* 정회원, 한전KDN(주) 전력IT연구원
(Korea Electric Power Data Network)
** 종신회원, 광운대학교 전자통신공학과
(Dept. of Electronics and Communications Engineering, Kwangwoon Univ.)
접수일자: 2006년10월10일, 수정완료일: 2006년11월18일

Efficient Stream Loss-tolerant Authentication) 해쉬 체인 방법을 적용하였다.[9] MANET 라우팅 프로토콜 보안에 관한 연구들은 Self Securing과 같은 키 분배 알고리즘에 의해서 사전에 비밀키가 분배되고 노드들에 대한 인증이 이루어진 것으로 가정함으로써, 키 분배 및 관리 과정을 생략하고 비밀키를 MAC (Message Authentication Code)키로 사용한다.[9],[10],[11]

LR WPAN의 표준화를 담당하고 있는 IEEE 802.15.4와 ZigBee Alliance에서는 대칭키 방식의 키 설정 및 관리 프로토콜인 SKKE (Symmetric -Key Key Establishment)를 권고하고 있으나, 키의 생성과 교환에서 전자서명과 같은 인증과정이나 보안 알고리즘의 부재로 보안에 취약성이 있다.

세계 각국 유수의 전력회사들은 전력산업 구조개편에 따른 경쟁력 확보와 투자 대비 효율성 측면에서 원격검침 시스템을 검침 용도로만 활용할 뿐 아니라 발전 및 배전 시스템의 효율적인 운영과 수용가를 위한 부가서비스 차원에서 활용 가능한 시스템으로 구축하고자 한다. 전력회사에서 고려 중인 부가서비스에는 전력 수요 관리, 정전 예보, 도전 방지, 홈 네트워크 등으로, 이러한 부가서비스들은 전력망 기반으로 이루어지기 때문에 수용가와 가장 밀접한 검침 네트워크를 통해서 이루어질 가능성이 크다.[12]

국내 저압 원격검침 시범사업은 PLC (Power Line Communication) 방식으로 추진하고 있다. 전력선 통신 방식의 원격검침은 전력회사의 고유자원인 전력선을 통신 전달 매체로 활용 가능하고 인터넷 서비스 등 대용량 데이터 서비스 가능하다는 장점이 있다. 고객의 개인 정보 및 요금 관련 정보로 이루어진 원격검침 데이터는 보안성이 높아야 하지만 전력선 통신 방식은 여러 가지 문제점을 안고 있다. 저속 PLC 방식은 업체들간 이견으로 표준 프로토콜을 거의 사용하지 않고 있으며, 오버헤드가 많아 속도가 너무 느리고, 단순 암호화 알고리즘만 사용함으로써 보안적으로 취약하다는 단점이 있다. 고속 PLC 방식은 표준화가 아직 미비하고, 발열 현상으로 인한 문제점과 56bit DES 알고리즘을 사용하여 통신의 신뢰성과 보안성이 떨어지며, 효과 대비 비용이 높다는 단점이 있다.[13~16]

본 논문에서는 위에서 서술한 LR WPAN의 보안적인 문제점들을 해결하기 위하여 공개키 기반의 키 교환 및 보안 알고리즘을 제안하였다. 또한 통신 신뢰성 및 보안에 대한 취약성을 가지는 전력선 통신 기반의 원격검침시스템의 단점을 보완하기 위하여 IEEE 802.15.4 WPAN 기반의 원격검침 모델을 제시하고, 보안 대상이 되는 원격검침 프로파일을 설계하였다. Ⅱ장에서는 기존 MANET에서의 보안 알고리즘 연구들과 LR-WPAN (IEEE802.15.4와 ZigBee)의 키 교환 알고리즘인 SKKE 프로토콜 특징을 검토하고, Ⅲ장에서는 공개키 기반의 WPAN 보안 알고리즘을 제안하고, Ⅳ장에서는 LR-WPAN 원격검침 시스템에 제안한 보안 알고리즘을 적용한 실험 결과를 제시하고, Ⅴ장에서는 제안한 보안 알고리즘과 기존 알고리즘과의 성능을 평가하고 마지막으로 Ⅵ장에서 결론을 맺는다.

Ⅱ. WPAN 보안 알고리즘

1. MANET 보안 알고리즘

MANET에서 보안을 향상시키는 매커니즘은 키 분배 및 관리, 라우팅 보안, Threshold Cryptography 기반의 손상(Compromised)된 노드 검색(detection) 등의 방법이 있다. 첫째, 키 분배 및 관리는 인증(Authentication)과 관련있는 부분으로 안전하게 키를 생성하고, 분배하는데 중점을 둔다. 둘째, 라우팅 보안은 Confidentiality와 Data Integrity와 관련 있는 부분으로 인접(intermediate) 노드들간의 라우팅 메시지가 안전하게 송수신 되도록 한다. 셋째, 손상된 노드 검색은 Availability와 관련 있는 부분으로 n개의 노드들로 이루이진 MANET이 k-1개의 노드가 손상될 때까지 안전하다는 가정하에 공개키 기반의 비밀공유분을 공유하고 기존 유·무선 네트워크에서의 인증기관의 역할을 노드들이 분산하여 수행하는 것이다.

MANET에서 키 분배 및 관리는 대칭키 방식의 키 설정 방법과 공개키 방식의 키 설정 방법으로 분류된다. 대칭키 방식의 키 설정 방법에는링크 키를 유도하는 두 개의 대칭키 프로토콜이 제안되었는데, SKKE 프로토콜과 UKE (Unprotect Key Establishment) 프로토콜이다. SKKE 프로토콜에서 믿을 수 있는 연결은 마스터키를 사용해서 이루어진다. 마스터키는 생산되는 과정에서 pre-installed되거나, 어떤 암호학적인 방법을 사용해서 유도하거나, KDC를 사용해서 분배해주는 방법을 사용한다. 마스터키의 비밀성과 인증은 SKKE 프로토콜을 수행하는데 있어서 가장 중요하다. UKE 프로토콜은 마스터키는 고정되어 있다. 이러한 경우에 악의 있는 공격자가 마스터키를 알 수가 있다. UKE 프로토콜에서 믿을 수 있는 연결은 초기에 메시지를 교환하면서 얻어지는 디바이스의 IEEE 64 비트 주소를 사용해

서 이루어진다. 이렇게 유도된 링크키는 어떤 암호학적인 보안을 제공하지 않는다. UKE 프로토콜은 보안성이 낮아도 되는 환경에서 유용하고, 마스터키를 교체를 하지 못하는 low cost 환경에 적당하다. UKE나 SKKE 프로토콜을 구현하기 위해서는 AES block cipher와 unkeyed hash 함수(Matyas- Meyer-Oseas hash)와 random number generator가 필요하다. AES 알고리즘이 수행될 수 있는 하드웨어와 소프트웨어가 필요하다. 공개키 방식의 키 설정 프로토콜로는 PKKE (Public-Key Key Establishment) 프로토콜과 CBKE (Certificate-Based Key Establishment) 프로토콜이 있다. PKKE 프로토콜은 키 연결 과정을 모니터링해서 도청하는 passive 공격을 막는데 사용한다. 디바이스의 신뢰는 공개키와 그에 상응하는 디바이스의 ID의 교환으로 이루어진다. 이러한 방법에서 어떤 누구도 공개키가 누구의 키인지 확인을 할 수가 없다. 따라서 공개키와 적당한 디바이스의 ID의 적당한 증명을 제공하는 환경에 의존한다. PKKE 프로토콜은 CA를 채택한 네트워크 어플리케이션에서 사용하기 적당하다. CBKE 프로토콜은 인증서와 루트 키의 공개키 기술을 사용한다. 디지털 서명은 인증기관에 의해서 서명된 디바이스의 64비트 IEEE 주소와 함께 단순한 공개키를 사용한다. 인증서는 누구의 공개키인지 디바이스가 네트워크의 합법적인 사용자인지를 암호학적으로 확인하는 메커니즘을 제공할 수 있다. 인증서와 루트 키는 안전하게 제공되어져야 되고 active 공격과 passive 공격에 강해야 한다.[17]

라우팅 보안 프로토콜은 Self Securing과 같은 키 분배 알고리즘에 의해 미리 분배되어 있는 비밀키를 MAC (Message Authentication Code)키로 사용하여 TESLA 또는 이중 해쉬 함수를 통하여 RREQ 패킷과 RREP 패킷을 안전하게 전송하는 알고리즘이다. TESLA는, 대칭키 암호화방법으로, 공유 키(shared key)에 의한 attack을 방지하기 위하여 'loose time synchronization'과 'delayed key disclosure'개념을 사용한다. Sender는 'Kn, Kn-1', ... ,K0'의 key chain을 형성하고 'K0,'...'',Kn'의 순서로 key publication을 한다. 패킷을 전송하고 일정시간이 지난 후(packet delivery time + a)에 publish될 key(Ki)로 MAC값을 계산하여 함께 전송한다. Receiver는 패킷을 받았을 때, key Ki가 아직 publish되지 않았다는 보안 상태(Security Condition)를 점검하고, 유효하면 Sender가 Ki를 publish할 때까지 패킷을 버퍼링해 두었다가, key publication후 패킷을 인증하게 된다. 패킷이 전송되는 중간에는 shared key가 유출되지 않으므로 attack을 방지할 수 있다. 라우팅 보안 프로토콜들은 다음의 조건을 만족한다. 첫째, Self Securing과 같은 키분배 알고리즘에 의하여 각각의 노드는 자신의 개인키를 인식하고 있으며, 주변 노드의 공개키를 인식하고 있어야 한다. 둘째, 키분배 알고리즘으로 분배된 공개키와 개인키를 가지고 각 노드는 서로 MAC키를 알고 있다. 셋째, 경로상의 모든 노드는 PGP(Pretty Good Privacy)와 같은 프로토콜에 의해서 신뢰도가 검증된 노드이다.[9],[10],[11]

Threshold Cryptography 기반의 손상된 노드 검색 알고리즘들은 인증기관의 역할을 k개(k-threshold) node에 분산시키는 방법이다. 이 알고리즘들은 비밀 공유분(secret share) 분산 단계, 인증 서비스(certification service) 단계, 비밀 공유분 업데이트 단계로 이루어진다. 첫째, 비밀 공유분 분산 단계는 전체 네트워크의 비밀 키(SK : Secret Key)를 k개의 node에게 비밀 공유분(secret share)의 형태로 분산시키는 단계이다. 여기서 SK는 위 방법에서 CA의 개인 키처럼 전체 네트워크의 보안을 책임지는 비밀 키이다. 이 과정은 system bootstrapping 단계에서 이루어지며, 우선 임의로 k-1 degree의 secret polynomial f(x)를 선택한다. (단, f(0)=SK) 그리고, secret share는 secret polynomial f(x)에 의해 'f(vi) mod n'형태로 형성된다.(vi = node id). 비밀 공유분을 가지고 있는 노드는 자신의 비밀 공유분으로부터 SKi, 즉 부분 비밀 키(partial secret key)를 만들 수 있고, 결과적으로, 여러 비밀 공유분 중에서 임의의 k개만 있으면 k개의 부분 비밀 키부터 SK를 복구할 수 있다. 둘째 인증 서비스 단계에서는 어떤 노드가 인증 서비스를 요청하면, 주위의 k개의 비밀 공유분을 보유한 인접 이웃 노드들이 부분 인증서(Partial Certificate)를 인증 서비스를 요청한 노드에게 전송한다. 여기서 부분 인증서는 부분 비밀 키로 서명된 값이다. 인증 서비스 요청 노드는 k개의 부분 인증서를 모아서 완성된 인증서(complete certificate)를 얻고 인증받을 수 있게 된다. 셋째, 비밀 공유분 업데이트 단계는 하나의 손상된 node개수가 k개가 되기 전까지는 MANET은 안전할 수 있으므로, 비밀 공유분을 주기적으로 업데이트한다.[4~8]

2. ZigBee 보안 알고리즘

ZigBee에서는 정보의 처리, 전달 및 저장을 안전하게

하기 위해선 보안이 필요하다. 특히 개방된 환경에서의 보안의 중요성은 더욱더 중요하다. 이러한 ZigBee 보안에서 필요로 하는 보안 기능으로는 암호 알고리즘, 키 관리 및 보안 프로토콜, 인증 및 secure routing, secure data 등으로 암호화하는 것이 필요하다. ZigBee Security 1.0 Specification에서 지원하는 보안의 특성은 다음과 같다.[18]

- Access Control List : 리스트 테이블에 있는 디바이스만이 통신이 가능하다.
- Freshness Counter : Incoming and outgoing freshness counter를 사용하여 공격자로부터 오는 반복적인 패킷을 차단한다.
- Integrity Code : 어떤 공격자가 전달되는 패킷을 modify하는 것을 막기 위해 패킷의 마지막에 Integrity Code를 붙여 패킷의 무결성을 체크할 수 있다. 0, 32, 64, 128 bit의 Integrity Code를 지원하며 Integrity Code가 크면 메시지가 커지게 되므로 적절한 것을 사용해야 한다.
- Authentication : Network Key와 Link Key를 이용하여 네트워크 레벨과 디바이스 레벨로 인증을 지원하고 있다.
- Encryption : ZigBee는 128-bit AES를 사용하고 Network Key와 Link Key를 이용하여 네트워크 레벨과 디바이스 레벨로 데이터를 암호화하여 패킷을 전송할 수 있다.

그림 1은 보안 프로토콜 스택 구조로서, 네트워크 계층(Network Layer)과 응용 지원 하부 계층(Application Support Sublayer)에서는 보안 서비스 제공자(Security

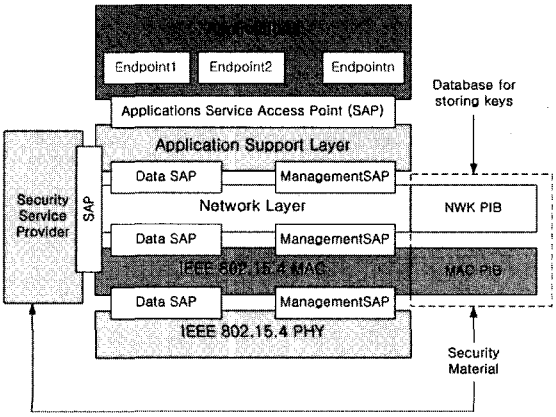

그림 1. ZigBee 프로토콜 스택 구조
Fig. 1. ZigBee Protocol Stack Structure.

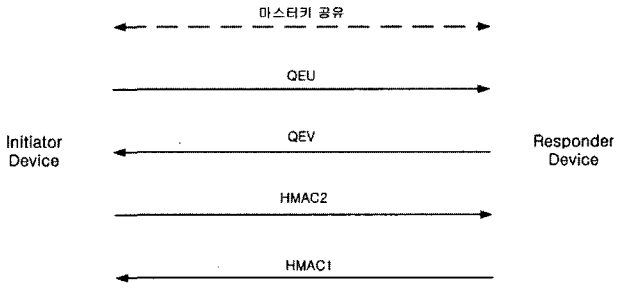

그림 2. SKKE 프로토콜
Fig. 2. SKKE Protocol.

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.

SKKE 프로토콜은 initiator 디바이스와 responder 디바이스 사이에서 믿을 수 있는 비밀키를 사용해서 새롭게 믿을 수 있는 관계를 만드는 방법이다. 즉 initiator 디바이스와 responder 디바이스가 비밀키(마스터키)를 사용해서 initiator 디바이스와 responder 디바이스가 믿을 수 있는 새로운 키(링크키)를 유도하는 과정을 의미한다. SKKE 프로토콜을 통해서 initiator 디바이스와 responder 디바이스는 다음과 같은 결과를 얻을 수 있다. 첫째로 initiator 디바이스와 responder 디바이스는 링크키를 안전하게 공유할 수 있다. 둘째로 initiator 디바이스와 responder 디바이스는 키 confirmation을 확인할 수 있다. 셋째로 initiator 디바이스와 responder 디바이스는 안전한 채널을 확보할 수 있다.[18]

그림 2는 SKKE 프로토콜을 보여주고 있다. QEU는 initiator 디바이스에서 발생한 임의의 비트 스트링이고, QEV는 responder 디바이스에서 발생한 임의의 비트 스트링이다. $MacTag_2$은 initiator 디바이스에서 계산한 $HMAC_2$ 값이고, $MacTag_1$은 responder 디바이스에서 계산한 $HMAC_1$ 값이다.

그림 3은 마스터키를 가지고 있지 않은 디바이스가 코디네이터에게 조인을 할 때, 코디네이터가 디바이스를 인증한 후 네트워크 키를 전송해주는 과정을 보여주고 있다. 디바이스가 Beacon 신호를 코디네이터와 주고

받은 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.

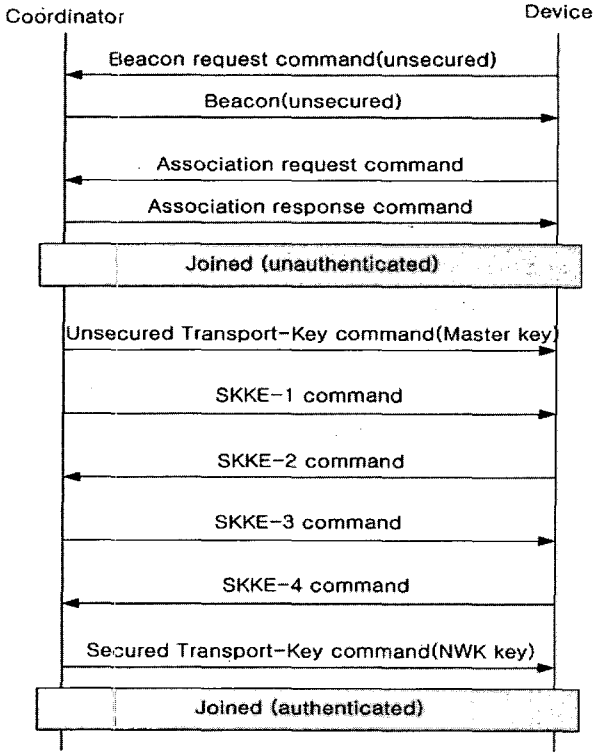

그림 3. 코디네이터와 디바이스 간의 인증 및 키 연결 과정

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

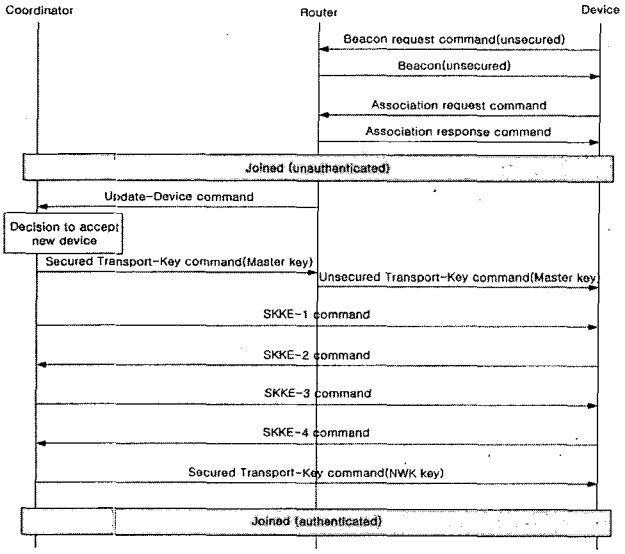

그림 4. 라우터를 통해서 조인한 디바이스와 코디네이터 간의 인증 및 키 연결 과정

Fig. 4. Authentication and Key Establishment Process between Coordinator and Device through Router.

그림 2-11 은 마스터키를 가지고 있지 않은 디바이스가 라우터를 통해서 코디네이터에게 조인할 때, 코디네이터가 디바이스를 인증하는 과정을 보여주고 있다. 중간에서 라우터가 중계 역할을 해주는 것만 빼고는 그림 2-11과 같은 과정을 통해서 인증과정이 수행되어진다. 디바이스가 코디네이터에게 인증과정이 설공하면 디바이스는 네트워크 키를 코디네이터에게 받게 된다.

여기서, 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 뜻한다.

III. 공개키 기반의 WPAN 보안 알고리즘

제안한 공개키 기반의 WPAN 보안 알고리즘은 그림 4와 같이 네 과정으로 이루어진다.

첫째, 키 설정(Key Establishment) 과정은 IEEE 802.15.4 노드간 안전하게 키를 생성하고 상호 인증과 키를 교환하는 과정으로 코디네이터와 라우터간 키를 생성하고 상호 인증과 키를 교환하는 알고리즘과 디바이스와 코디네이터간 라우터를 통해 키를 설정하고 상호 인증과 키를 교환하는 알고리즘으로 되어 있다. 둘째, 데이터 암복호화 (Data Encryption/Decryption) 과정은 데이터를 코디네이터와 라우터간, 코디네이터와 디바이스간, 라우터와 디바이스간 데이터를 암복호화하는 알고리즘으로 되어 있다. 셋째, 키 및 Trust 데이터

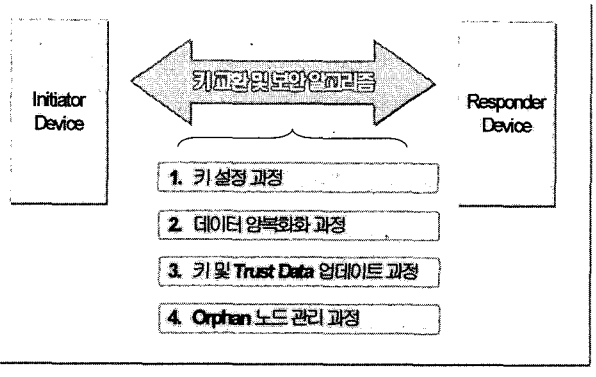

그림 5. 제안한 키 교환 및 보안 알고리즘

Fig. 5. Proposed Key Establishment & Security Algorithm.

업데이트 과정은 키 설정 과정에서 설정한 키와 Trust 데이터를 주기적으로 업데이트하는 알고리즘이다. 넷째, Orphan 노드 관리 과정은 WPAN상의 코디네이터나 라우터의 장애시 노드들이 Orphan 디바이스가 되어 네트워크 재등록 과정시 안전하게 네트워크에 등록하는 알고리즘이다.

1. 키 설정 과정

제안한 키 설정 과정은 코디네이터와 라우터간 키 설정 알고리즘과 코디네이터와 디바이스간 키 설정 알고리즘으로 되어 있다. 제안한 알고리즘은 공개 키 기반의 키 설정 프로토콜이며, 각 IEEE 802.15.4 노드에서 생성된 공개 키와 개인 키를 각각 링크 키와 서명 키로 정의한다. 링크 키는 홉간(hop-by-hop) 데이터 암복호화에 사용되고, 서명 키는 디바이스 인증시 사용한다. 제안한 알고리즘은 반드시 인증과정을 거치고, 인증서의 기능과 유사한 Trust 데이터를 코디네이터가 생성하여 상대 노드에게 전송한다. Trust 데이터는 WPAN이 메쉬(Mesh) 토폴로지로 동작할 때도 코디네이터의 인증 과정을 생략하고 IEEE 802.15.4 노드간 Trust 데이터를 상호 교환하여 인증하고 통신하기 위해서 생성한다.

제안한 키 설정 과정은 다음과 같다.

[초기상태]

- 64bit IEEE address, 채널(Channel), 최대 홉(hop) 수, 최대 등록 디바이스 수, 마스터 키, 시퀀스 번호(Sequence Number) 정의

(1) 코디네이터와 라우터간 키 설정 알고리즘

[단계 1] 키 생성

- 코디네이터는 공개 키 알고리즘을 이용하여 자신의 공개 키(링크 키)와 개인 키(서명 키) 생성
- 라우터는 공개 키 알고리즘을 이용하여 자신의 공개 키(링크 키)와 개인 키(서명 키)를 생성

[단계 2] 라우터 인증

- 라우터가 코디네이터에게 Join을 요청
- 코디네이터는 마스터 키로 자신의 링크 키를 암호화하여 라우터에게 전송
- 라우터는 코디네이터의 링크 키로 자신의 IEEE address와 링크 키를 전송
- 코디네이터는 마스터 키와 IEEE address를 통하여 라우터 인증

[단계 3] 라우터의 Trust 데이터 생성과 확인

- 코디네이터는 라우터의 링크 키, IEEE address, 사용주기로 이루어진 라우터의 Trust 데이터를 코디네이터의 서명 키로 전자서명하여 라우터에게 전송
- 라우터는 자신의 Trust 데이터를 확인하고, 자신의 Trust 데이터를 라우터 자신의 서명 키로 전자서명하여 코디네이터에게 전송
- 코디네이터는 라우터의 링크 키로 복호화하여 확인

[단계 4] 네트워크 키 생성 및 전송

- 코디네이터는 네트워크 키를 생성
- 코디네이터는 네트워크 키와 16 bit short address를 라우터의 링크 키로 암호화하여 라우터에게 전송

(2) 코디네이터와 디바이스간 키 설정 알고리즘

[단계 1] 디바이스 키 생성 및 인증

- 디바이스는 공개 키 알고리즘을 이용하여 자신의 공개 키(링크 키)와 개인 키(서명 키)를 생성
- 디바이스가 라우터에게 Join을 요청
- 라우터는 코디네이터에게 디바이스가 Join을 요청했음을 알림
- 라우터는 마스터 키로 코디네이터의 링크 키와 라우터의 링크키를 암호화하여 디바이스에게 전송
- 디바이스는 코디네이터의 링크 키로 자신의 IEEE address와 링크 키를 라우터에게 전송하고 라우터는 이를 코디네이터에게 전달
- 코디네이터는 마스터 키와 IEEE address를 통하여 디바이스 인증

[단계 2] 디바이스의 Trust 데이터 생성과 확인

- 코디네이터는 디바이스의 링크 키, IEEE address, 사용주기로 이루어진 디바이스의 Trust 데이터를 코디네이터의 비밀 키로 전자서명하여 라우터에게 전송하고 라우터는 이를 디바이스에게 전달
- 디바이스는 자신의 Trust 데이터를 확인하고, 자신의 Trust 데이터를 디바이스 자신의 비밀 키로 전자 서명하여 라우터에게 전송하고 라우터는 이를 코디네이터에게 전달
- 코디네이터는 라우터의 링크 키로 복호화하여 확인

[단계 3] 디바이스로의 네트워크 키 전송

- 코디네이터는 디바이스의 링크 키로 네트워크 키와 16bit short address를 암호화하여 라우터에게

전송
- 라우터는 디바이스에게 이를 전달

2. 데이터 암복호화 과정

제안한 데이터 암복호화 과정은 코디네이터와 라우터간, 코디네이터와 디바이스간, 코디네이터와 디바이스간 데이터를 암복호화하는 알고리즘으로 되어 있다. 데이터를 안전하게 전송하기 위해서 데이터를 전송하는 IEEE 802.15.4 송신 노드는 수신 노드의 링크 키를 사용하여 데이터를 암호화하여 전송하고, 데이터를 수신한 노드는 자신의 서명 키로 복호화한다. 코디네이터를 제외한 WPAN상의 IEEE 802.15.4 모든 송신 노드들은 자신의 Trust 데이터를 함께 전송하여 수신 노드로부터 인증을 받는다.

(1) 코디네이터가 라우터에게 데이터를 안전하게 전송하는 과정

[단계 1] 코디네이터 → 라우터 데이터 암호화
- 코디네이터는 라우터의 링크 키로 데이터를 암호화하여 전송

[단계 2] 코디네이터 → 라우터 데이터 복호화
- 라우터는 자신의 서명 키로 데이터를 복호화

(2) 라우터가 코디네이터에게 데이터를 안전하게 전송하는 과정

[단계 1] 라우터 → 코디네이터 데이터 암호화
- 라우터는 코디네이터의 링크 키로 암호화된 데이터와 Trust 데이터를 코디네이터에게 전송

[단계 2] 라우터 → 코디네이터 데이터 복호화
- 코디네이터는 자신의 서명 키로 데이터를 복호화하고 Trust 데이터를 확인

(3) 코디네이터가 디바이스에게 데이터를 안전하게 전송하는 과정

[단계 1] 코디네이터 → 디바이스 데이터 암호화
- 코디네이터는 디바이스의 링크 키로 데이터를 암호화하여 라우터에게 전송

[단계 2] 라우터의 데이터 중계
- 라우터는 데이터와 자신의 Trust 데이터를 디바이스에게 전달

[단계 3] 코디네이터 → 디바이스 데이터 복호화
- 디바이스는 자신의 서명 키로 데이터를 복호화하고 라우터의 Trust 데이터를 확인

(4) 디바이스가 코디네이터에게 데이터를 안전하게 전송하는 과정

[단계 1] 디바이스 → 코디네이터 데이터 암호화
- 디바이스는 코디네이터의 링크 키로 암호화한 데이터와 Trust 데이터를 라우터에게 전송

[단계 2] 라우터의 중계
- 라우터는 디바이스의 Trust를 확인하고 데이터와 디바이스의 Trust 데이터를 코디네이터에게 전달

[단계 3] 디바이스 → 코디네이터 데이터 복호화
- 코디네이터는 디바이스의 Trust 데이터를 확인하고 자신의 서명 키로 데이터를 복호화

(5) 라우터가 디바이스에게 데이터를 안전하게 전송하는 과정

[단계 1] 라우터 → 디바이스 데이터 암화화
- 라우터는 디바이스의 링크 키로 암호화한 데이터와 자신의 Trust 데이터를 전송

[단계 2] 라우터 → 디바이스
- 디바이스는 라우터의 Trust 데이터를 확인하고 자신의 서명 키로 데이터를 복호화

(6) 디바이스가 라우터에게 데이터를 안전하게 전송하는 과정

[단계 1] 디바이스 → 라우터 데이터 암호화
- 디바이스는 라우터의 링크 키로 암호화한 데이터와 Trust 데이터를 전송

[단계 2] 디바이스 → 라우터 데이터 복호화
- 라우터는 디바이스의 Trust 데이터를 확인하고 자신의 서명 키로 데이터를 복호화

3. 키와 Trust 데이터 업데이트 과정

제안한 키와 Trust 데이터 업데이트 과정은 코디네이터가 키의 손실과 무관하게 일정 주기로 마스터 키를 재생성하여 안전하게 마스터 키를 라우터와 디바이스에게 전송하여 1절의 키 설정 과정을 반복함으로써 키와 Trust 데이터를 업데이트 하는 과정이다.

[단계 1] 새로운 마스터 키 재생성 및 전송
- 코디네이터는 새로운 마스터 키와 Sequence number를 자신의 서명키로 전자서명한 데이터를 네트워크 키로 암호화하여 전체 노드에게 전송

[단계 2] 새로운 마스터 키 수신 확인
- 코디네이터를 제외한 모든 노드는 Sequence

Number를 자신의 서명 키로 전자서명한 데이터를 코디네이터의 링크 키로 암호화하여 코디네이터로 전송

[단계 3] 키 설정 과정 재진행

- 코디네이터와 모든 노드들은 새로운 마스터 키를 사용하여 키 설정과정을 재진행

키 업데이트 과정중 장애 발생하여 새로운 마스터 키를 받지 못한 라우터와 디바이스는 코디네이터에 Join 시 Sequence Number와 마스터 키에 전자서명하여 코디네이터의 인증을 받아야 한다.

4. Orphan 노드 관리 과정

제안한 Orphan 노드 관리 과정은 코디네이터 장애 복구후 WPAN내의 노드들이 안전하게 네트워크를 재형성하는 과정과 라우터 장애시 디바이스가 다른 라우터를 통해서 코디네이터에 안전하게 Join하는 알고리즘으로 되어 있다.

(1) 코디네이터 장애복구시 노드들의 Orphan 노드 관리 과정

[단계 1] 키와 Trust 데이터 재생성

- 코디네이터가 일정 시간 이상 장애 발생 후 새로운 네트워크를 형성하려고 할 때는 3.2.3의 키와 Trust 데이터 업데이트 과정 수행

[단계 2] 키 설정 과정 재진행

- 코디네이터와 모든 노드들은 새로운 마스터 키를 사용하여 3.2.1의 키 설정 과정을 재진행

(2) 라우터 장애시 디바이스의 Orphan 노드 관리 과정

[단계 1] 새로운 라우터 스캔

- 라우터가 일정 시간 이상 장애 발생하면, 디바이스는 새로운 라우터를 스캔

[단계 2] 키 설정 과정 재진행

- 디바이스는 새로운 라우터와 3.2.1의 키 설정 과정 수행

IV. 성능시험

1. LR-WPAN 기반 원격검침시스템

LR-WPAN 기반 원격검침 시스템의 구성도는 그림3과 같다. 전체 시스템은 검침 WPAN, 기간사업자의 전송망, 지역 AMR(Automatic Meter Reading)망, 한전 인트라넷으로 구성된다. 검침 WPAN은 수용가에 ZigBee 모뎀 일체형 전자식 전력량계가 설치되고, 수용가의 검침 데이터는 전주에 설치된 데이터 수집장치에 ZigBee 무선망을 통하여 수집된다. 데이터 수집장치는 수집된 검침 데이터를 기간사업자의 전송망인 CDMA 또는 HFC망을 통하여 데이터 부하 관리를 담당하는 FEP장치로 전송한다. FEP장치는 TCP/IP 전용선을 통하여 수집된 검침 데이터를 지역 AMR망의 원격검침서버로 전송한다. 원격검침 서버는 전기 요금 부가하기 위하여 검침 데이터를 한전 인트라넷을 통하여 빌링 호스트로 전송한다. 또한 원격검침 데이터를 활용한 고객 서비스를 제공하기 위하여 AMR WEB 서버로 검침 데이터를 전송한다.

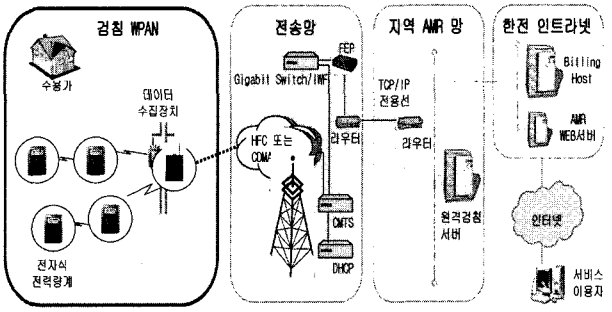

그림 6. LR-WPAN 기반 원격검침 시스템
Fig. 6. LR-WPAN based AMR System.

2. 원격검침 프로파일

본 논문에서 설계한 원격검침 프로파일은 다음과 같이 크게 6개의 개념으로 분류된다.

(1) Profile Identifier

- Name : AMRP - AMR Profile
- Code : 0x15A0
- 설명 : 사용자 정의 AMR Profile Identifier

(2) Device Identifier

- Name : ZigBee AMR Coordinator
- Code : 0x15D0
- Name : ZigBee AMR Device (AMR End Node)
- Code : 0x15D1
- Name : ZigBee AMR Monitoring Device
- Code : 0x15D2
- 설명 : ZigBee AMR Monitoring Device 를 위하여 정의함

(3) End Point

- Name : ZigBee AMR Coordinator
- Code : 0x01

· 설명 : 1 개의 End Point 만을 사용함

(4) Cluster

· Name : IO_MNGT

· Code : 0x01

· 설명 : AMR Data 가 아닌, 관리 및 Test 에 필요한 명령어

· Name : IO_DATA

· Code : 0x02

· 설명 : AMR Data 에 관계 있는 명령어

(5) Attribute Identifier

· IO_MNGT Cluster 의 Attribute

Profile	Cluster	Attribute	Data Type	Attribute Data	Note
AMRP (0x15A0)	IO_MNGT (0x01) +Input +Output	LoopBack	HEX STRING	Byte 0: 1 2 3 4 5 6 / 6: Test Pattern	Loop Back 테스트
		PARA_D (0x0001)		Byte 0: 1 2 3 4 5 6 / 6: Y Y M M D D	Data Setting
		PARA_C (0x0002)		Byte 0: 1 2 3 4 5 6 / 6: h h m m s s	현재시간 Setting
		PARA_M (0x0003)		Byte 0: 1 2 3 4 5 6 / 6: D D X X X X	검침일 Setting
		PARA_T (0x0004)		Byte 0: 1 2 3 4 5 6 / 6: A H H B H H	Tariff Setting
		DeviceId (0x0005)		Byte 0: 1 2 3 4 5 6 / 6: N U M B E R	디바이스 시리얼 번호
	IO_DATA (0x02) +Input +Output	AmrData (0x0000)		Data Format: Byte 0: 1 2 3 4 5 6 7...16 / 0x11: AmrData Payload	원격검침 데이터 포맷참조
		LoadData (0x0001)		Send :: Data Format: Byte 0: 1 2 3 4 / 0x04: Load Identifier; Receive :: Data Format: Byte 0: 1 2 3 4 5 6 7:...20 / 0x14: LoadData Payload	로드프로파일 데이터 포맷 참조

그림 7. 원격검침 프로파일

Fig. 7. WPAN based AMR System.

- 0x0000 : LoopBack Test
- 0x0001 : Date Configuration
- 0x0002 : Current Time Configuration
- 0x0003 : Metering Date Configuration
- 0x0004 : Tariff Configuration
- 0x0005 : Device serial number

· IO_DATA Cluster 의 Attribute

- 0x0000 : AMR Data
- 0x0001 : LOAD Data

(6) Attribute Data

모든 Attribute 에 관계된 Attribute Data 는 "Hex String" Format 이다. Hex String Format 은 LSB 는 Data 의 길이를 나타내고, 데이터 길이 만큼 Payload Data가 확장되는 형식이다.

본 논문에서 설계한 원격검침 프로파일을 정리하면 그림 7과 같다.

원격검침 데이터 포맷과 로드프로파일 데이터 포맷은 각각 그림 8, 그림 9와 같다. 그림 8의 원격검침 데이터 포맷에서 Time은 검침시간으로 각각 월, 일, 시간, 분을 나타내고, 현재월T는 현월 전체 유효전력량(사용량)을 나타내고, 현재월A는 현월 A시간대 사용량을 나타내고, 전월T는 전월 전체 유효전력량을 나타내고, 전월A는 전월 A시간대 사용량을 나타낸다.

그림 9의 로드프로파일 데이터 포맷에서 L1, L2, L3, L4는 각각 전력량계의 레지스터에 저장된 1시간 단위의 전력부하량을 나타낸다.

Time				현재월T	현재월A	전월T	전월A	Status
M	D	h	m	3-byte	3-byte	3-byte	3-byte	1-byte

그림 8. 원격검침 데이터 포맷

Fig. 8. AMR Data Format.

L1	L2	L3	L4
5-byte Load Data	5-byte	5-byte	5-byte

그림 9. 로드 프로파일 데이터 포맷

Fig. 9. Load Profile Data Format.

3. 실험결과

가. 실험 시스템 및 파라미터

성능평가를 위해 사용한 시스템은 그림 10과 같고, 사용한 RF모듈들은 네트워크 확장성과 테스트 편의성

그림 10. 성능평가를 위한 실험 시스템
Fig. 10. Test System for Performance Evaluation.

표 1. 실험 파라미터
Table 1. Test Parameter

구 분	값	비 고
사용 채널	#13	
네트워크 Depth	4 Hop	
데이터 Size	30Byte	
검침 주기	15분	
암호화 알고리즘	ECC-169	
해쉬 함수	CCM*	
키 사이즈	169bit	링크 키, 서명 키

을 고려하여 FFD(Full Function Device)이며, Beacon-Enabled 네트워크를 형성하기 위하여 Channel Access 매커니즘으로는 Slotted CSMA-CA방식을 사용하고, 다중 홉 (Multi-hop) 기반의 점 대 점 방식으로 클러스터 트리(Cluster tree) 네트워크 토폴로지를 가지고 요구기반 라우팅 알고리즘인 AODV 라우팅 알고리즘을 사용한다.

검침 네트워크가 운영되는 장소가 실외인 점을 감안하여 성능평가를 위한 실험장소는 실내 및 실외 테스트를 시행하고 실험에 사용된 노드 수는 실험 항목에 따라 다르지만 코디네이터 2개, 디바이스 38개가 사용되었다. 실험을 위해서 사용한 전원은 실내 테스트에는 일반 상용전원을 사용하고, 실외에서는 보유한 전력량계의 수가 한정되어 전력량계에 RF 모듈 내장시에는 12V 밧터리를 이용하여 전력량계에 전원을 공급하고 RF 모듈이 전력량계에서 전원을 공급받도록 하였고, RF 모듈만 동작시킬 경우에는 3V 밧터리 전원을 사용하였다. 전력량계에 내장된 RF 모듈은 IR 통신을 통하여 전력량계내의 데이터를 읽고 전송하고, 3V 밧터리로 동작하는 RF 모듈은 모듈 자체에 저장된 데이터를 전송하도록 하였다. 표 1은 성능평가를 위한 실험 파라미터를 나타낸다.

나. 실험결과

38개 노드에 15분 주기로 시행한 화면은 그림 4-5와 같다. 10개의 노드는 실내에 설치하고, 28개의 노드는 실외에 설치하였다. 이 때 에러율은 11,985회의 코디네이터 요구에 38개의 에러가 있었다.

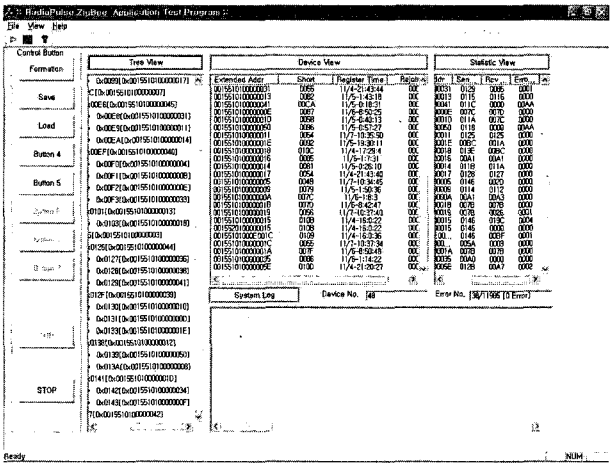

그림 11. 실내외 주기적인 테스트
Fig. 11. Indoor and Outdoor Test.

V. 비교 및 고찰

1. 기존 MANET 보안 알고리즘과의 비교

기존 MANET 보안 알고리즘과 제안한 공개키 기반의 키 설정 및 보안 알고리즘에 대한 보안 성능을 비교하면 다음과 같다. 첫째, n개의 노드로 이루어진 네트워크에서 전체 노드에 기존 대칭키 기반의 키 분배 및 관리 프로토콜을 사용하여 링크 키를 생성하면 2n-1개의 링크 키가 생성되고, 공개키 기반의 키 분배 및 관리 프로토콜을 사용하면 n개의 링크 키가 생성되므로 코디네이터의 키 관리가 훨씬 수월하다. 또한 SKKE 프로토콜은 코디네이터로 집중 트래픽이 발생되고, Trust Relation 과정에서 코디네이터가 디바이스에게 마스터 키를 전송할 때 인증과정이나 암호화 과정이 없다는 단점이 있다. UKE 프로토콜은 SKKE의 문제점을 그대로 수용하고, 마스터 키가 고정적인 디폴트 값이기 때문에 링크 키를 생성하는 암호학적인 보안 알고리즘을 적용하지 않았고, 디바이스의 인증과정없이 링크 키를 설정하기 때문에 보안적인 취약성이 있다.

둘째, 기존 공개 키 방식의 키 분배 및 관리 프로토콜인 PKKE는 디바이스간 Trust를 디바이스의 ID와 상응하는 서명되지 않은 공개 키를 교환하여 설정하기 때문에 암호학적으로 공개키를 소유한 디바이스를 확인할 수 없으므로 디바이스의 ID와 공개 키에 대한 인증을 할 수 없다는 단점이 있다. CBKE 프로토콜은 별도의 인증기관을 필요로 하는데 Ad hoc 네트워크인 WPAN에서 일반적으로 별도의 CA를 설치하는 것은 현실적으로 어렵고, CA와 WPAN상의 코디네이터, 라우터, 디바이스 등 각 노드들간의 인증과정이 생략되어 있고, 인증서의 사용기간, CRL(Certificate Revocation List) 관리 방법, CA간 상호 인증 등 PKI(Public Key Infrastructure) 구조에 고려가 되어 있지 못하다는 단점이 있다.

셋째, 기존 라우팅 보안 프로토콜은 라우팅 알고리즘마다 알고리즘을 수정하여 적용해야 한다는 단점이 있고, 대부분의 라우팅 알고리즘에서 사용하는 TESLA라이중 해쉬 알고리즘에서는 키 분배 및 관리 과정을 생략하고 안전하게 키가 교환되었고 모든 노드들이 주변 노드의 공개 키를 인식하고 있다는 가정에서 진행한다. 또한 경로상의 모든 노드의 Trust가 기검증된 것으로 가정한다. 즉, 라우팅 보안 프로토콜에서 인증은 노드에 대한 인증이 아닌 메시지에 대한 인증을 뜻하고, 메시지에 대한 인증도 실시간으로 이루어지는 것이 않고 패킷을 버퍼링해 두었다가 일정시간이 지난 후에 가능하다.

넷째, 기존 연구에서는 MANET의 견고성 (robust)을 향상시키기 위해서 손상된 노드들이 자기 편인 적대 노드들 (adversary nodes)을 인증하여 네트워크에 합류시키는 것을 막는 것이 중요한 논점이었다. MANET 상의 어떤 노드가 중간에 손상되는 것을 막을 수 없지만, 이러한 손상된 노드들로 인하여 네트워크 전체가 손상되는 일이 없도록 하기 위해서이다. Threshold Cryptography 기반의 손상된 노드 검색 알고리즘은 SK가 k개의 node들에 분산되어 k-threshold security를 제공해 주지만 threshold값을 넘어서 손상된 노드가 k개 이상이 되면 전체 네트워크 보안이 무너지게 된다는 단점이 있다. 또한 인증 서비스 단계에서는 어떤 노드가 인증 서비스를 요청하면, 주위의 k개의 비밀 공유분을 보유한 인접 이웃 노드들이 부분 인증서(Partial Certificate)를 인증 서비스를 요청한 노드에게 전송하기 때문에 메시지를 송수신 하는 노드마다 인증 서비스를 요청하면 트래픽이 너무 많이 발생되고 비효율적이라는 단점이 있다.

제안한 키 교환 및 보안 알고리즘의 장점은 다음과 같다. 첫째, 기존 MANET 또는 WPAN 보안 알고리즘들은 보안 알고리즘에 의한 인증 과정없이 코디네이터에 인증이 가능하지만, 제안한 키 교환 및 보안 알고리즘은 WPAN상의 노드가 코디네이터에 Join하기 위해서는 공개 키 기반의 인증 과정을 거치고, 서명 키와 Trust 데이터를 이용할 뿐 아니라 이를 주기적으로 업데이트하는 과정을 거침으로써 코디네이터와 노드들간 또는 노드와 노드간 안전하게 통신할 수 있다. 둘째, Threshold Cryptography 알고리즘들은 k개의 노드가 손상되면 전체 네트워크 보안이 위협을 받지만 제안한 공개키 기반의 알고리즘은 해당 노드의 보안만 문제가 되기 때문에 네트워크 견고성이 향상된다. 셋째, WPAN의 장애발생시 Orphan 노드에 대한 인증과정을 통하여 손상된 노드들을 통하여 적대 노드들이 네트워크에 합류하는 것을 차단할 수 있다

2. SKKE 알고리즘과의 성능 평가

가. 2 홉에서의 제안한 알고리즘의 성능 평가

그림 12와 같은 2 홉 WPAN 토폴로지에서 기존 SKKE 알고리즘과 제안한 공개키 기반의 키 설정 알고리즘을 비교하여 성능평가를 시행한다.

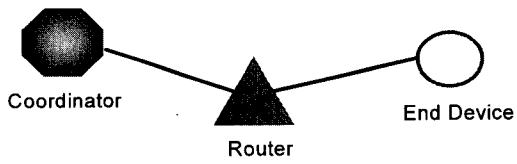

그림 12. 2 홉 WPAN 토폴로지
Fig. 12. 2 Hop WPAN Topology.

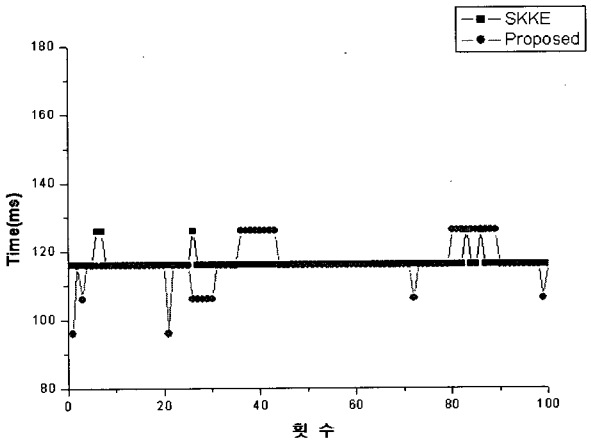

그림 13. 2 홉에서의 제안한 알고리즘의 성능 평가
Fig. 13. Performance Evaluation of Proposed Algorithm Appling 2 Hop.

2 홉에서 기존 SKKE 알고리즘과 제안한 공개키 기반의 키 설정 알고리즘을 비교하여 성능평가를 100회 시행한 결과는 그림 13과 같다. 2홉에서는 기존 알고리즘과 제안한 알고리즘의 성능이 거의 같거나 제안한 방식이 성능이 조금 떨어지는 것으로 나타났다.

나. 3 홉에서의 제안한 알고리즘의 성능 평가

그림 14와 같은 3 홉 WPAN 토폴로지에서 기존 SKKE 알고리즘과 제안한 공개키 기반의 키 설정 알고리즘을 비교하여 성능평가를 시행한다.

3홉에서 기존 SKKE 알고리즘과 제안한 공개키 기반의 키 설정 알고리즘을 비교하여 성능평가를 100회 시행한 결과는 그림 15와 같다. 3홉에서는 제안한 알고리즘의 성능이 기존 알고리즘보다 성능이 조금 향상되는 것으로 나타났다.

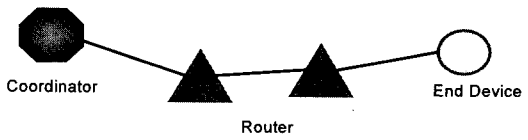

그림 14. 3 홉 WPAN 토폴로지
Fig. 14. 3 Hop WPAN Topology.

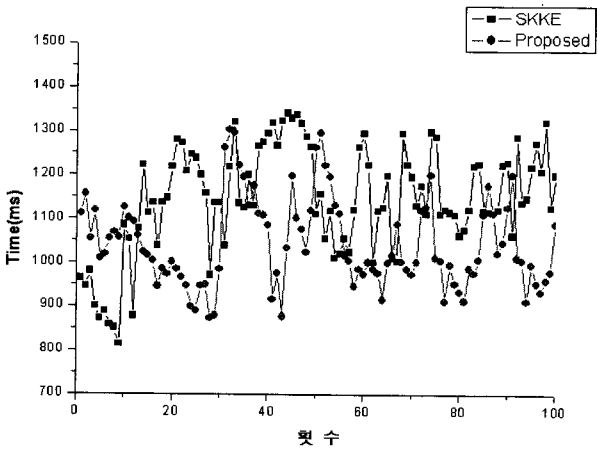

그림 15. 3 홉에서의 제안한 알고리즘의 성능 평가
Fig. 15. 3 Performance Evaluation of Proposed Algorithm Appling 3 Hop.

다. 4 홉에서의 제안한 알고리즘의 성능 평가

그림 16과 같은 4 홉 WPAN 토폴로지에서 기존 SKKE 알고리즘과 제안한 공개키 기반의 키 설정 알고리즘을 비교하여 성능평가를 시행한다.

4홉에서 기존 SKKE 알고리즘과 제안한 공개키 기반의 키 설정 알고리즘을 비교하여 성능평가를 100회 시행한 결과는 그림 17과 같다. 4홉에서는 제안한 알고리즘의 성능이 기존 알고리즘보다 성능이 많이 향상되는 것으로 나타났다.

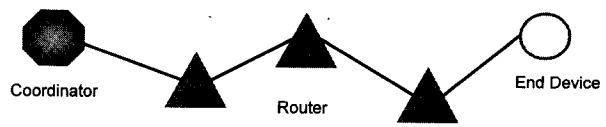

그림 16. 4 홉 WPAN 토폴로지
Fig. 16. 4 Hop WPAN Topology.

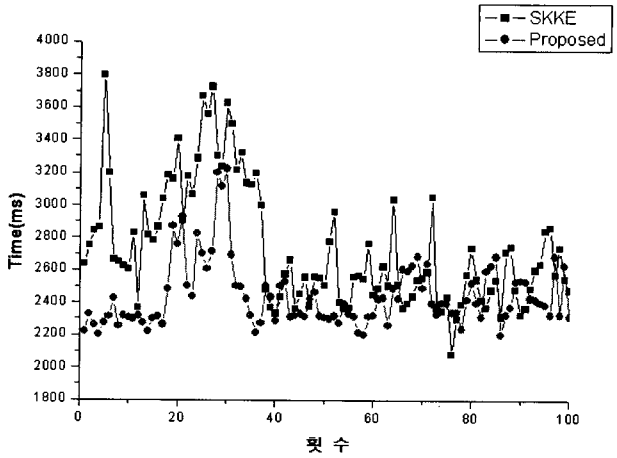

그림 17. 4 홉에서의 제안한 알고리즘의 성능 평가
Fig. 17. Performance Evaluation of Proposed Algorithm Appling 4 Hop.

3. 성능 평가에 대한 고찰

키 교환 및 보안 알고리즘에서 데이터 암복호화 과정은 대칭 키 기반 알고리즘이 속도면에서 공개키 기반 알고리즘보다 빠르다는 것은 주지의 사실이기 때문에 비교하지는 않았다. 또한 키 및 Trust 데이터 업데이트

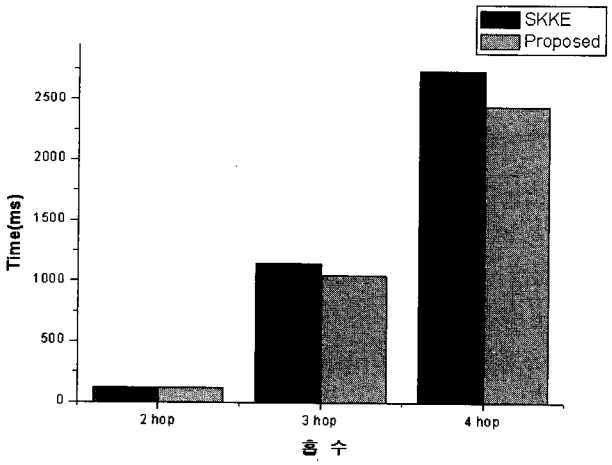

그림 18. 제안한 키 설정 알고리즘에 대한 평균시간 분석
Fig. 18. Mean Time Analysis of Proposed Key Establishmen.

과정이나 Orphan Management 과정은 비교 대상이 없기 때문에 구현한 결과를 제시하였다. 제안한 공개키 기반의 키 설정 과정에 대한 성능평가 결과를 분석하기 위하여 홉 수의 변화에 따른 기존 SKKE 알고리즘과 제안한 키 설정 과정을 비교하면 그림 18과 같다. 본 논문에서 SKKE 알고리즘과 비교하여 성능평가를 시행한 이유는 ZigBee Alliance에서 Commercial 어플리케이션에서는 SKKE를 사용하도록 권고하고 있기 때문이다. 홉 수가 증가될수록 기존 알고리즘보다 제안한 알고리즘의 성능이 향상됨을 알 수 있다. 기존 SKKE 알고리즘은 대칭키 기반이기 때문에 홉 수가 적을 때는 제안한 알고리즘보다 빠르지만, SKKE 알고리즘의 복잡성으로 말미암아 홉 수가 증가되면 오히려 제안한 알고리즘보다 시간이 많이 걸림을 알 수 있다.

V. 결 론

본 논문에서는 IEEE 802.15.4 LR WPAN의 보안적인 문제점들을 해결하기 위하여 공개키 기반의 키 교환 및 보안 알고리즘을 제안하였다. 제안한 키 교환 및 보안 알고리즘은 네 과정으로 이루어진다. 첫째, 키 설정 과정은 IEEE 802.15.4 노드간 안전하게 키를 생성하고 상호 인증과 키를 교환하는 과정으로 코디네이터와 라우터간 키를 생성하고 상호 인증과 키를 교환하는 알고리즘과 디바이스와 코디네이터간 라우터를 통해 키를 설정하고 상호 인증과 키를 교환하는 알고리즘으로 되어 있다. 둘째, 데이터 암복호화 과정은 데이터를 코디네이터와 라우터간, 코디네이터와 디바이스간, 라우터와 디바이스간 데이터를 암복호화하는 알고리즘으로 되어 있다. 셋째, 키 및 Trust 데이터 업데이트 과정은 키 설정 과정에서 설정한 키와 Trust 데이터를 주기적으로 업데이트하는 알고리즘이다. 넷째, Orphan 노드 관리 과정은 WPAN상의 코디네이터나 라우터의 장애시 노드들이 Orphan 디바이스가 되어 네트워크 재등록 과정시 안전하게 네트워크에 등록하는 알고리즘이다.

또한 통신 신뢰성 및 보안에 대한 취약성을 가지는 전력선 통신 기반의 원격검침시스템의 단점을 보완할 수 있는 IEEE 802.15.4 WPAN 기반의 원격검침 모델을 제시하고, ZigBee Alliance의 프로파일 규격을 따르면서, Attribute Data를 IEC 1107의 계량기 프로토콜 규격을 기반으로 하는 원격검침 프로파일에 제안한 보안 알고리즘을 적용함으로써 보안성을 향상시키도록 하였다.

제안한 사항들에 대한 성능평가를 다음과 같이 수행하였다. 첫째, 실험 시스템에 제안 사항들을 구현하여, 제안한 사항별로 구현한 결과와 실험 결과를 분석하였다. 코디네이터와의 거리가 반경 20m이내의 실내에 있는 10개의 노드에 대해서는 10초 주기로 주기검침을 시행하였고, 코디네이터와 반경 50m이내의 실내외에 있는 38개의 노드에 대해서는 15분 주기로 시행하였는데, 38개 노드에 대해서 11,985회 시행시 38개의 에러가 발생하여 에러율은 약 0.3%로 나와서 신뢰성이 높은 것으로 나타났다. 둘째, 제안 사항 중 키 설정 과정에 대해서 기존 알고리즘과 비교하여 성능 평가를 수행하였다. 기존 SKKE 알고리즘과 제안한 알고리즘을 비교하여 성능평가를 시행한 결과, 홉 수가 증가될수록 기존 알고리즘보다 제안한 알고리즘의 성능이 향상됨을 알 수 있었다. 제안한 알고리즘과 SKKE 알고리즘간 비교시 2홉에서는 거의 같고, 3홉에서는 약150ms정도, 4홉에서는 약 300ms정도 향상됨을 알 수 있었다.

참 고 문 헌

[1] Frank Stajano, Ross Anderson, "The Resurrecting Duckling : Security Issues in Ad-Hoc Wireless networks,", Security Protocols, 7th International Workshop Proceedings,

[2] Frank Stajano, "The Resurrecting Duckling: What Next?," Security Protocols, 7th International Workshop Proceedings, Springer-Verlag, Lecture Notes in Computer Science, April 2000

[3] Konrad Wrona, "Distributed Security: Ad Hoc Networks & Beyond," Ad Hoc Network Security PAMPAS Workshop, September 2002.

[4] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, pp. 24-30, November/December 1999

[5] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks," Proceedings of International Conference on Network Protocols (ICNP '01), November 2001.

[6] J. Staddon, S. Miner, and M. Franklin, "Self-Healing Key Distribution with Revocation," Proceedings of 2002 IEEE Symposium on Security and Privacy (S&P2002), May 2002.

[7] Haiyun Luo, Petros Zefros, Jiejun Kong, Songwu Lu, and Lixia Zhang, "Self-securing Ad Hoc Wireless Networks," 7th IEEE Symposium on Computers and Communications (ISCC '02), July

2002.
[8] V. Shoup, "Practical Threshold Signatures," Proceedings of EUROCRYPT '00, Springer-Verlag, Lecture Notes in Computer Science 1807, pp. 207-220, May 2000.
[9] Yih-Chum Hu, Adrian Perrig, David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,"Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom '02), September 2002.
[10] Xinjun Du Ying Wang Jianhua Ge Yumin Wang, "A Method for security Enhancements in AODV Protocol," Proceedings of the 17 th International Conference on Advanced Information Networking and Applications (AINA'03), March 2003
[11] 유병익, 임정미, 유선영, 박창섭, "이중 해쉬체인에 기반을 둔 Link-State 라우팅 보안 매커니즘," 한국정보보호학회 논문지 제13권 제2호, 2003.
[12] Chartwell, "The Chartwell AMR Report 2003 8th Edition", October 2003.
[13] PLC포럼 디지털 가전위원회, "Home Network Control Protocol (HNCP)PreSpec. Ver.1.0," PLC 포럼, 2002.
[14] 기술표준원, "고속 전력선통신(PLC) 국가표준(KS) 공청회," 2006.
[15] 이지홍, 하인수, 김인식, "PCS와 원칩 마이크로콘트롤러를 이용한 원격검침 시스템," 2000년도 대한전자공학회 하계종합학술대회 논문지 제23권 제1호, pp. 171-174, 2000.
[16] 박종연, 조호찬, 최승지, "전력선 통신과 공중 전화망에 의한 전력량의 원격 검침 시스템의 개발," 2002년도 대한전자공학회 하계종합학술대회 논문지 제25권 제1호, pp. 311-314, 2000.
[17] Messerges T. et al, "A Security Design for a General Purpose, Self-organizing, Multihop Ad Hoc Wireless Network," MITSUBISHI ELECTRIC RESEARCH LABORATORIES TR2003-114, December 2004,
[18] ZigBee Alliance Document 03522 : Security Service Specification, December 2004.

저 자 소 개

김 진 철(정회원)
1995년 광운대학교 전자통신공학과 학사
1997년 광운대학교 대학원 전자통신공학과 석사
2006년 광운대학교 대학원 전자통신공학과 박사
1996~현재 한전KDN(주) 전력IT연구원 차장
<관심분야> MANET, Network Security

오 영 환(종신회원)
2006년 대한전자공학회 논문지 제45권 TC편 제4호 참조